



CHAPTER 5

Upgrade Management

Revised: July 24, 2009, OL-16776-01

Because Cisco Security MARS and the products it monitors depend on signatures that are current, the upgrade strategy you employ is critical to the overall health and accuracy of the MARS system. You should develop an operational strategy and process for performing updates.

This chapter contains the following sections:

- [Upgrade Management Overview, page 5-1](#)
- [Checklist for Upgrades of Appliance Software, page 5-3](#)
- [Before You Begin, page 5-7](#)
- [Verify the MARS Appliance Version and State, page 5-8](#)
- [Specify Interval for Master Catalog Polling, page 5-10](#)
- [Select an Upgrade Package for a MARS Appliance \(local\), page 5-13](#)
- [Manage Local Upgrade Packages, page 5-14](#)
- [Upgrading a Local Controller from the Global Controller, page 5-16](#)
- [Burn an Upgrade CD-ROM, page 5-18](#)
- [Prepare the Internal Upgrade Server, page 5-19](#)
- [Upgrade from the CLI, page 5-22](#)

Upgrade Management Overview

Feature Modification History

Release	Modification
6.0.1	Feature introduced. Separates product package from data packages. Introduces automated image management, new image management interface, and updates pnupgrade command.

These features were introduced with the 6.0.1 release of MARS. To upgrade from an earlier release, see the appropriate document:

- **5.x Releases.** If you are running an earlier 5.x version, you must first upgrade to 5.3.6 (see the [Release Notes for Cisco Security MARS Appliance 5.3.6](#) for the required upgrade path.).
- **4.x Releases.** For details on how to migrate your appliance, follow the step-by-step instructions specified in the [Migrating Data from Cisco Security MARS 4.x to 6.0.1](#).

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

**Caution**

Never try to upgrade the hardware components of the MARS Appliance. Doing so could result in bodily injury and void support contracts. Contact Cisco for your hardware upgrade needs.

MARS supports three distinct upgrade package types:

- **Product package.** This package contains the system binaries, such as the OS and backend processes and services.
- **Data package.** This package contains signature updates, rules, reports, event types, and event type groups.
- **Combined product and data package.**

**Note**

In addition to the system binary and data package versions, MARS maintains separate version information for the Cisco IPS signatures and custom signature packages running on an appliance. The management of dynamic signature updates for Cisco IPS devices is managed from **ADMIN > System Setup > IPS Signature Dynamic Update Settings**. For details on this feature, see “[IPS Signature Dynamic Update Settings](#)” in the *Device Configuration Guide for Cisco Security MARS*.

The image management feature of MARS keeps your appliances current with the product and data packages whether running a standalone Local Controller or managing a set of Local Controllers with a Global Controller. This feature discovers updates when they are released by Cisco as “.zip” files that contain a “.pkg” file and a catalog file and allows you to schedule when to download the package and perform the upgrade operation.

Each “.pkg” file is an encrypted tarball that contains the upgrade binary, data files, or both depending on the package type. The catalog file describes:

- The version of the upgrade package
- The type of upgrade to be performed (binary, data, or both)
- Any and all version dependencies
- All of the above information for all upgrade packages in existence up to the release of the particular upgrade package

The MARS Appliance saves the catalog locally for reference, and it uses that file to ensure packages are applied in proper order. When a newer catalog is found, the MARS Appliance replaces the local catalog with the new one. A catalog update can occur during an upgrade or, if configured to do so, when the MARS Appliance polls Cisco.com, where the master catalog resides.

**Note**

A failed upgrade operation can potentially update the local catalog file when the upgrade contains a catalog file newer than the one saved on the MARS Appliance.

All upgrades must be performed sequentially. The data work version number is tracked separately from the binary version number. To determine the versions running on an appliance, see [Determine Version Information, page A-1](#).

To configure the upgrade management feature, you must configure the following:

1. [Verify the MARS Appliance Version and State](#)
2. Interval for downloading the master catalog. See [Specify Interval for Master Catalog Polling, page 5-10](#).
3. Identify the server from which upgrade packages should be downloaded and provide authentication credentials that enable the appliance to connect to that server. See [Specify Download Sever Settings, page 5-11](#).
4. Select and schedule the upgrade for each downloaded package. You can perform this task either local to a MARS Appliance or from a Global Controller. See [Select an Upgrade Package for a MARS Appliance \(local\), page 5-13](#) or [Schedule Package Download and Upgrades from a Global Controller, page 5-17](#).

Checklist for Upgrades of Appliance Software

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



Caution

Never try to upgrade the hardware components of the MARS Appliance. Doing so could result in bodily injury and void support contracts. Contact Cisco for your hardware upgrade needs.

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

✓	Task
	<p>1. Determine whether you should upgrade, reimage, or migrate the MARS Appliance.</p> <p>Two scenarios exist for bringing your MARS Appliance in line with the current software release: upgrade versus reimage. The method required to get to the current release can differ greatly between these two scenarios.</p> <ul style="list-style-type: none"> • (4.x Only) Migrate the MARS Appliance to the current release and preserve the configuration and event data. This process applies only to appliances running a 4.x release. For details on how to migrate your appliance, follow the step-by-step instructions specified in the Migrating Data from Cisco Security MARS 4.x to 6.0.1. • (5.x and 6.x Only) Upgrade the MARS Appliance to the current release and preserve the configuration and event data. To preserve the configuration and the event data, you must perform the upgrade following the tasks in this checklist; continue with Task 2. • (Any) Reimage the MARS Appliance to the current release without preserving any configuration or event data. If you have no desire to preserve configuration and event data, you can reimage the appliance using the most recent ISO image. For information on how to reimage your appliance, see Recovery Management, page 6-17. <p><i>Result:</i> You determine whether you will upgrade or reimage your MARS Appliance.</p>
☐	<p>2. Determine the version that you are running.</p> <p>Before you upgrade your appliance, you must determine what version you are running. You can determine this in one of two ways:</p> <ul style="list-style-type: none"> • web interface. To determine the version in the web interface, select Help > About. • CLI. To determine the version from the CLI, enter version at the MARS command prompt. <p>The format of the version appears as <code>x.y.z (build_number)</code>, for example, <code>6.0.2 (3102)</code>.</p> <p>Note If you are running a version earlier than 3.2.2, please contact Cisco support for information on obtaining the appropriate upgrade files. If you are running 3.2.2 or later, follow the instructions in this checklist.</p> <p><i>Result:</i> You have identified the version running on your appliance and know whether you must contact Cisco support or continue with this checklist.</p>
☐	<p>3. Verify the status of the MARS Appliance.</p> <p>Before upgrading, verify that the hardware and software services are operating in an expected state. If an issue is found, you want to address those issues prior to beginning the upgrade process. The following components are verified:</p> <ul style="list-style-type: none"> • fans, CPUs, hard drives, Ethernet interfaces, power supplies, flash drive, and backup battery units • MARS system services and processes • hard drive array, if running RAID <p><i>Result:</i> You determine whether the MARS Appliance is operating correctly.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> • Verify the MARS Appliance Version and State, page 5-8

✓	Task
☐	<p data-bbox="228 285 721 315">4. Determine the medium for upgrading.</p> <p data-bbox="269 327 1510 390">Before upgrading your appliance, you must determine what medium to use. Your choice of medium determines whether you must upgrade from the CLI.</p> <ul data-bbox="282 407 1510 779" style="list-style-type: none"> <li data-bbox="282 407 1510 499">• CD-ROM. Before you can upgrade, you must download the software and burn an image to a CD-ROM. You can insert this CD-ROM in the DVD drive of the MARS Appliance to perform the upgrade. If you select the CD-ROM medium, you must upgrade each appliance individually and you must use the CLI. <li data-bbox="282 516 1510 674">• Internal Upgrade Server. Identify the Internal Upgrade Server to be used. Before you can upgrade, you must download the software image to an internal HTTP, HTTPS, or FTP server. It is from this internal server that you must upgrade your MARS Appliance. This server should meet specific requirements, allowing each MARS Appliance to quickly and securely download the updates. When using an Internal Upgrade Server, you can upgrade from the CLI or the web interface unless otherwise noted. <li data-bbox="282 690 1510 779">• Cisco.com. Identify your CCO login credentials to import packages to either a Global Controller or Local Controller. You can upgrade all managed Local Controllers from the Global Controller. If you select Cisco.com, you must upgrade using the web interface. <p data-bbox="224 798 1510 890">Note If you are running a version earlier than 3.4.1, you cannot use the web interface to upgrade. In versions earlier than 3.4.1, the web interface only allows for connections to the upgrade.protegonetworks.com support site, which is no longer available. To upgrade from versions earlier the 3.4.1, you must use the CLI.</p> <p data-bbox="269 917 1510 1041"><i>Result:</i> You have determined which medium to use for your upgrade. If you chose the Internal Upgrade Server option, you have identified and prepared your server, and you have verified that the server can be reached by each standalone Local Controller or Global Controller that you intend to upgrade. If a proxy server resides between the Internal Upgrade Server and the appliance, you must provide those settings before upgrading.</p> <p data-bbox="269 1058 570 1087">For more information, see:</p> <ul data-bbox="282 1104 1208 1358" style="list-style-type: none"> <li data-bbox="282 1104 984 1134">• Download the Upgrade Package from Cisco.com, page 5-19 <li data-bbox="282 1150 748 1180">• Burn an Upgrade CD-ROM, page 5-18 <li data-bbox="282 1197 846 1226">• Prepare the Internal Upgrade Server, page 5-19 <li data-bbox="282 1243 813 1272">• Specify Download Sever Settings, page 5-11 <li data-bbox="282 1289 1089 1318">• Select an Upgrade Package for a MARS Appliance (local), page 5-13 <li data-bbox="282 1335 1208 1365">• Schedule Package Download and Upgrades from a Global Controller, page 5-17

✓	Task
☐	<p>5. Understand the required upgrade path and limitations.</p> <p>Upgrading from one version of the appliance software to the next must follow a cumulative upgrade path; you must apply each upgrade package in the order it was made available between the version running on the appliance and the version you want to run. Review the <i>Required Upgrade Path</i> section in the release notes for the target version.</p> <p>Also, a limitation exists between a Global Controller and any Local Controllers that it monitors. The Global Controller can only monitor Local Controllers that are running the same version it is. If you are attempting to monitor a Local Controller that is running an earlier software version, the Local Controller will appear offline to the Global Controller. However, MARS includes an upgrade option where the Global Controller pushes the same upgrade version to the Local Controllers that it is monitoring, allowing you to manage the upgrade process from within the Global Controller user interface.</p> <p>You have identified the complete list of upgrade packages that you must download.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> • Before You Begin, page 5-7 • Verify the MARS Appliance Version and State, page 5-8.
☐	<p>6. Download all required upgrade packages from the Cisco.com website.</p> <p>After you have identified the upgrade packages to download, either log in to Cisco.com using your Cisco.com account and download the various packages or configure your MARS Appliance to do so. To download upgrade packages, you must have a valid SMARTnet support contract for the MARS Appliance.</p> <p>Depending on your selection in Step 4., you will either store these files on the Internal Upgrade Server, burn a CD-ROM image, or allow the MARS Appliance to store them until they are applied.</p> <p><i>Result:</i> All upgrade packages that are required to upgrade from the version you are running to the most recent version are located in a known path on either the MARS Appliance, Internal Upgrade Server, or a CD-ROM.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> • Specify Download Sever Settings, page 5-11 • Manage Local Upgrade Packages, page 5-14. • Download the Upgrade Package from Cisco.com, page 5-19.
☐	<p>7. Understand the upgrade approach you want to use.</p> <p>Select from the following upgrade options:</p> <p>Note If you are running a version earlier than 3.4.1, you must select an option that supports upgrading from the CLI.</p> <ul style="list-style-type: none"> • Upgrade from an appliance that connects to Cisco.com directly (web interface only). • Upgrade from an appliance that connects to the Internal Upgrade Server directly (CLI or web interface). • Upgrade from an appliance that connects to the Internal Upgrade Server through a proxy (CLI or web interface). • Upgrade a Local Controller using the Global Controller via a proxy server or a direct connection to the Internal Upgrade Server or from Cisco.com (web interface only). • Upgrade from a CD-ROM at the command line (CLI only). <p><i>Result:</i> You have determined the appropriate upgrade approach to use based on your selected medium and currently running version.</p>

✓	Task
☐	<p>8. Identify any required proxy server settings.</p> <p>If your appliance runs on a network that is separated from the Internal Upgrade Server by a proxy server, you must identify the proxy server settings. If you are using the HTML interface to upgrade, you can specify these settings using the Admin > System Parameters > Proxy Settings page. Otherwise, make note of the settings so that you can include them in the command string of the command line interface upgrade.</p> <p>Note You can specify the proxy server settings in the web interface for versions 3.4.1 and later. However, you can specify proxy server settings at the CLI for versions 2.5.1 and later.</p> <p><i>Result:</i> You have either specified the proxy server settings in the web interface, or you have noted the settings for later use.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> • Specify the Proxy Settings for a MARS Appliance, page 5-20.
☐	<p>9. Upgrade the appliance to the next appropriate version, as determined by the upgrade path.</p> <p>From the appliance, use the method you chose in Step 7. to upgrade incrementally, as determined in Step 6., to the desired version.</p> <p><i>Result:</i> You have applied each required upgrade package.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> • Select an Upgrade Package for a MARS Appliance (local), page 5-13 • Upgrade from the CLI, page 5-22 • Upgrading a Local Controller from the Global Controller, page 5-16.

Before You Begin

The following notes apply to the 6.0.1 upgrade:

Upgrade to 6.0.1

The upgrade process to 6.0.1 differs based on the release you are upgrading from. If you are upgrading a 5.x release, then you can upgrade to 6.0.1 if you are running 5.3.6. If you are running an earlier 5.x version, you must first upgrade to 5.3.6 (see [Release Notes for Cisco Security MARS Appliance 5.3.6](#) for details).

However, if you are upgrading a 4.x release, you must migrate the system instead of upgrading. To migrate from a 4.x, you must follow the step-by-step instructions specified in the [Migrating Data from Cisco Security MARS 4.x to 6.0.1](#).

The following notes apply to all upgrades:

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.

Cisco recommends that you upgrade your system using the web interface. See [Upgrade Management Overview, page 5-1](#) for details on the recommended process.

Consistency Checks

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

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

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

Verify the MARS Appliance Version and State

To avoid data loss and other issues, verify the appliance software and hardware are operating correctly before attempting to upgrade the software. This procedure explains how to determine whether an issue exists with the appliance as configured.

Prerequisites

- Ensure the appliance is running 6.0.1 or later.

Restrictions

- The **raidstatus** command only applies to models: 100, 100e, 110, 110R, 200, 210, GC, GCr, GC2, and GC2R.

Summary Steps

10. **version**
1. **model**
2. **show healthinfo**
3. **pnstatus**
4. **raidstatus** (if applicable)

Verifying the MARS Appliance System Settings

To use the console to verify the system status the MARS Appliance, follow these steps:

-
- Step 1** Log in to the MARS Appliance. For more information, see [“Log In to the Appliance via the Console” section on page 4-1](#).
- Step 2** At the system prompt, type **version**, and then press **Enter**. Record the output and verify the version is 6.0.1 (3066) or later. If the version is not 6.0.1 (3066), you must upgrade or migrate your system to 6.0.1 (3066) and re-run this verification process.

**Note**

If you are upgrading a 5.x release, then you can upgrade to 6.0.1 if you are running 5.3.6. If you are running an earlier 5.x version, you must first upgrade to 5.3.6 (see the [Release Notes for Cisco Security MARS Appliance 5.3.6](#)).

However, if you are upgrading a 4.x release, you must migrate the system instead of upgrading. To migrate from a 4.x, you must follow the step-by-step instructions specified in the [Migrating Data from Cisco Security MARS 4.x to 6.0.1](#).

- Step 3** At the system prompt, type **model**, and then press **Enter**. Record the output.
- Step 4** At the system prompt, type **show healthinfo**. Verify the fans, CPUs, hard drives, Ethernet interfaces, power supplies, flash drive, and backup battery units are operating properly.
- Step 5** At the system prompt, type **pnstatus**, and then press **Enter**. Verify that all applications are running properly. If an application is in an incorrect state, wait 30 seconds and run the **pnstatus** command again. If the application is still in an improper state, make a note of it and continue to the next step.

**Note**

All services should be running on a Local Controller. However, a Global Controller only has three services running: graphgen, pnarchiver, and superV—all other services are stopped.

- Step 6** (100, 110, 200, 210, GC, GC2 only) At the system prompt, type **raidstatus**, and then press **Enter**. Verify the RAID is in the OK state, not DEGRADED.
- If the RAID appears in the DEGRADED state, refer to the “Hard Drive Troubleshooting and Replacement” sections of *Cisco Security MARS Hardware Installation Guide 6.x* to rebuild or reconfigure the RAID.
 - (Gen 2) http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/hardware/installation/guide/maintain_gen2.html
 - or
 - (Gen 1) http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/hardware/installation/guide/maintain_gen1.html
- See the hotswap command for details. Once the operation is complete, re-verify the system before attempting to perform the migration or upgrade.
- If the RAID configuration is in an INIT/INITIALIZING state, proceed with the system inspection.
- Step 7** If the show healthinfo, pnstatus, or raidstatus commands reveal issues, you must resolve them prior to upgrading the system. Otherwise, continue with the upgrade.

Related Documents

Related Topic	Document Title
Related MARS CLI commands: <ul style="list-style-type: none"> • model • version • show healthinfo • pnstatus • raidstatus • hotswap 	Cisco Security MARS Command Reference, 6.x.
Hardware Maintenance Tasks—MARS 25R, 25, 55, 110R, 110, 210, GC2R, and GC2	Cisco Security MARS Hardware Installation Guide 6.x.
Hardware Maintenance Tasks—Hardware Maintenance Tasks—MARS 100E, 100, 200, GCM, and GC	Cisco Security MARS Hardware Installation Guide 6.x.

Specify Interval for Master Catalog Polling

The master catalog is maintained on Cisco.com. Each time a new package is released, the master catalog is updated. If you've configured your MARS Appliance to check Cisco.com automatically, a notification will appear on the Network Summary page when an update is available for download.

To specify the interval to check for a new master catalog, follow these steps:

-
- Step 1** From the web interface of a MARS Appliance, select **ADMIN > System Maintenance > Upgrade**.
Result: The Upgrade Installation page appears with the Upgrade Zones tab selected.
- Step 2** To download the latest catalog file, select the **Advanced** tab.

Upgrade Installation

Upgrade Zones	Local Packages	Download Connection Information	Advanced
<p>Catalog Polling URL: <input type="text" value="https://www.cisco.com/cgi-bin/front.x/ida/d"/> The system periodically checks this location for a new package catalog.</p> <p>Package Polling Interval: <input type="text" value="NEVER"/> Indicates how often the Catalog polling URL is checked.</p> <p><input type="button" value="Save Changes"/></p>			
<div style="border: 1px solid black; padding: 5px;"> <p>NEVER</p> <p>Every 1 hour</p> <p>Every 2 hours</p> <p>Every 3 hours</p> <p>Every 6 hours</p> <p>Every 12 hours</p> <p>Every day</p> <p>Every 2 days</p> <p>Every 3 days</p> <p>Every 4 days</p> <p>Every 5 days</p> <p>Every 6 days</p> <p>Every 7 days</p> <p>Every 8 days</p> <p>Every 9 days</p> <p>Every 10 days</p> <p>Every 11 days</p> <p>Every 12 days</p> <p>Every 13 days</p> <p>Every 14 days</p> </div>			

Step 3 Select a value from the Package Polling Interval list, and click **Save Changes**.

Using the authentication information you provided on the Download Connection Information page, it checks to see if there is a new catalog. If a new one shows up, an indication displays on the **Network Summary** page. Then you can return to Download Connection Information page to get import the pages.

Specify Download Sever Settings

The download server settings identify the server from which the upgrade packages are to be downloaded. If you are using a Global Controller to manage Local Controller, you only need to specify these settings on the Global Controller. You can configure the Global Controller to push the upgrade package to each managed Local Controller.

If the MARS Appliance cannot directly access the download server (whether it is Cisco.com or an Internal Upgrade Server), you must specify the proxy settings for the appliance as defined in [Specify the Proxy Settings for a MARS Appliance, page 5-20](#).

To configure the upgrade options for a MARS Appliance, follow these steps:

- Step 1** From the web interface of a MARS Appliance, select **ADMIN > System Maintenance > Upgrade**.
Result: The Upgrade Installation pages appears with the Upgrade Zones tab selected.
- Step 2** To specify the download server settings, select the **Download Connection Information** tab.

Upgrade Installation

Upgrade Zones Local Packages Download Connection Information **Advanced**

Package Download Connection Information

Cisco.com Local Server

User Name:
 Password:
 Re-enter Password:

Server Type:
 IP Address:
 User Name:
 Password:
 Re-enter Password:
 Path:
 File Name:

Available Storage: 2000000000
 (Note: A fixed amount of storage space is available. If the limit is reached you must delete some packages to import new ones.)

Step 3 Specify the following settings:

- **Server location:**
 - Cisco.com—Downloads the upgrade packages from Cisco.com using your CCO user account information.
 - Local Server—Downloads upgrade packages from an Internal Upgrade Server.
- (local only) **Server Type**—Select the appropriate protocol. You can download the install package using either HTTPS or FTP.
- (local only) **IP Address**— Enter the address of the server where the upgrade package files are stored.
- **User Name**—Identifies the user credentials to use when downloading the upgrade packages. This detail is recorded in the audit logs when packages are downloaded.



Note MARS requires that the Internal Upgrade Server enforces user authentication. Therefore, you must specify a username and password pair to authenticate to the server.

- **Password**—Password assigned to the account specified.
- **Re-enter Password**—Confirms your password.
- (local only) **Path**—Specify the path where the package file is stored, relative to the type of server access used.
- (local only) **File Name**—Specify the full name of the package file that you have downloaded.

Step 4 Click **Save Changes**.

Step 5 Select a value from the Package Polling Interval list, and click **Save Changes**.

Select an Upgrade Package for a MARS Appliance (local)

Step 1 From the web interface of a MARS Appliance, select **ADMIN > System Maintenance > Upgrade**.

Result: The Upgrade Installation pages appears with the Upgrade Zones tab selected.

Upgrade Installation

Upgrade Zones | Local Packages | Download Connection Information | Advanced

Upgrade Status Logs

Upgrade Zones

This table lists the zones and the local packages that can be installed on them. To schedule a package for installation, check the zone(s) and select the package from the drop-down list, then click "Install"

	Zone Name	Zone Address	Status	Version	Install Package
<input type="checkbox"/>	pnmars/ITS-FW2	10.4.200.141	Active	6.0.1	<input type="text"/>

Install

Time	Log Message

Back

This page presents details about the current status of the appliance.

- **Zone Name**—Identifies the DNS name of the appliance. If you are viewing this page on a Global Controller, an entry for each managed Local Controller appears. If you are viewing this page on a Local Controller, only the entry for that appliance appears.
- **Zone Address**—Identifies the IP address of the appliance. If the word 'local' appears in this field, then it identifies the appliance you are logged into via the web interface.
- **Status**—Identifies the status of the appliance. The possible states depend on whether this appliance is being managed by a Global Controller or not. Possible status values are:
 - **GC**—Identifies the local appliance as a Global Controller. This status appears only when you are viewing this page on a Global Controller.
 - **Active**—The appliance is online and operational. If managed by a Global Controller, then this state indicates that the Local Controller-Global Controller communications are successful.
 - **Synchronizing**—The Local Controller is forwarding topology information to this Global Controller.
 - **Upgrade Scheduled**—An upgrade is scheduled for this appliance.
 - **No Connection**—The connection is down. This issue could be due to network interruption, invalid connectivity information, or an upgrade currently in progress
 - **Deleting In Progress**—The Local Controller is being deleted from this Global Controller.
- **Version**—Identifies the version of MARS software running on the appliance.

- **Install Package**—A list of upgrade packages stored locally to the selected appliance and for which the dependencies match the version currently running on the appliance. When a package is local to the appliance, you can schedule to install the upgrade. If you are working in a Global Controller, this list includes any applicable package downloaded to the Global Controller, which you can schedule to download and apply to valid Local Controller targets.
- **Upgrade Status Logs**—Normal status logs appear in green text, warnings appear orange, and errors appear red.

Step 2 Select the check box to the left of the Zone Name for this appliance.

Step 3 From the **Install Package** list box, select the upgrade package for which you want to schedule an install. This list identifies the upgrade packages downloaded onto the selected appliance.

Step 4 Click **Install**.

Result: The Package Installation page appears.

Step 5 Select the **Install Now** option, and then click **Submit**.

Result: After you click Install, the system needs some time to process the upgrade. The status of the upgrade appears in the **Upgrade Status Logs** box. After the upgrade is complete, the system reboots. During the upgrade, the user interface is also restarted.

Manage Local Upgrade Packages

When an upgrade package is downloaded to a MARS Appliance, you can review the details about that package, as well as import new packages or delete old packages to ensure there is adequate disk space on the MARS Appliance.

If an upgrade completes successfully on a Local Controller, the upgrade package is deleted. However, on a Global Controller the upgrade package is not deleted. After upgrading the Global Controller and all monitored Local Controller, navigate to the **Local Packages** page and manually delete any upgrade packages that are no longer needed.



Note

If a proxy server is between MARS and the Internal Upgrade Server, and proxy information is not configured on MARS, an attempt to download an upgrade package directly from the Internal Upgrade Server fails after a period of time. See [Specify the Proxy Settings for a MARS Appliance, page 5-20](#)

To manage the upgrade packages that are downloaded on a MARS Appliance, follow these steps:

Step 1 From the web interface of a MARS Appliance, select **ADMIN > System Maintenance > Upgrade**.

Result: The Upgrade Installation pages appears with the Upgrade Zones tab selected.

Step 2 To select an upgrade package to apply to this MARS Appliance, select the **Local Packages** tab.

Upgrade Zones	Local Packages	Download Connection Information	Advanced										
<p>Upgrade Packages</p> <p>This list shows the install packages that have been downloaded to the Local Controller. You may select a package and view its release notes or delete it. You may also import a new package.</p> <table border="1"> <thead> <tr> <th>Package Name</th> <th>Type</th> <th>Dependencies</th> <th>Download Time</th> <th>Size</th> </tr> </thead> <tbody> <tr> <td colspan="5" style="height: 100px;"> </td> </tr> </tbody> </table> <p> <input type="button" value="Import Package"/> <input type="button" value="Delete"/> <input type="button" value="View Release Notes"/> </p> <p> Available Storage: 2000000000 (Note: A fixed amount of storage space is available. If the limit is reached you must delete some packages to import new ones.) </p>				Package Name	Type	Dependencies	Download Time	Size					
Package Name	Type	Dependencies	Download Time	Size									

The following details appear for each package that is downloaded to this MARS Appliance:

- **Package Name**—Name of the package that is downloaded. This name is the filename of the package downloaded.
- **Type**—Identifies the type of upgrade package:
 - UPGRADE_IMAGE: The upgrade image contains both data and binary updates.
 - DATA_ONLY: The upgrade image contains data only updates.
 - BINARY_ONLY: The upgrade image contains binary only updates.
 - DEVICE_SUPPORT: This upgrade image contains support for new device types only.
 - BASE_IMAGE: The image contains the full ISO image.
- **Dependencies**—Identifies the dependencies of this package. It identifies which version must be running before the selected package can be installed.
- **Download Time**—Identifies the date and time that this package was downloaded to the appliance.
- **Size**—Identifies the amount of disk space consumed by this package.
- **Available Storage**—Identifies the amount of space available for additional packages.

Step 3 To free space on the appliance so that you can download additional packages, select a package and click **Delete**.

Step 4 To view the release notes for a package, select the package and click **View Release Notes**.

Step 5 To update the list of packages from the upgrade server (whether internal or Cisco.com) and download them to the appliance, click **Import Package**.

Result: The Package List page appears.

Cisco.com Package List

	Package Name	Summary	Version	Creation Time	Size
<input type="checkbox"/>	cs_mars	cs-mars binary package 6.0.1.2991	6.0.1.2991	Thu Jul 03 07:39:47 PDT 2008	179587873
<input type="checkbox"/>	cs_mars	CS-MARS Upgrade Package for 5.3.2 (2764)	5.3.2.2764	Tue Dec 11 06:39:47 PST 2007	146797061
<input type="checkbox"/>	cs_mars	CS-MARS Upgrade Package for 5.2.8 (2591). This Upgrade is applicable for the upgrade from 5.2.7 (2555) or from 5.2.8 (2590) on MARS 110R, 110, 210, and GC2	5.2.8.2591	Fri Nov 23 06:39:47 PST 2007	137557686
<input type="checkbox"/>	cs_mars	CCS-MARS Upgrade Package for 5.2.7 (2556). This Upgrade is applicable for the upgrade from	5.2.7.2556	Tue Oct 23 07:39:47 PDT 2007	142463718

* Installation of packages marked with an asterisk will cause a system reboot.

Step 6 Select the checkbox next to each package you want to download and click **Import**.

**Tip**

To learn about a package before you download it, select the check box next to the package and click **View Release Notes**.

**Note**

You cannot download packages if insufficient space exists to store them.

If you have specified proxy settings for the selected appliance, a popup window prompts you to verify the settings. After you verify the information, click **OK**. If you have forgotten to enter proxy information, click **Cancel** and then enter the proxy information for that Local Controller as described in [Specify the Proxy Settings for a MARS Appliance, page 5-20](#).

Result: Depending on the size of the package, this download can take some time. After the download is complete, the Install Package list is populated with this package on the Upgrade Zones page.

Upgrading a Local Controller from the Global Controller

From within the Global Controller user interface, you can schedule the download and install of an upgrade package for each managed Local Controller. Instead of requiring access to an Internal Upgrade Server, only the Global Controller needs to be able to connect to the server. Once the Global Controller downloads an upgrade package locally, it can push a copy of the upgrade package to its managed Local Controllers.

When you upgrade a Global Controller and its monitored Local Controllers, you first upgrade Global Controller, which requires that you specify which download server connection information (see [Specify Download Sever Settings, page 5-11](#)).

Before You Begin

- This procedure is valid for versions 6.0.1 and later.

- Verify that each Local Controller is running the same software version that the Global Controller was running before its upgrade. Target Local Controllers must be running the prerequisite software version that the Global Controller was running before its upgrade.

**Note**

If you upgrade a Global Controller/Local Controller pair, the Local Controller may appear offline for the first 10 minutes after the appliances reboot. The scheduler wakes up and re-syncs 10 minutes after startup.

If you notice that the Local Controller appears offline, verify that at least 10 minutes have passed since the appliances rebooted. Alternatively, you can jump start the communication by navigating to Admin > Local Controller Management in the Global Controller user interface.

Schedule Package Download and Upgrades from a Global Controller

From a Global Controller, you can download, distribute, and schedule product and data updates for each of the managed Local Controllers. You can upgrade any Local Controllers that are managed by a Global Controller from within the Global Controller user interface. This enables you to work your way through the list of Local Controllers without connecting to each appliance individually.

To schedule a managed Local Controller upgrade from the Global Controller, follow these steps:

- Step 1** From the web interface of the Global Controller, select **ADMIN > System Maintenance > Upgrade**.

Result: The Upgrade Installation pages appears with the Upgrade Zones tab selected. The list of Local Controllers that can be selected to upgrade appears.

Upgrade Installation

Upgrade Zones | Local Packages | Download Connection Information | Advanced

Upgrade Zones

This table lists the zones and the local packages that can be installed on them. To schedule a package for installation, check the zone(s) and select the package from the drop-down list, then click "Install"

	Zone Name	Zone Address	Status	Version	Install Package
<input type="checkbox"/>	AST4-210-GC-20	local	GC	6.0.1	<input type="text" value=""/>
<input type="checkbox"/>	LC-26	10.89.178.26	Active	6.0.1	<input type="text" value=""/>

Upgrade Status Logs

Time	Log Message
Mar 26, 2008 8:44:40 AM	FTP download testpatch.zip
Mar 25, 2008 7:49:30 AM	Successfully downloaded csmars-4.2.6.2458.pkg.
Mar 25, 2008 7:33:50 AM	Attempted to download csmars-4.2.6.2458.pkg was halted because the file is already stored locally.
Mar 24, 2008 10:29:55 AM	Attempted to download csmars-4.2.6.2458.pkg was halted because the file is already stored locally.
Mar 18, 2008 8:28:19 PM	Package download failed: Package link error.
Mar 18, 2008 12:51:18 PM	Catalog update successful.
Mar 18, 2008 12:51:12	FTP download testpatch.zip

- Step 2** Select the check box next to the Local Controller to upgrade, and click **Install**.

Result: The Package Installation page appears.

Package Installation

Zone Name	Zone Address	Version	Install Package	Package File
AST4-210-GC-20	"local	February 2008	27.pkg	package.zip

<input type="radio"/> Install Now	Today
<input checked="" type="radio"/> Schedule Install	02/20/08 1:30 AM

Result: Depending on the size of the package, this download can take some time. After the download is complete, the Install button becomes active.

Step 3 Do one of the following:

- Select **Install Now**, and then click **Submit**.
- Select **Schedule Install**, specify the date and time that the install should occur, and the click **Submit**.

Result: After you click Submit, the package is downloaded to the remote appliance. Depending on the size of the package, this download can take some time. The status of the upgrade appears in the **Upgrade Status Logs** box. If you chose Install Now then once the download is complete, the remote appliance needs some time to process the upgrade. After the upgrade is complete, the remote appliance reboots. During the upgrade, the user interface is also restarted. Otherwise, the install will occur as scheduled after which the remote appliance will be rebooted.

Burn an Upgrade CD-ROM

Burning an upgrade CD-ROM does not have any special requirements. If you require more than one upgrade package, you can include three upgrade packages per CD, as packages are typically around 200 MB.



Note

You must apply the upgrade packages in sequential order, and the appliance will reboot between each upgrade. It can take 30-40 minutes for an upgrade to be applied and the system to restart before you can apply the next patch.

Prepare the Internal Upgrade Server

If your MARS appliance is running a Release version earlier than 3.2.2, please contact Cisco support to obtain the appropriate upgrade files. If you are running Release 3.2.2 or more recent, follow the instructions in this section.

For Release versions prior to 3.4.1, you must use the CLI to upgrade because the old web interface allows connections only to the defunct upgrade.protegonetworks.com support site.

For CLI-based upgrades of Release versions 2.5.1 or later, the Internal Upgrade Server must meet the following requirements:

- Be an FTP, HTTP, or HTTPS server
- Require user authentication
- Accept connections from the MARS Appliance

For upgrades using the web interface (Releases 3.4.1 or later), the Internal Upgrade Server must meet the following requirements:

- Be an HTTPS or FTP server
- Require user authentication
- Accept connections from the MARS Appliance

**Note**

If you are accessing the Internal Upgrade Server through a proxy server, the proxy server must enforce inline authentication. All proxy server settings for Release 3.4.1 or later must be configured in the web interface before starting the upgrade.

Download the Upgrade Package from Cisco.com

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

Specify the Proxy Settings for a MARS Appliance

If you know that your appliance cannot directly access the Internal Upgrade Server, you can use a proxy server. This procedure describes the proxy server settings required by MARS. For information on upgrading a Local Controller from within the Global Controller user interface, see [Upgrading a Local Controller from the Global Controller](#), page 5-16.

To specify proxy settings, follow these steps:

-
- Step 1** Open the MARS user interface in your browser.
- Step 2** Select **Admin > System Parameters > Proxy Settings**.

Proxy Information

Proxy Address:	<input type="text" value="10"/> <input type="text" value="1"/> <input type="text" value="1"/> <input type="text" value="23"/>
Proxy Port:	<input type="text" value="8080"/>
Proxy User:	<input type="text" value="user"/>
Proxy Password:	<input type="password" value="****"/>

- Step 3** In the Proxy Address and Proxy Port fields, enter the address and port used by the proxy server that sits between your appliance and the Internal Upgrade Server.

- Step 4** (Optional) In the Proxy User field, specify the username that the appliance must use to authenticate to the proxy server.

**Note**

This username and password pair is neither the Cisco.com nor the Internal Upgrade Server login and password.

- Step 5** (Optional) In the Proxy Password field, specify the password associated with the username you just provided.

132536

Step 6 Click **Submit** to save your changes.

Upgrade from the CLI

You can use the **pnupgrade** CLI command to upgrade from the Internal Upgrade Server. The **pnupgrade** command supports HTTP, HTTPS, and FTP. For more information on the upgrade command, see [pnupgrade, page 1-58](#).

To upgrade using the CLI, follow these steps:

Step 1 Log in to the MARS Appliance through a console port connection or an SSH session.
Enter your MARS login name and password.

Step 2 Identify the running version of the MARS Appliance software by entering the **version** CLI command as follows:

```
[pnadmin]$ version
6.0.1 (3066) 31
```

Verify that the running version supports the upgrade to the target upgrade package, as specified in the upgrade path matrix of the [Release Notes](#) of the target upgrade version. If the running version does not support your intended upgrade, you must change your target upgrade package in accordance with the upgrade path matrix.

Step 3 Enter a **pnupgrade** command string according to your transport and media requirements as follows:



Note

MARS requires that the Internal Upgrade Server enforce user authentication. Therefore, you must specify a username and password pair to authenticate to the server whether it is accessed via HTTP, HTTPS, or FTP. In addition, if you are passing through a proxy server, that server must also enforce inline authentication.

- To upgrade from a CD-ROM located in the appliance's DVD drive:

```
[pnadmin]$ pnupgrade cdrom://package/csmars-version.zip
```

- package*—Path on the CD where you have stored the upgrade package file
- version*—Upgrade package file version number, for example, 6.0.2 (3102)

- To upgrade from an internal HTTP or HTTPS server:

For HTTPS:

```
[pnadmin]$ pnupgrade -u user:password
https://upgrade.myserver.com/upgrade/packages/csmars-version.zip
```

For HTTP:

```
[pnadmin]$ pnupgrade -u user:password
http://upgrade.myserver.com/upgrade/packages/csmars-version.zip
```

- user:password*—Your Internal Upgrade Server login name and password.
- upgrade.myserver.com/upgrade/packages*—Internal upgrade server name and path on the server where you downloaded the upgrade package file
- version*—Upgrade package file version number, for example, 6.0.2 (3102)

- To upgrade from an FTP server:

```
[pnadmin]$ pnupgrade -u user:password
ftp://upgrade.myftpserver.com/upgrade/packages/csmars-version.zip
```

- *user:password*—Your Internal Upgrade Server login name and password.
- *upgrade.myftpserver.com/upgrade/packages*—FTP server name and path on the server where you downloaded the upgrade package file
- *version*—Upgrade package file version number, for example, 6.0.2 (3102)
- To upgrade from an Internal Upgrade Server through an HTTP proxy server :

```
[pnadmin]$ pnupgrade -x proxyServerIP:proxyServerPort -U proxyUser:proxyPassword  
https://user:password@upgrade.myserver.com/upgrade/packages/csmars-version.zip
```

- *proxyServerIP:proxyServerPort*—IP address and port number of the proxy server between the MARS Appliance and the Internal Upgrade Server.
- *proxyUser:proxyPassword*—Username and password pair required for the MARS Appliance to authenticate to the proxy server. The “-U” option must be in uppercase.
- *upgrade.myserver.com/upgrade/packages*—Server name and path on the server where you downloaded the upgrade package file. In this example, an HTTPS Internal Upgrade server is specified, but HTTP and FTP are also supported.
- *version*—Upgrade package version number, for example, 6.0.2 (3102).
- *user:password*—Your Internal Upgrade Server login name and password.

Result: A progress bar indicates the download percentage. After download is complete, the system takes some time to process the upgrade. After the upgrade is complete, the system reboots.
