



# Release Notes for Cisco Security MARS Appliance 4.3.1

---

Revised: July 24, 2009, OL-14668-01



**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 4.3.1 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 6](#)
- [Important Notes, page 14](#)
- [Quick Install Notes, page 16](#)
- [Caveats, page 20](#)
- [Product Documentation, page 41](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 42](#)

## Introduction

Version 4.3.1 is now available as an upgrade to 4.2.8 of your MARS Appliance software. Registered SMARTnet users can obtain version 4.3.1 from the Cisco support website at:

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

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



---

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

© 2007 Cisco Systems, Inc. All rights reserved.

# Supported Hardware

Cisco Security MARS Version 4.3.1 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:

- [Data Migration Support, page 3](#)
- [Centralized Password Management—External AAA Server Support, page 3](#)
- [Account Locking—Login Security, page 3](#)
- [Monitoring Global Controller Connection Status from the Local Controller, page 4](#)
- [GUI and CLI Timeout Interval, page 4](#)
- [Support for Cisco IPS 6.0 Dynamic Signature Updates, page 4](#)
- [Miscellaneous Changes and Enhancements, page 5](#)
- [New Vendor Signatures, page 5](#)

## Data Migration Support

Beginning with this release, you can migrate configuration and event data from a MARS Appliance running 4.x to a newer model running 5.x. For detailed instruction on how to perform this operation, see *Migrating Data from Cisco Security MARS 4.x to 5.3.x*. at the following URL:

[http://www.cisco.com/en/US/docs/security/security\\_management/cs-mars/4.3/migration/guide/dmigrate.html](http://www.cisco.com/en/US/docs/security/security_management/cs-mars/4.3/migration/guide/dmigrate.html)

## Centralized Password Management—External AAA Server Support

External Authentication, Authorization, and Auditing (AAA) servers can now act as the authentication mechanism for MARS Appliance GUI logins (username and password). Previously, each MARS Appliance authenticated login name/password combinations with the appliance's local user database. Release 4.3.1 supports the following external RADIUS AAA servers:

- Cisco Secure Access Control Server (ACS)
- Microsoft Internet Authentication Service (IAS) Server
- Juniper Networks Steel belted RADIUS

Further Information is available at the following URL:

[http://www.cisco.com/en/US/docs/security/security\\_management/cs-mars/4.3/user/guide/local\\_controller/authen.html](http://www.cisco.com/en/US/docs/security/security_management/cs-mars/4.3/user/guide/local_controller/authen.html)

## Account Locking—Login Security

Previously, MARS Appliances permitted an unlimited number of login attempts. With Release 4.3.1, the administrator can configure the GUI to lock after a specified number of failed login attempts, or can configure the GUI to never lock. To set the Account Lockout Policy, navigate to the AAA configuration page (**Admin > System Setup > Authentication Configuration**).

The administrator can unlock accounts from the User Management page (**Management > User Management**), or with the new **unlock** CLI command.



### Note

---

Per Open Caveat CSCsk31615 in Release 4.3.1, when MARS fails in an attempt to connect to a specified external AAA server, MARS behaves as if the user had performed a failed login. This can result in users being locked out of the GUI even when they are entering the correct login name and password combination. For example, if three AAA servers are specified, and all three attempts to connect to them fail, and the Maximum Login Failures parameter is set to 3, the user will be locked out of the GUI with one valid login attempt. This behavior will change in a future release.

---

Further information is available at the following URL:

[http://www.cisco.com/en/US/docs/security/security\\_management/cs-mars/4.3/user/guide/local\\_controller/authen.html#wp1198343](http://www.cisco.com/en/US/docs/security/security_management/cs-mars/4.3/user/guide/local_controller/authen.html#wp1198343)

## Monitoring Global Controller Connection Status from the Local Controller

Previously, the connection status between a Local Controller and a Global Controller was reported on the Global Controller's Zone Controller Information page (**Admin > System Setup > Local Controller Management**).

With Release 4.3.1, the Local Controller now generates syslogs to record communication problems caused by the following events:

- Local Controller cannot connect to the Global Controller
- Local Controller certificate is not on the Global Controller or vice versa
- Local Controller and Global Controller are operating with incompatible MARS release versions

Release 4.3.1 defines seven new events, three new system rules, and two new system reports on the Local Controller to monitor the connection status with the Global Controller.

Further information is available at the following URL:

[http://www.cisco.com/en/US/docs/security/security\\_management/cs-mars/4.3/user/guide/global\\_controller/gccfg.html#wp1055211](http://www.cisco.com/en/US/docs/security/security_management/cs-mars/4.3/user/guide/global_controller/gccfg.html#wp1055211)

## GUI and CLI Timeout Interval

Previously, the GUI would timeout after 30 minutes of inactivity. With Release 4.3.1, the timeout interval for the GUI can be set at 15, 30 (default), 45, and 60 minutes, or as Never (never will timeout). Different GUI timeout intervals can be set for the Administrator, Security Analyst, and Operator roles. The Administrator parameter also sets the CLI timeout.

To access the Timeout Configuration page, navigate to **Admin > System Parameters > Timeout Settings**.

## Support for Cisco IPS 6.0 Dynamic Signature Updates

This feature downloads new signatures from CCO and correctly process and categorize received events that match those signatures, which includes them in inspection rules and reports. These updates provide event normalization and event group mapping, and they enable your MARS Appliance to parse day zero signatures from the IPS devices.

By default, this feature is enabled and requires you to configure it. If you do not configure it, the following rule fires:

System Rule: CS-MARS IPS Signature Update Failure

This rule fires daily until you configure the feature. To address the issue identify by this firing rule, do one of the following:

- Specify the username and password pair to use when pulling the signature updates from CCO.
- Specify a local server where the MARS-IPS packages reside in the URL for Signature update field.
- Disable the feature.

For information on configuring the feature, see [IPS Signature Dynamic Update Settings](#).

## Miscellaneous Changes and Enhancements

The following changes and enhancements exist in 4.3.1:

- **Global Controller-to-Local Controller Communication Enhancements.** Enhancements include more efficient data batches, reduced transfer times, and a prioritization on recent data. If a data backlog occurs due to a Global Controller-to-Local Controller disconnect, the Local Controller sends recent data first and stays in sync with new data coming in. The Local Controller catches up with older data over time.
- **Syslog Forwarding.** Designate a syslog collector and forward syslog messages received from one or more IP addresses to that collector. See the **syslogrelay setcollector**, **syslogrelay src**, and **syslogrelay list** commands in *Appendix A: Command Reference* in the *Install and Setup Guide for Cisco Security MARS*. See “Syslog Relay Support” in *Chapter 2: Reporting and Mitigation Devices Overview* of the *User Guide for Cisco Security MARS Local Controller*.
- **Password Management Enhancement.** Non-administrative users can change the password associated with their account. Previously, editing a MARS user was considered an administrative task and limited to those accounts with the admin role.
- **Raw Message Log Enhancement.** To view and delete queries in the local cache, click the **View Cache** button on the Retrieve Raw Messages page accessed from **Admin > System Maintenance > Retrieve Raw Messages**. Previously, queries were purged automatically every two weeks; this feature helps avoid disk space shortages that could occur before that period elapsed.
- **GC2R Support.** The 4.3.1 and 5.3.1 releases are interoperable, allowing the GC2R to manage Local Controllers running 4.3.1 on the following models: MARS 20R, MARS 20, and MARS 50.
- **Enhanced Cisco Device Support:**
  - IPS 6.0
  - PIX / ASA 7.2
  - CSA 5.0, 5.1, and 5.2
  - Cisco IOS Release 12.4(11)T through IOS Release 12.4(11)T4
  - FWSM 3.1.3 and 3.1.5
- **Enhanced 3rd-Party Device Support.**
  - ISS Site Protector 2.0
  - CheckPoint R61, R62, and R65.
- **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 5](#)
- **Bug fixes.** For the list of resolved issues, see [Resolved Caveats - Release 4.3.1, page 28](#).

## New Vendor Signatures

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

Revised in 4.3.1	Product	Signature Version Supported
<b>Intrusion Prevention and Detection Signatures</b>		
Yes	Cisco IDS 4.0, Cisco IPS 5.x, Cisco IOS 12.2	Current through S299 signature release.
Yes	Snort NIDS 2.6.1	Current through the July 7, 2007 signature release
No	ISS RealSecure Network Sensor 6.5 and 7.0, and ISS RealSecure Server Sensor 6.5 and 7.0	XPU 27.010 Release date: May 8, 2007
No	McAfee IntruShield NIDS 1.8 McAfee Network Intruvert v 2.1.9.104	2.1.68.5 Release date: June 12, 2007
Yes	McAfee Entercept HIDS 6.x	Current through the August 21, 2007 signature release.
Yes	CheckPoint Application Intelligence (VPN-1 NG with Application Intelligence R55)	Current through the August 6, 2007 signature release
No	Netscreen IDP 2.1	Signature version: 2.1 r7. Release date: March 10, 2007
Yes	Enterasys Dragon 6.x, 7.x	Current through the July 3, 2007 signature release.
Yes	Symantec NIDS, v 4.0	Signature package: 84 Release date: July 15, 2007
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.
<b>Vulnerability Scanner Signatures</b>		
Yes	Qualys QualysGuard 3.x, 4.7.161-1	Current through the August 17, 2007 signature release.
Yes	E-Eye, Retina Scanner Vulnerability Software, version 5.6 <sup>1</sup>	Current through the August 20, 2007 signature release.
Yes	Foundstone, version 4.x	Current through the August 23, 2007 signature release.
Yes	Common Vulnerabilities and Exposures (CVE) Database	Current with the August 15, 2007 definition update.

1. eEye REM 1.0 is supported in 4.2x.

## Upgrade Instructions

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

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

## Important Upgrade Notes

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

### Upgrade to 4.3.1

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 5.3.1 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 8](#)).
  - Step 2** Log into the Global Controller web interface, and select **Admin > System Setup >- Local Controller Management**.
  - Step 3** For each Local Controller, select the Local Controller checkbox and click **Details**.

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

---

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

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

## Upgrade to 4.2.2

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

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

The following issues can occur when upgrading your reporting devices:

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

## Upgrade to 4.2.1

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

## Upgrade to 4.1.5

No important notes exist for the 4.1.4 upgrade.

## Upgrade to 4.1.4

No important notes exist for the 4.1.4 upgrade.

## Upgrade to 4.1.3

No important notes exist for the 4.1.3 upgrade.

## Upgrade to 4.1.2(2042)

The following notes detail changes to the standard upgrade process:

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

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

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

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

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

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

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

## Upgrade to 4.1.1

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

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

## Required Upgrade Path

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

**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              |

**Table 1 Upgrade Path Matrix**

| From Version           | Upgrade To <sup>1</sup> | Upgrade Package  |
|------------------------|-------------------------|------------------|
| 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 |

1. An asterisk (\*) next to a package name in this column identifies that this upgrade must be performed from the command line, as GUI support was lost with the closing of the upgrade.proteogonetwork.com website.
2. To upgrade from 4.1.1 or 4.1.2 (2040) to 4.1.2(2042), please review the special upgrade notes in the *Quick Install and Release Notes for Cisco Security MARS Appliance 4.1.2 (2042)*.
3. The 4.2.3 upgrade package is approximately 1.6 GB due to the large number of signatures updated and due to the inclusion of a patch to the database software. Downloading the ISO image may take longer than previous packages.

## Downloading the Upgrade Package from CCO

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

**Top-level page:**

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

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

*Result;* The Download Software page loads.

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

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



**Note**

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

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

- [http://www.cisco.com/en/US/applicat/cdcrgrstr/applications\\_overview.html](http://www.cisco.com/en/US/applicat/cdcrgrstr/applications_overview.html)

## Important Notes

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

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

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>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Reference Number | Description                                                                                                                                                                                                                                                                                                                                             |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 17](#)

## Installation Quick Reference

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

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

**Table 2**      **Quick Reference**

| Task                                                            | References in Install Guide                                                |
|-----------------------------------------------------------------|----------------------------------------------------------------------------|
| Use the rack mount kit to install the MARS Appliance in a rack. | <a href="#">Installing the MARS Appliance in a Rack</a>                    |
| Connect the MARS Appliance to an AC power source.               | <a href="#">Connecting to the AC Power Source</a>                          |
| Connect network and console cables.                             | <a href="#">Connecting Cables</a>                                          |
| Turn on the appliance.                                          | <a href="#">Powering on the Appliance and Verifying Hardware Operation</a> |

**Table 2** Quick Reference (continued)

| Task                                                       | References in Install Guide                                                |
|------------------------------------------------------------|----------------------------------------------------------------------------|
| Verify initial power up.                                   | <a href="#">Powering on the Appliance and Verifying Hardware Operation</a> |
| Perform initial configuration of the MARS Appliance.       | <a href="#">Checklist for Initial Configuration, page 17</a>               |
| Configure the MARS Appliance to monitor reporting devices. | <a href="#">Next Steps</a>                                                 |

## Checklist for Initial Configuration

Initial configuration of the appliance accomplishes several goals:

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

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

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

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

| ■ | Task                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ■ | <p data-bbox="228 281 638 310"><b>4. Command Line Configuration.</b></p> <p data-bbox="269 325 1507 483">The third and final task of the initial CLI configuration involves specifying those settings that help ensure the integrity of the event correlation and complete your network connection, allowing access to the appliance from other hosts on the network. In other words, after you complete this phase, you can connect to and complete the appliance configuration using a non-console connection from any host on your network. To complete this task, you must:</p> <ul data-bbox="282 499 1284 751" style="list-style-type: none"><li>• Log in to the appliance using the system administrative account and the new password.</li><li>• Set any additional static routes.</li><li>• Set the clock.</li><li>• Set the NTP server settings.</li><li>• Set the DNS domain name.</li><li>• Connect the appliance to the network (that is, plug in the Cat 5 cables.)</li></ul> <p data-bbox="269 768 1507 861"><i>Result:</i> Now you have network connectivity. You can access the CLI interface using an Secure Shell (SSH) client on any host that can reach the appliance, and you can log in to the web interface to complete the initial configuration.</p> <p data-bbox="269 877 570 907">For more information, see:</p> <ul data-bbox="282 924 708 1041" style="list-style-type: none"><li>• <a href="#">Specify the Time Settings</a></li><li>• <a href="#">Set Up Additional Routes</a></li><li>• <a href="#">Completing the Cable Connections</a></li></ul> |

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

## Caveats

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

- [Open Caveats - Release 4.3.1, page 21](#)
- [Resolved Caveats - Release 4.3.1, page 28](#)
- [Resolved Caveats - Releases Prior to 4.3.1, page 41](#)

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 4.3.1

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

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

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

| Reference Number | Description                                                             |
|------------------|-------------------------------------------------------------------------|
| CSCsk90015       | Cisco ACS 3.x not accessible after upgrade to MARS x.3.1                |
| CSCsk60311       | Mars - Option to check logs pulling status                              |
| CSCsk59030       | MARS OpenSSH GSSAPIDelegateCredentials vulnerability                    |
| CSCsk57521       | Test Connectivity to CSM fails when CSM password contains special chars |
| CSCsk51397       | Adding many incidents to the case slows down the MARS gui performance   |
| CSCsk49710       | User Guide - NetScreen device configuring syslog screenshot incorrect   |
| CSCsk45704       | User account always display locked                                      |
| CSCsk43710       | Gen2 GC miss Gen1 LC's info on the license page                         |
| CSCsk42805       | Statistics backlog creates high CPU condition                           |
| CSCsk39645       | GUI doesn't check duplicate agent ip address when adding application    |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsk31615       | Should not increase the number of failure for AAA server unaccessible    |
| 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         |
| CSCsk21865       | LC/GC comm broken due to java io stream header corruption exception      |
| CSCsk19730       | Null XML_KEY_VALUE XML causes rule to go inactive on LC/GC sync          |
| CSCsk17861       | Mars released DVD contains GUI management source codes                   |
| CSCsk12489       | operator role can not resubmit report                                    |
| CSCsk12156       | Configuration Sync (GC --> LC) can have parallel threads doing dupe work |
| CSCsk11592       | ids didn't get monitored networks from msfc if discover ids first        |
| CSCsk08028       | Real time multi column query is not working.                             |
| CSCsk06363       | System Rule: Resource Issue: CS-MARS should include drop counts events   |
| CSCsk04282       | MARS failed to import 1000 hosts vulnerablilty information               |
| CSCsk03722       | Test Connectivity returning error                                        |
| CSCsk03186       | Error during discovery of Netscreen SSG5 w/ ScreenOS 5.0                 |
| CSCsk03022       | After LC was deleted from GC, GC-LC communication goes on forever        |
| CSCsk02989       | GC is not usable when LC has lots of deleted devices                     |
| CSCsk02261       | XPATH is change to find open ports information from QG 5.0 xml file      |
| CSCsk62114       | Wrong spelling Error Messages                                            |
| CSCsk62697       | IPS6x is not supported in seed file import in 4.3.1/5.3.1                |
| CSCsj96747       | Networks and Groups propogated 2 LC are deleted after its removed fr GC  |
| CSCsj96592       | Adding LC with version lower than 4.3.1 should version mismatch err      |
| CSCsj90875       | Inline/Batch query: result mismatch on Matched Rule Ranking              |
| CSCsj90505       | Inline/Batch query not match on NAT connection report                    |
| CSCsj89299       | MARS unable to discover ASA through ssh using DES                        |
| CSCsj87207       | GUI cannot show the full topology because of constant process crash      |
| CSCsj74155       | Cannot Retrive Raw Messages while sending PIX72,ASA72 and SNORT messages |
| CSCsj73189       | IOS and IPS certificates aren't deleted when the device is deleted       |
| CSCsj71119       | Loading devices from seed file didn't populate interface info            |
| 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                           |
| CSCsj63552       | PN log agent should check ACS config before allowing user to App name    |
| CSCsj57812       | Mars unable to parse CP R61 Hide NAT behind gateway config               |
| CSCsj57315       | Mars doesn't parse and store CP R61 User/Client/Session auth rules       |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsj51240       | Paging does not work for report right after adding it to a case.         |
| CSCsj51181       | Batch query submitted from a GC to LC is still in progress after two day |
| CSCsj42467       | LC not showing up on certificate page                                    |
| CSCsj41168       | Error when trying to accept new sensor certificate                       |
| CSCsj33614       | MARS SSH discovery of ASA fails if login banner is set                   |
| CSCsj31990       | pnparser: to avoid flooding log file                                     |
| CSCsj30328       | Hosts not loading when existing hosts slected.                           |
| CSCsj29441       | rpcclient2 abnormal uder 1050 windows devices env                        |
| CSCsj28376       | Box may not be able to reboot after recovery, under certain conditions   |
| CSCsj23845       | The Action filter doesn't work if it is 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       |
| CSCsi95074       | low-traffic bytes ranking report causes process_inlinerep_srv to restart |
| CSCsi93594       | Pnparser stops processing each time it tries to load the topology        |
| CSCsi93283       | Mismatch between query and report results for source port ranking.       |
| CSCsi91734       | Mismatch in results between query and report for All Matching Events     |
| CSCsi89837       | MARS does not recognize SNMP traps from IPS device                       |
| 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. |
| CSCsi65713       | Index needs to be removed for the pn_report_result table                 |
| CSCsi62384       | The performace test kills all the process during the weekend run         |
| CSCsi53831       | performace test causes all the process restarted                         |
| CSCsi52731       | mars reboots w/o asking for confirmation after user clicked cfg update   |
| CSCsi51999       | Edit SW based Application device need submit twice                       |
| CSCsi50058       | GC not merging the same reporting device from LCs                        |
| CSCsi50024       | IPS is not visible in Global Zone Hot Spor 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.                            |
| CSCsi32559       | Able to run a query when the limit is reached                            |
| CSCsi32553       | MARS Client CPU hits 95-100% during Real-Time (raw events) query         |
| CSCsi29398       | CS-Mars does mitigate to the proper endpoint                             |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsi23209       | Some unsupported nfs cause system errors on MARS.                        |
| CSCsi18757       | CS-MARS - Request to have the "ssldump" command in the MARS CLI.         |
| CSCsi17607       | GC - Zone Model for Auriga 210 showing as 200                            |
| CSCsi15769       | NLS_LANG variable should be updated in environment                       |
| CSCsi13100       | gui.sh dev build makes different JBOSS web.xml than make release         |
| CSCsi11963       | MARS 4.2.4 not parsing IOS Router NAT properly                           |
| CSCsi11312       | pn_incident_log and pn_report_log should be archived                     |
| CSCsi09318       | Mars - Using IE7, any query over 2 mins to process result in error       |
| 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. |
| CSCsh94361       | Events with port 0 cannot be filtered using port in query/reports/rules  |
| CSCsh89445       | GUI allow users create rule without putting rule name                    |
| CSCsh82939       | MARS failed to restart if the hostname is changed after a restore        |
| CSCsh73553       | USB Keyboard does not work while re-imaging with DVD                     |
| CSCsh58754       | Lots of oracle files on HD can cause upgrade failure, succeeds on retry  |
| CSCsh57236       | Unknown Reporting Device was missing on GC's DB pn_device table          |
| CSCsh52537       | Repeated upgrades of oracle fills hard drive                             |
| CSCsh44351       | CSM multiple hostname matches failed to return multiple hosts            |
| CSCsh41920       | No warning for Invalid entry to Query maximum number of rows returned.   |
| CSCsh35953       | MARS unable to add similar named contexts from different fwsm            |
| CSCsh29243       | MARS Device Type label needs to reflect support for IOS 12.2 and later   |
| CSCsh14454       | server.log can grow unbounded with in a single day                       |
| CSCsh00013       | Case Management: history does indicate change of ownership               |
| CSCsg98026       | pnlogagent causes acs log files to add (01) to file name                 |
| CSCsg91816       | Query for ICMP port 0 shows UDP/TCP results                              |
| 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 |
| CSCsg75303       | GC: If chose LC specific device in rule, it doesn't pass to LC correctly |
| CSCsg74922       | MARS: License invalid after re-image from 3.4.3 to 4.2.2                 |
| CSCsg73786       | Devices should not be added to MARS if Discovery is unsuccessful         |
| CSCsg70386       | SSL uses key less than 1024                                              |
| CSCsg64119       | rule's keyword editor treats NOT as binary rather than unary             |
| CSCsg54313       | ORA-01654: unable to extend index on MARS 200                            |
| CSCsg47022       | CS-MARS - Incorrect Start Times on Retrieved Raw Message Files           |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsg38029       | high CPU usage in pnparsers due to checkpoint NAT rules                  |
| CSCsg26352       | Getting an internal server error when trying to access an incident on GC |
| CSCsg20987       | CSMARS DTM sdf files are sent with invalid format                        |
| CSCsg20408       | FW-6-SESS_AUDIT_TRAIL Parsing Error                                      |
| CSCsg14082       | Default query Changed in system defined report                           |
| CSCsg13767       | SuperV doesn't detect/restart processes                                  |
| CSCsg08166       | Unable to discover ASA 7.0 Error:There is no Error Log for this Device   |
| CSCsf99844       | wrong values for current connections using CLI "show resource usage"     |
| CSCsf99767       | provide encoding selection for adding agent to device/host               |
| CSCsf96634       | MARS cannot discover new route added to a router                         |
| CSCsf31228       | Unknown device events for FWSM 3.1 FWSM-3-717001 till FWSM-4-717031      |
| CSCsf31207       | Mars doesn't support new/changed FWSM 3.1.3 maintenance release syslogs  |
| CSCsf31121       | Exception in Case Management code when deleting a report                 |
| 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   |
| CSCsf06141       | high CPU usage in pnparsers sessionization                               |
| CSCsf06019       | Generic Router UI must support multiple reporting applications           |
| CSCse99039       | Redundant tab add available module under Device type Cisco IOS 12.2      |
| CSCse98029       | Occasionally corrupted event data enters into MARS database              |
| CSCse91636       | MARS - not all columns seen in CSV reports generated using custom column |
| 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                 |
| CSCse82017       | View HTML option for reports turns back to default report format - csv   |
| CSCse78738       | FWSM ifspeed incorrectly reported as 0 for per-context vlan interfaces   |
| CSCse78089       | Unable to upgrade CS-Mars via GUI                                        |
| CSCse54976       | Some incidents are not written to DB                                     |
| 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%                                |
| 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  |
| CSCse35758       | Inability to trace when first and last event occurred on a query         |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| 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                            |
| CSCse03237       | Changes made to GC network groups are not propagated to active LC rules  |
| CSCse03097       | CheckPoint LEA record comes to MARS later and later                      |
| CSCse00626       | IP Management -> device group displays hosts only.                       |
| CSCsd95582       | Both successful/failed mitigation reports show same results              |
| CSCsd92916       | CS MARS - Raw Ip Addresses in Custom Query email have incomplete URL     |
| CSCsd90181       | increasing pntorestore robustness                                        |
| CSCsd89457       | Incorrect handling of time range for rules that fire periodically.       |
| CSCsd86896       | Clicking the clear button when editing the query type doesn't work.      |
| CSCsd84350       | CS-MARS/CSM: Credentials change on CSM side not checked.                 |
| CSCsd74681       | OS 4.0: FlexLM License                                                   |
| CSCsd61749       | pntorestore doesn't restore all of the system config                     |
| CSCsd15695       | Summary dashboard showing incorrect statistics for false positives       |
| CSCsd13969       | resetting italics for GUI links                                          |
| CSCsd06302       | device name with single quote causes pink box                            |
| CSCsc97963       | Netscreen logical interfaces (vlan intf) not discovered                  |
| CSCsc95831       | log messages of MARS processes stopped being written into backend log    |
| CSCsc90480       | MARS Incident notification options are not configurable                  |
| CSCsc78878       | snort signature 2570 incorrectly mapped                                  |
| CSCsc59363       | Need improvement to GUI for multi-line rules                             |
| CSCsc42396       | CS-MARS Viewing IP of grouped sessions throws Exception, no Time var     |
| CSCsc15590       | MARS not including all events in a report, query returns events fine     |
| CSCsc04484       | LC Rule/Report list shows empty after deletion of GC group               |
| CSCsb80082       | Deleting a LC w/o exchanging 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     |

| Reference Number | Description                                                          |
|------------------|----------------------------------------------------------------------|
| CSCpn03052       | JBoss 'OutOfMemoryError' when accessing Management/Event Management  |
| CSCpn02976       | GC/LC - Communication issues after time zone change                  |
| CSCpn02973       | Not able to downgrade a security analyst to Notification only user   |
| CSCpn02968       | Network group search is not working for "All IP addresses            |
| CSCpn02901       | GC/LC, rule does not display user <cxu> but allows such cfg          |
| CSCpn02883       | Event management search works only for event description             |
| CSCpn02869       | Rules editing: changing entry for select window pulldown after error |
| CSCpn02804       | Replay History feature not working correctly                         |
| CSCpn02688       | GC/LC: gc lc displayed diff time rage for the same global report     |
| CSCpn02666       | Batch Query Results with one item returned -> no data in graph in em |
| CSCpn02656       | System error occurs when # of java connections runs out              |
| CSCpn02653       | 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          |
| CSCpn02011       | discovery for special passwd 1"1 failed                              |
| CSCpn01489       | BQ: Query summary doesn't mention "severity" if it's a criterion     |
| CSCpn01438       | Batch Query: Under high load, some batch queries may not complete    |
| 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                      |
| CSCpn01051       | Browser: Open non-supported browser to MARS causes other browsers to |
| CSCpn01045       | Archiving: Need better error message                                 |
| CSCpn00908       | "Domain" in Configuration page - no use                              |

| Reference Number | Description                                                     |
|------------------|-----------------------------------------------------------------|
| 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 |
| CSCpn00166       | Inconsistent behavior for "ANY" in Rules and Queries            |
| CSCpn00146       | Report names that differ by only slashes or dashes conflict     |

## Resolved Caveats - Release 4.3.1

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

| Reference Number | Description                                                             |
|------------------|-------------------------------------------------------------------------|
| CSCsk41641       | 5 nasl scripts' references need to be removed from bigfiles             |
| CSCsk37063       | LLV Query Resume button does nothing                                    |
| CSCsk35202       | unable to modify IP address                                             |
| CSCsk33730       | eth0 and eth1 not setup - after upgrade from 4.2.8 to 4.3.1.2585        |
| CSCsk12572       | Datawork merge from 4.2.8 to BOOTES(4.3.1)                              |
| CSCsk12317       | IPS signature status incorrect                                          |
| CSCsk12130       | Editing system rules before upgrading can cause LC/GC sync problems     |
| CSCsk02952       | High rate events/netflows with large topo can be dropped on an activate |
| CSCsj98279       | IPS Autoupdate CCO URL                                                  |
| CSCsj86127       | Merge issue with datawork in 4.3.1/5.3.1 branch                         |
| CSCsj83596       | Restore and migration for GC failed, one extra data field needed.       |
| CSCsj81545       | Netflow processing has an unnecessary STL call that uses 20% CPU        |
| CSCsj73189       | IOS and IPS certificates aren't deleted when the device is deleted      |
| CSCsj63436       | IPS Signature Download From CCO failed                                  |
| CSCsj55791       | ACS device type not showing up                                          |
| CSCsj55344       | Pink box on the Batch query page                                        |
| CSCsj54055       | GUI doesn't prompt for different/new CSM SSL cert                       |
| CSCsj53807       | Wrong results for event filter != 'ET group' in scheduled reports/LLV   |
| CSCsj52468       | Parsing not happening for Materialized events of Oracle 10g             |
| CSCsj51496       | Scheduled Report of Rpt Device Type Ranking generate empty result       |
| CSCsj47615       | Mars is unable to retrieve logs from CheckPoint NGX CLMs                |
| CSCsj46242       | System report "Spyware -Top Hosts" has wrong query                      |
| CSCsj46089       | parsing error for pix/asa 302003 , 302004                               |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsj45065       | linux events from syslog-ng are seen as generic event type on MARS       |
| CSCsj44151       | Need to remove replicated system data from the GC                        |
| CSCsj44134       | jboss stopped after mode 3 pnrestore                                     |
| CSCsj44116       | after mode 3 restore, user needs to re-type licens keys                  |
| CSCsj43393       | Getting "Unknown character = (35 #)" as first line while exec cmd in pn  |
| CSCsj42390       | enh: trim leading/trailing spaces in reported user, wksn, domain names   |
| CSCsj40715       | Report results could be delayed in synchronizing between LC and GC       |
| CSCsj39347       | pnrestore stopped because SQL Loader cannot continue                     |
| CSCsj39346       | pnrestore purged ES data in wrong partition when DB is full              |
| CSCsj38610       | CSMARS stopped receiving alarms after changing time on sensor            |
| CSCsj33016       | Timeout feature is not working as expected.                              |
| CSCsj29432       | need to purge inactivated report data                                    |
| CSCsj29192       | Dates lost in the duplicated report                                      |
| CSCsj23003       | Event Type Info contains invalid characters                              |
| CSCsj22964       | PnExport All Job Does not Stop All processes                             |
| CSCsj22950       | Deleted Report should be removed from the available reports list         |
| CSCsj22660       | GC: Pink box when compose a batch query with filter                      |
| CSCsj20953       | 'printsb' prints wrong shared buffer "jump counts                        |
| CSCsj19220       | Unable to download signature files when a proxy is configured            |
| CSCsj18798       | Trigger Packet not parsed correctly in ips 6.0 events                    |
| CSCsj18753       | MARS not parsing source ip, dest ip from 6.0 ips event                   |
| CSCsj18388       | Apostrophe character in IP Range/Network Name field causes MSIE to hang. |
| CSCsj16584       | GC: Notification user cannot be added                                    |
| CSCsj16089       | Event 103006 and 103007 of FWSM 3.1.5 not handled properly               |
| CSCsj15714       | Collect topology/configuration information in logs for debugging         |
| CSCsj15236       | Top Rule Fired report is missing in the Summary page.                    |
| CSCsj15204       | Pink box when the deleted report is re-add                               |
| CSCsj14215       | Unable to add ASA 7.0/ASA 7.0 in MARS with Version 4.3.1.2493            |
| CSCsj13655       | Pnparser doesn't use the new SNMP trap port changed in janus.conf        |
| CSCsj11768       | Add Info level logging for debugging topo synchronization                |
| CSCsj11759       | Some reports do not generate email alerts                                |
| CSCsj11689       | errors thrown when archive data to NFS share on a NetApp                 |
| CSCsj11201       | pnparser: avoid flooding log when errors occur in parsing SNMP traps     |
| CSCsj09479       | superV should cause processes to dump a backtrace before restarting them |
| CSCsj07565       | Increase shared buffer stall thresholds from 2 mins to 5 mins            |
| CSCsj07526       | The maximum size for an internal netflow queue is too large              |
| CSCsj07275       | Incorrect mapping of an attempted ftp login event                        |

| Reference Number | Description                                                             |
|------------------|-------------------------------------------------------------------------|
| CSCsj06461       | Web server log events do not update the received event count            |
| CSCsj02153       | cannot add nm-cids module to ios router                                 |
| CSCsj00904       | Cannot change versions on IPS devices                                   |
| CSCsi98818       | pn_agent.agent_subtype not getting set for IPS 5.x modules of ASA       |
| CSCsi98607       | if AAA server is not reachable, user accounts never lock up             |
| CSCsi98592       | Print netflow capacity drop event information in janus_log as well      |
| CSCsi95117       | changes needed in areas for introduce of report status=64               |
| CSCsi95086       | report deletion design changes                                          |
| CSCsi94282       | reports can have the same names with diffs on extra blank spaces        |
| CSCsi94202       | Upgrade doesn't update log_server or log_client                         |
| CSCsi91936       | remove index rebuild from upgrade                                       |
| CSCsi91755       | Admin Tab : Raw message retrieval performance improvements              |
| CSCsi91644       | Batch query for maximum rank return set to 100 shows 5000 results.      |
| CSCsi89028       | Support for FWSM 3.1.5                                                  |
| CSCsi86351       | superV falsely restarted pnparsner when timestamp file got removed      |
| CSCsi84817       | MARS 4.2.5 - not categorising Windows Security event ID 672 properly    |
| CSCsi82960       | Add Oracle RDA tool into system image                                   |
| CSCsi82387       | System Error after deleting NetG referenced by a Rule                   |
| CSCsi80781       | Priority field incorrectly updated for an existing event type           |
| CSCsi79438       | Percentages in Summary page often add to 99%, not 100%                  |
| CSCsi79327       | pnarchive disk low, migration could not finish for days                 |
| CSCsi79105       | export data job fails to finish                                         |
| CSCsi77859       | IDS3.1 needs to be removed from GUI                                     |
| CSCsi77753       | Improper grammer in error message                                       |
| CSCsi77558       | ET exists without DET                                                   |
| CSCsi77501       | Audit Log transactions for NetG change failing at LC                    |
| CSCsi75622       | Enh: LC dramatic perf improvement for false pos if many devices         |
| CSCsi74080       | correct the debug log levels for certain syslog relay related messages  |
| CSCsi73935       | Last Updated time updates every time                                    |
| CSCsi71511       | http status 500 appears while clicking the incident on the summary page |
| CSCsi71176       | When AAA is enabled, users can not change pndadmin email address        |
| CSCsi70352       | Sync LC will cause the GC IPs pushed back to the GC                     |
| CSCsi68698       | Reported User GUI notification for GC rule is broken                    |
| CSCsi68051       | GUI FTP upgrade fails due to incorrectly calling the CLI pnpupgrade cmd |
| CSCsi65736       | Getting error when clicked on Resume button                             |
| CSCsi65719       | Able to see networks which are not part of valid network                |
| CSCsi64918       | Oracle 10g support                                                      |

| Reference Number | Description                                                             |
|------------------|-------------------------------------------------------------------------|
| CSCsi64913       | Snort 2.6 Support                                                       |
| CSCsi64679       | Bootes: PIX7.2 8 syslogs have parsing error or unknown event            |
| CSCsi64605       | pnparser restarts frequently with sessionization turned on (default)    |
| CSCsi64138       | Upgrade/installation script needs to call post_cleanup.sql              |
| CSCsi64090       | parsing set wrong dest ports for some CheckPoint Generic Events         |
| CSCsi60690       | mars leaves open ips subscription after removing ips from gui           |
| CSCsi60547       | Long LC/GC disconnect leads to report sync problem                      |
| CSCsi60506       | deletion of host/ip addr/iprange/network/network grp will affect report |
| CSCsi60491       | delete devices will affect report if the report includes these devices  |
| CSCsi60217       | Sending report records and firing events from LC to GC is slow.         |
| CSCsi60206       | Should set protocol = tcp, dest port = 443 in GUI login event msg       |
| CSCsi59191       | too much IDS log flooding when doing performance testing                |
| CSCsi57369       | schema from_to scripts incorrect for autoupdate process                 |
| CSCsi57283       | pn_audit_log is not restored                                            |
| CSCsi54570       | tzdata update for Turkey, Mongolia, Cuba, Resolute, Nunavut             |
| CSCsi54469       | pnrestore does not check gen1/gen2 SW version                           |
| CSCsi54350       | mars restored archive data when start time is in the future             |
| CSCsi54173       | Signature package name is missing when download is failed               |
| CSCsi52622       | postfire lags behind due to doing large amount of NetBios name updating |
| CSCsi52495       | Always Prompt for SSL cert, Test Conn removes IPS' Monitored Nets       |
| CSCsi52093       | "confirmation" field in the shared secret field for RADIUS              |
| CSCsi52086       | the syslog for "pnadmin" login should show "Local authentication        |
| CSCsi51994       | One system rule has wrong description                                   |
| CSCsi50292       | Cannot add mars 20r to gc                                               |
| CSCsi49997       | Attack Diagram - Large Graph issue                                      |
| CSCsi48259       | GC allows to suspend a LC in "Not Responding " state                    |
| CSCsi47531       | IPS's "Test connectivity" doesn't discover the "Monitoring networks     |
| CSCsi45619       | Pink box when run NAC report on firing events                           |
| CSCsi45197       | CLI: exclude option not working properly                                |
| CSCsi42780       | GUI timeout feature is not working for the real time queries.           |
| CSCsi42488       | CF be archived daily regardless archiving is turned on or not           |
| CSCsi42066       | CLI: Inconsistent Output for syslogrelay list command .                 |
| CSCsi41173       | If error occurs sending config change to LC, no other config sent       |
| CSCsi39575       | Extra word should not be shown from the GUI                             |
| CSCsi39264       | Cannot Configure an IDSM Module to PULL IPS logs                        |
| CSCsi35209       | Cannot Add IPS 5.x/6.x as a ASA module                                  |
| CSCsi33474       | documentation incorrectly says user rules can be deleted                |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsi32777       | Configuring many events in drop rule can cause pink box error            |
| CSCsi31867       | csips crashes due to memory corruption                                   |
| CSCsi31569       | csips process restarts very frequently                                   |
| CSCsi31277       | autoupdate process stopped on GC                                         |
| CSCsi30271       | system rule needs updating for new internal events due to syslog relay   |
| CSCsi30169       | GUI still asks password even GC has authentication set to AAA            |
| CSCsi30168       | BOOTES: Add AAA support on MARS                                          |
| CSCsi30110       | Exception happened when clicking details ... button                      |
| CSCsi29930       | GUI: remove feedback in the GUI bottom                                   |
| CSCsi29451       | Different Version of LC-GC should be compatible                          |
| CSCsi28286       | GC-LC upgrade to 4.2.4 resulted in Standalone display on LC              |
| CSCsi27957       | LC generats Software versions syslog even when GC-LC have same version   |
| CSCsi27939       | Post-Bootes Upgrade script error reporting                               |
| CSCsi27891       | 'hostname' command should update workstation in mars reported users      |
| CSCsi26753       | "Path/Mitigation" should be "N/A" for internal syslog msg                |
| CSCsi24098       | AAA auth user account locked message is inconsistent                     |
| CSCsi24077       | Event "password remains default" is generated with wrong event type      |
| CSCsi24013       | ADMIN > Custom Setup > User Defined ... does not set subtab              |
| CSCsi23326       | Merge changes from 004.002(005) FCS build to the Bootes branch           |
| CSCsi22877       | wrong message is generated while doing non admin user unlock from GUI    |
| CSCsi22689       | wrong message is generated while CS_MARS failed to connect to AAA server |
| CSCsi22662       | wrong message is generated while unlocking admin user from CLI           |
| CSCsi21278       | GC/LC does not time out with 15 minutes and 30 minutes setting           |
| CSCsi19423       | Bootes: Change Version doesn't work for ASA7.0/7.2                       |
| CSCsi19322       | In AAA mode, password entry should be hidid when new user added in GC    |
| CSCsi19319       | pnadmin's oracle setting incorrect                                       |
| CSCsi19317       | Bootes: sessionization for dynamic nat in ASA7.2 failed                  |
| CSCsi19227       | Some reports/rules/queries match events outside specified IP ranges      |
| CSCsi17782       | Some OS/application setting not archived.                                |
| CSCsi15258       | Accepting the collector, and source ip address as MARS ip address        |
| CSCsi15246       | Accespting the MARS IP address, 10.1.1.255 and loopback address as sourc |
| CSCsi15167       | Accespting the MARS IP address and loopback address as source IP address |
| CSCsi14586       | Mars generated syslogs with mars as source IP do not trigger incidents   |
| CSCsi14027       | Oracle process not shutdown properly on a reboot                         |
| CSCsi13353       | Timezone Indiana-Pulaski County shows up as GMT in GUI                   |
| CSCsi13128       | Timestamp wrong for syslog MARS-2-350052                                 |
| CSCsi12240       | Pink box on Summary page of GC when cases are active                     |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsi11225       | pn_report_group2report is not included in cf archive (and should be)     |
| CSCsi11020       | pnrestore took more than 2 hours to restore one report result archive    |
| CSCsi10795       | MARS didn't pull syslog from generic window                              |
| CSCsi10692       | FWSM2.3: protocol is missing for FWSM-6-106025                           |
| CSCsi08897       | CS-MARS - CLI may display incorrect timezone after 03/11/07 DST change.  |
| CSCsi08151       | Incidents should not be pushed to GC when LC/GC has incompatible version |
| CSCsi08144       | No syslog generated when network cable is unplugged from GC              |
| CSCsi07719       | pnlog packaging should be more error resilient during 'pnlog mailto      |
| CSCsi07641       | Allow cloning of reports to allow more rapid report creation             |
| CSCsi07236       | connectivity test failed even microsoft IAS configuration is correct     |
| CSCsi07175       | Erroneous install/deployment gets wrong error messages                   |
| CSCsi07165       | Login failure window has misleading link name                            |
| CSCsi06257       | timeout feature does not work properly while it sets to be 30 & 60       |
| CSCsi06130       | GUI timed out too quickly in query page                                  |
| CSCsi04404       | auto-update required during data import process                          |
| CSCsi04306       | need to add CPU check for csips, csiosips, and cswin                     |
| CSCsi03807       | Make DB Changes for IPS Signature Autoupdate                             |
| CSCsi03686       | CS-MARS - HTML/XML tags are not escaped when displaying packet context   |
| CSCsi02718       | Checkpoint module removal triggered AAA                                  |
| CSCsi02638       | Need to implement deleteCmd in DBAPI class DbEventType2App.java          |
| CSCsi00963       | CS-MARS Archiving Causes pidof[xxxxxx] Messages to Appear on Monitor     |
| CSCsi00683       | CSA Administrative events not parsed by CS-MARS                          |
| CSCsi00493       | Implement IPS Dynamic signature support                                  |
| CSCsh99201       | MARS-Scheduled ranking report with ACTION filter produces empty results  |
| CSCsh95942       | data migration from Gen1 to Gen2                                         |
| CSCsh95924       | PIX/ASA 7.2 support in MARS                                              |
| CSCsh95836       | Add utility SQL scripts to installation for customer support             |
| CSCsh93759       | Rules/reports with large queries not working                             |
| CSCsh93364       | Creating a Case gets (harmless) ClassNotFoundException in JBOSS log      |
| CSCsh93354       | BOOTES: compiler optimization for pix 7.2 parser used up memory, stopped |
| CSCsh89885       | Mitigation command not display properly in 4.2.4                         |
| CSCsh88897       | race condition in pnparser triage handling caused syslog processing stop |
| CSCsh88639       | Add DB utility methods (log, long running query stats...)                |
| CSCsh85870       | Admin->Maintenance->Retreive Raw Message causes out of memory error      |
| CSCsh83470       | DB function to convert unix time to readable string for convenience      |
| CSCsh83184       | Device added as an Enterasys Dragon 6 does not show in Full Topology map |
| CSCsh83068       | Report and query return no results under device type ANY                 |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsh82764       | GC: Device-related Interface data left in DB after LC deleted            |
| CSCsh80210       | Generate locking and unlocking events.                                   |
| CSCsh78668       | Extra ';' following '>' in keyword query result                          |
| CSCsh78439       | Gc to LC: edited user rule not in rule group when passed to LC           |
| CSCsh77508       | MARS is not displaying CSM icon for access-list syslog with severity 0   |
| CSCsh77146       | Do not delete LC certificate from the GC when the zone is deleted        |
| CSCsh75216       | InLine multiColumn query case attachment Fails                           |
| CSCsh72929       | OutOfMemoryError/Bad performance in RULES/QUERY- large configuration     |
| CSCsh71637       | re-add a deleted CSA console may cause the submit page hang              |
| CSCsh69765       | CLI date/time/ntp commands should reboot if time change exceeds 30 mins  |
| CSCsh68717       | GUI Should change: Cisco ACS --> Cisco Secure ACS                        |
| CSCsh68503       | ISS SNMP trap: need to parse another format for ICMP type/code fields    |
| CSCsh68397       | pnstatus hostname mismatch says protego networks should say Cisco        |
| CSCsh68374       | Need to update Oracle shared_pool_size to match recommended settings     |
| CSCsh67287       | t_semaphore class not thread safe                                        |
| CSCsh60413       | LC pulls data very slow when encountering DbException                    |
| CSCsh60184       | 4.3.1 and 5.3.1 should include the update /usr/bin/tzselect script       |
| CSCsh59873       | Copyright in GUI is inconsistent in format - 2 lines to fix              |
| CSCsh58561       | ADMIN > System Parameters pages have easy-to-fix heading problems        |
| CSCsh58518       | Many ADMIN sub-windows have easy-to-fix vertical alignment issue         |
| CSCsh57236       | Unknown Reporting Device was missing on GC's DB pn_device table          |
| CSCsh56931       | Rule engine fires only once if only SAME is present in any column        |
| CSCsh56499       | Mars should learn FWSM dynamic nat from syslog for sessionization        |
| CSCsh56259       | pnarchive - CF production blocked, failing silently                      |
| CSCsh55172       | GC: Networks changed while LC deleted not correct after LC re-added      |
| CSCsh54239       | GC/LC pull and push servlets call CheckBoxInfo to check license every 30 |
| CSCsh52614       | Scheduler process creates extra audit log records for login              |
| CSCsh52443       | Invalid syslog message generated while upgrading through GUI             |
| CSCsh51271       | GC is unable to update LC's device name under admin/LC management        |
| CSCsh50446       | parsing error for PIX-6-113015                                           |
| CSCsh49009       | Duplicated GC and LC networks not displayed in fixed order on the LC     |
| CSCsh48988       | IP groups not displayed in order                                         |
| CSCsh47461       | 'Details' button does not return                                         |
| CSCsh46958       | pnparser does not clean up Oracle device map when it receives db Change  |
| CSCsh46868       | Custom column query not returning data                                   |
| CSCsh46448       | Agent list of a device not displayed in order                            |
| CSCsh46445       | The device type list of a device not displayed in order                  |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsh46428       | Available hosts list not display in order when adding agents to CSA      |
| CSCsh46424       | User group list not displayed in order                                   |
| CSCsh46417       | User list not displayed in order on LC                                   |
| CSCsh46401       | Service groups not displayed in order                                    |
| CSCsh46387       | Device Event IDs not displayed in order                                  |
| CSCsh46183       | GC - Should put up error when select details for "Non Responding" LC     |
| CSCsh45922       | archive/restore - ranged restore fails to fully preserve identity        |
| CSCsh45675       | Pink box on GC device page                                               |
| CSCsh45564       | PIX/ASA 7.2 messages 415001 to 415020 needs rewriting for parsing code   |
| CSCsh44548       | GC does not appear to update LC status                                   |
| CSCsh44179       | Connection Errors cause inability to select zone in incident/rule edit   |
| CSCsh43998       | system ctx for PIX/ASA 7.0 discovered as vesion 7.2                      |
| CSCsh43845       | IP management GUI: User can add VA Service to a host                     |
| CSCsh42151       | GUI Summary pg shows #events < #sessions & negative data reduction rate  |
| CSCsh41594       | LC is not moved from the GC after it is deleted                          |
| CSCsh40743       | pink box when doing real time query and click access rule icon           |
| CSCsh40698       | VPN GroupName and Username disappeared from its raw event message        |
| CSCsh40475       | Custom GC Error display when comm to LC fails - DISA requested feature   |
| CSCsh39200       | MARS charts only display the data for few days                           |
| CSCsh38818       | GC-LC upgrade 4.2.2->4.2.3 results in inverted online-offline status     |
| CSCsh38491       | Duplicate entries in 5-bigFile.txt                                       |
| CSCsh36021       | Need to distinguish between CSA versions on GUI                          |
| CSCsh35130       | Cancel edit removes Enterasys/NS IDP Server and sensors from device list |
| CSCsh34170       | Change/Modify report needs to purge existing reports                     |
| CSCsh32558       | custom column query: for acs event log, reported user is missing         |
| CSCsh31253       | Rules can't be edited after upgrade from 4.1.5 to 4.2.3                  |
| CSCsh27882       | Database Client: Debug Logging leads to incomplete scheduled discovery   |
| CSCsh27853       | Report results for a 10 minute window is dropped on an 'activate         |
| CSCsh23983       | DbExportFile not working                                                 |
| CSCsh22871       | User can create a device named ANY                                       |
| CSCsh20815       | In GUI new SSL/SSH Settings window has wrong sub-tab highlighted         |
| CSCsh20677       | Qualys: Discovery failed syslog from C++ backend needs to be suppressed  |
| CSCsh20219       | Confirmed user false positive query error java.lang.NullPointerException |
| CSCsh19644       | Get browser error when select to add a new host                          |
| CSCsh18265       | null drop rule causes parse error in the GUI                             |
| CSCsh14075       | scheduler-service.xml.contrib present in deploy directory                |
| CSCsh14070       | CS-Mars - Microsoft Misspelled in VA section                             |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsh13261       | syslog related to upgrade through GUI sends invalid syslog messg         |
| CSCsh13253       | syslog related to upgrade server missing                                 |
| CSCsh11027       | clicking 'next' button for IOS hangs up on GC                            |
| CSCsh11012       | Security issue with devices and logging                                  |
| CSCsh06027       | CS-MARS - DataBase file retrieval hyperlink uses wrong timestamp         |
| CSCsh02908       | The order of backend processes change randomly when setting log level    |
| CSCsh02885       | Cannot set GUI logging level to Trace                                    |
| CSCsh02501       | Query page text boxes should truncate input                              |
| CSCsh01636       | JDBC update to ojdbc14.jar                                               |
| CSCsh01620       | The javaDbTool did not handle NULL value dump correctly.                 |
| CSCsh00199       | Cannot add service/application to a host's vulnerability accessment info |
| CSCsg99611       | CS-MARS - Radio buttons are confusing on Retrieve Raw Messages page      |
| CSCsg98826       | LC interfaces are missed in the All IP Address list on GC                |
| CSCsg98822       | A device on GC( pushed from LC) is not deleted even after deleting LC    |
| CSCsg98622       | Incidents ready to fire are discarded on clicking 'Activate              |
| CSCsg98574       | pnsuperv not working properly                                            |
| CSCsg94880       | GC Pink box when doing keyword search on GC                              |
| CSCsg93242       | Allow customization to 15-minute session timeout setting                 |
| CSCsg93235       | zone_id of Unknown Reporting Device on GC is not correct                 |
| CSCsg91976       | Need to update Cisco logo and copyright year                             |
| CSCsg89582       | Multiple Agents ( ISS RealSecure 6.5 and Cisco CSA )on same host fails   |
| CSCsg88644       | recent connection in ui report is much higher than snmpwalk value        |
| CSCsg87864       | Recent average percentage for memory just is only half of actual value   |
| CSCsg86481       | CS-MARS parsing error for ASA7.0 msg 302018                              |
| CSCsg86370       | FR: MARS should support CSA 5.x                                          |
| CSCsg83055       | parsing error for FWSM-n-302003 and FWSM-n-302004                        |
| CSCsg80661       | memory percentage is over 100% in UI report                              |
| CSCsg77577       | incorrect resource utilization for concurrent conn                       |
| CSCsg77339       | auriga-2: Windows pull not work on build 2359                            |
| CSCsg76793       | Suspended LC still communicates with GC                                  |
| CSCsg73843       | GC - Unable to change configuration information (email IP) from GUI      |
| CSCsg73590       | Changing status of user confirmed positive type incident yeilds pink box |
| CSCsg71475       | Submitting Unconf. FP Firing Event only query generates system error.    |
| CSCsg69859       | SNMP Layer 2 Discovery Error, when community string has been corrected.  |
| CSCsg67502       | Incident->False Positive note is grammatically incorrect                 |
| CSCsg66801       | Activity: All Events and NetFlow report chart is missing on summary page |
| CSCsg66099       | Devices from deleted LC should be removed from the GC                    |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsg64986       | Custom column query - got pink box if chose a rule as a filter           |
| CSCsg64951       | Certain ASA 7.0 syslogs do not get parsed by MARS                        |
| CSCsg64704       | DNS wasn't configured correctly, Pausing event processing for 40 seconds |
| CSCsg64254       | Add SiteProtector support in MARS                                        |
| CSCsg64243       | GC - Path Link to inactive LC in incident displays error                 |
| CSCsg64135       | 5000Line_InlineQueryAsBatchEventSessionNon5K returns <or> than defined   |
| CSCsg61262       | no page title for adding intruvert sensor                                |
| CSCsg60114       | System error when generating NAC report                                  |
| CSCsg59538       | GC and LC Summary Pages - Data Reduction shows negative percentage       |
| CSCsg54313       | ORA-01654: unable to extend index on MARS 200                            |
| CSCsg53084       | MARS - WebVPN ACL Parse error event fires on incorrect syslog            |
| CSCsg50811       | DTM Notification allows user to add without recipient                    |
| CSCsg49567       | Admin/Retrieve Rawmsg: some events appear twice                          |
| CSCsg44725       | need to downgrade log level of CSA snmp trap errors in backend log       |
| CSCsg44578       | need to add CheckPoint NGX R61 support in MARS BOOTES release            |
| CSCsg44273       | Native syslog relay support in BOOTES release                            |
| CSCsg42639       | Single quote in variables or host name text box causes browser to hang   |
| CSCsg41549       | MARS discovery issues with Loopback IP on IP Unnumbered interfaces.      |
| CSCsg41027       | MARS - Retrieve Raw Messages Fails at 0%                                 |
| CSCsg39552       | Certain FWSM 2.3 syslogs give parsing errors/unknown event type in 4.2.2 |
| CSCsg37886       | error log exception when user_id is 201 (with Case Management)           |
| CSCsg35110       | Entering a zone name with a / gives errors when importing the ssl cert   |
| CSCsg33636       | PIX/ASA version above 7.0 need to be treated the same way                |
| CSCsg30013       | windows pull watchdog sometimes restarts all MARS proc                   |
| CSCsg26225       | Graphs/Images do not show up in case related report emails               |
| CSCsg25306       | CS-MARS should support EMBLEM format of syslog                           |
| CSCsg23483       | device_monitor does not load device utilization history on startup       |
| CSCsg20514       | Mars backend processes need to save backtraces on a crash for debugging  |
| CSCsg16843       | MARS reporting misleading licensing problem while trying to add a LC.    |
| CSCsg12475       | pnarchiver crashed because of extra files under /pnarchvie/CF directory  |
| CSCsg10787       | CatOS telnet discovery failing.                                          |
| CSCsg05143       | Button functions on zone config page should be restricted                |
| CSCsg04079       | Lotus Notes client gets JavaScript error with emailed MARS report        |
| CSCsg03167       | 8 unknown event type CatOS events                                        |
| CSCsg02749       | custom column report generates empty results                             |
| CSCsf30116       | Event Rate on the Top Destination Port graph is not correct              |
| CSCsf27617       | pnparser enhancement - custom parser to expand three more user fields    |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsf18686       | 4.3.1 branch ES/RM file numbers don't match                              |
| CSCsf18192       | Slow rendering of the GC/LC Summary page                                 |
| CSCsf18175       | CS-Mars-4.2.x LC online user guide bad hyperlinks to 4.1.x LC user guide |
| CSCsf18147       | CS-Mars-4.2.x LC online user guide bad hyperlinks to 4.2.x GC user guide |
| CSCsf11222       | Sort encoding values in the Encoding dropdown                            |
| CSCsf11055       | CC: GUI and CLI allow different password lengths - should be same        |
| CSCsf06819       | vulnerabilities not updated for hosts reported by deleted eEye console   |
| CSCsf02072       | GC-LC communication abnormal after running long time                     |
| CSCse98046       | need to improve db partition rotation strategy                           |
| CSCse95493       | Hard Drive Notification Sender Address Uses protegonetworks.com          |
| CSCse95048       | dragon device not retrieved by pnparsr                                   |
| CSCse94284       | User created reports do not work                                         |
| CSCse91029       | MARS 4.3: Devices created from GUI are not retrieved to pnparsr          |
| CSCse89538       | 4.3 merge: pnids40_srv, pnids50_srv and pniosips_srv are not copied      |
| CSCse88764       | can't access a ftp server with a user ID/password including @            |
| CSCse86087       | csmars4.3 - Failed adding LC to GC                                       |
| CSCse85953       | pnarchive doesn't archive the /etc/motd file                             |
| CSCse85884       | PNDB creation scripts not fit in new schema                              |
| CSCse85564       | Cannot add devices to a report which has more than 35 devices.           |
| CSCse84962       | eEye: MARS does not remove resolved vulnerabilities from host info       |
| CSCse84945       | eEye: imported vulnerabilities that are unknown should be flagged        |
| CSCse84746       | in mars4.3 data delayed 20 min when written data from sharedbuffer to DB |
| CSCse73868       | pnrestore command should support end-time argument in the command line   |
| CSCse73788       | MARS rediscovers Juniper Netscreen firewalls with wrong OS               |
| CSCse68056       | Can't chage the GUI logging Level to trace                               |
| CSCse66656       | create utility to change an LC to standalone mode                        |
| CSCse60240       | CS-Mars - report for old events include real-time events                 |
| CSCse57955       | CS-Mars showing unknown parsing error for Netscreen 5.0 events           |
| CSCse56632       | Browser hangs if a device is added with more than 50 monitored networks  |
| CSCse56430       | Enhancement: Save release binaries with debug symbols for debuggability  |
| CSCse55186       | remove 'stitch' code handling multiple PnEvent blocks in IPS/IDS code    |
| CSCse53870       | Change Protego OS string to reflect Cisco                                |
| CSCse53856       | Got "Error on page" when displaying packet data from IDS device          |
| CSCse52782       | Can't change run-time to day in "Resource Issues: Server - Top Reporting |
| CSCse52761       | The sender of disk failure notification email is <protego-support>       |
| CSCse49863       | the default user is not pndadmin when deleting a case owner              |
| CSCse47519       | Traffic Event is not parsing for Netscreen FW4.0 & 5.0                   |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCse47244       | cpu utilization value greater then 100% on a single CPU ios router       |
| CSCse46299       | Entercept Events will be unknown device event type when host OS=solaris  |
| CSCse45018       | MARS is unable to parse NetScreen 5.x syslogs                            |
| CSCse44601       | java.lang.NumberFormatException : User Management screen                 |
| CSCse44345       | readWebLogThread in pnparser spins if servlet socket disconnects         |
| CSCse40904       | Save As report button not enabled.                                       |
| CSCse39426       | frequent superV & pnparser restarts cause log processing to fail         |
| CSCse38615       | Bucket_size field in pn_report_result table is negative                  |
| CSCse35420       | Interface error rate should be separate from discards and unknown protos |
| CSCse34216       | CPU utilization report numbers on UI doesn't match the SNMP query        |
| CSCse32591       | dealing with duplicate hostnames in VA import                            |
| CSCse26964       | CatOS Syslog %SYS-4-P2_WARN not parsed correctly by MARS                 |
| CSCse24391       | parsing error for PIX, ASA: PIX-6-607001                                 |
| CSCse23191       | Disable 'No Pager' cmd sent by MARS to PIX, ASA, FWSM firewalls          |
| CSCse23176       | MARS Global Controller not producing alerts when losing LC communication |
| CSCse23051       | viewing report of query type of MAC addresses report got pink box        |
| CSCse22838       | can't find priority for CSA NT-Event-Log events                          |
| CSCse22824       | CS-Mars - device_monitor: change resource not found log level to debug   |
| CSCse21626       | Clicking activate is not taking effect                                   |
| CSCse20684       | CSM: Test connectivity View Error message "Not Found                     |
| CSCse20290       | Ciscoization - system os load screen still shows "Protego OS             |
| CSCse20285       | Ciscoization - system cli banner still show "Protego MARS                |
| CSCse19198       | Device Cnf: Changes in Mail Gateway IP doesn't reflect Report/ Notif     |
| CSCse18240       | DOC: cs-mars doesn't handle vpn paths                                    |
| CSCse16058       | CS-Mars Inactivate a system rule from GC cannot be displayed correctly   |
| CSCse12512       | Missing CSM policy query icon for events with destIP 255.255.255.255     |
| CSCse11258       | After group is deleted, items under "All" group not shown                |
| CSCse07425       | JVM is using up to 1.5 GB on a GC or LC                                  |
| CSCse03134       | More control is needed over retrieve raw messages and cleanup            |
| CSCse01877       | It takes more than 2 minutes to open ip management (network) page        |
| CSCse00417       | Incorrect name for system report 'Attacks: All - Top Rules Fired         |
| CSCsd95535       | Sentence for suggested mitigation cmd is incorrect (extreme)             |
| CSCsd94152       | It takes more than 5 minutes to open the schedule discover page          |
| CSCsd92922       | deleteing item in sources available list got pink box                    |
| CSCsd92285       | Security Dev Edit page does not check for existing IP address conflict   |
| CSCsd88284       | optimizing incident inserts in DbIncidentLoaderSrv                       |
| CSCsd84094       | using rules in query/report definitions                                  |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsd74283       | changing report-result retention limit                                   |
| CSCsd73486       | Mars: Not able to recognize the event type for ISAKMP and IPSec messages |
| CSCsd69137       | Default Group in Scheduler need to be made to Run On Demand              |
| CSCsd69063       | Reported User with single-quote (') causes oracle error                  |
| CSCsd64438       | pnparser crashed at 2.5k/s for relayed syslog and stops receiving events |
| CSCsd56311       | MARS sslcert keytool error: java.io.IOException: Incorrect AVA format    |
| CSCsd53173       | Retrieve raw messages doesn't properly update the progress percentage    |
| CSCsd48544       | port 8444 required for GC/LC communication                               |
| CSCsd48097       | Event processing may stop if pnparser creates shared buffers first       |
| CSCsd45441       | unknown reporting IP: 127.0.0.1 from checkpoint                          |
| CSCsd37005       | user must be able to change own password                                 |
| CSCsd28382       | error in data work for event type 6000512 : "Virus - Possible pif Worm   |
| CSCsd22832       | Attempt to remove IP subnet from IP Management fails, with error         |
| CSCsd20196       | User and System Scheduled Reports fail to display data                   |
| CSCsd14107       | SMS alert documentation specifies improper field format.                 |
| CSCsd06811       | DOC - LC 4.1 Figure 16-20 incorrect                                      |
| CSCsd04931       | Archiving shows some error logs in the janus_log file                    |
| CSCsc91572       | Multiple target ports in IDS event show up as 'port 0' in query          |
| CSCsc87501       | if set IP address to 0.0.0.0 box trying to reboot                        |
| CSCsc73832       | Drop rule inactive for events received by netflow in CS-MARS             |
| CSCsc70982       | change the button string on the false/positive column to "Tune           |
| CSCsc70832       | SNMP Device Discovery should identify ASA device                         |
| CSCsc66267       | Oracle User name in the reported user field of MARS                      |
| CSCsc58485       | 5 tuple information missing from downloaded raw log file                 |
| CSCsc47210       | inline process srv could crash                                           |
| CSCsc38389       | Bookmarks in Mars 4.1.1 Local User Guide don't show chapter names.       |
| CSCsc32363       | Documentation request GC LC communication troubleshooting                |
| CSCsc30107       | Cs-Mars - Queries with != in service column don't work                   |
| CSCsc27856       | FR - CS-Mars - multiple email addresses for email case button            |
| CSCsc26340       | 'occured' misspelled in MARS e-mail alerts                               |
| CSCsc24955       | ISS Site Protector central server log's are not supported by MARS        |
| CSCsc12091       | System Error When Clicking on Dynamic Info From False Positives Page     |
| CSCsc10453       | Show resolved host name in report if device was not found in system      |
| CSCsc07741       | If Viewing closed Case, then do refresh, get an email sent               |
| CSCsc07377       | Dynamic Info page on mitigation shows ip address as -1.-1.-1.-1          |
| CSCsc04637       | Closing a Case does not deselect it                                      |
| CSCsc02847       | Rule disappears from its group after edited in its Inactive status       |

| Reference Number | Description                                                              |
|------------------|--------------------------------------------------------------------------|
| CSCsc01793       | GUI logging levels is not changed correctly                              |
| CSCsb85297       | GC/LC Query with manual refresh can get pink box                         |
| CSCsb60747       | Ciscoization - GC zone models aren't Cisco-ized                          |
| CSCsb60283       | 'Matched Incident Ranking' result format shows as having 'real time' opt |
| CSCsb57624       | Unknown report device in Checkpoint log                                  |
| CSCsb55704       | LC Certificate Mis-placed in GC after a new LC added                     |
| CSCsb44374       | FWSM's access was not displayed on the security info page                |
| CSCsb43627       | Source IP address is not correct for a VPN3K event                       |
| CSCsb39208       | Unrecognized Traps from McAfee EPO                                       |
| CSCpn03077       | GC, sys error when adding a LC which was added to GC already             |
| CSCpn03053       | GUI log level setting is not working as expected                         |
| CSCpn03005       | Loading Resource Util report as On-Demand query produces a system error  |
| CSCpn02930       | Error message when adding non-existent LC to GC is incorrect             |
| CSCpn02892       | Licensing: Inputting valid LC license onto GC allows the user to run     |
| CSCpn02693       | 6MB mem leak in process_event_srv after each activate                    |
| CSCpn02590       | In summary page, data reduction shows 100% when it should be 0%          |
| CSCpn02511       | need to fix errors in affected os                                        |
| CSCpn01934       | Back button is missing in logging level/log/audit trail pages            |
| CSCpn01465       | Reports: have "View", "Add" etc. buttons at top of page                  |
| CSCpn01317       | More data expected when populating pn_application table                  |
| CSCpn01293       | Host OS listing needs cleaning                                           |
| CSCpn00887       | Summary: Inconsistent title bar naming convention for the Summary Pa     |
| CSCpn00845       | Editing service to become ICMP w/o ICMP code -> no change                |

## Resolved Caveats - Releases Prior to 4.3.1

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

[http://www.cisco.com/en/US/products/ps6241/prod\\_release\\_notes\\_list.html](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.