



Cisco Security MARS Initial Configuration and Upgrade Guide, Release 6.x

Release 6.0.x
September 2008

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number:
Text Part Number: OL-16776-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco logo, and Welcome to the Human Network 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, 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, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, 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. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Security MARS Initial Configuration and Upgrade Guide, Release 6.x
Copyright © 2008 Cisco Systems, Inc. All rights reserved.



CONTENTS

| | |
|--|------|
| Preface | vii |
| Audience | vii |
| Organization | vii |
| Related Documentation | viii |
| Obtaining Documentation, Obtaining Support, and Security Guidelines | viii |

CHAPTER 1

| | |
|---|------|
| Deployment Planning Guidelines | 1-1 |
| MARS Components | 1-1 |
| Supporting Devices | 1-1 |
| Required Traffic Flows | 1-2 |
| Web Browser Client Requirements | 1-4 |
| Configuring Internet Explorer 7.0 | 1-4 |
| Configuring Internet Explorer Settings 6.x | 1-5 |
| Configuring Pop-Up Blockers | 1-9 |
| Correcting Issues Caused by the 832894 (MS04-004) Security Update or the 821814 Hotfix (IE 6.x only) | 1-10 |
| Obtaining the Required Browser Plug-ins | 1-10 |
| Web Browser Client Usage Guidelines and Notes | 1-11 |

CHAPTER 2

| | |
|--|------|
| Initial MARS Appliance Configuration | 2-1 |
| Checklist for Initial Configuration | 2-1 |
| Establishing a Console Connection | 2-4 |
| Configuring Basic Network Settings at the Command Line | 2-6 |
| Change the Default Password of the System Administrative Account | 2-6 |
| Specify the IP address and Default Gateway for the Eth0 Interface | 2-7 |
| Specify the IP Address for the Eth1 Interface | 2-8 |
| Specify the Appliance Hostname | 2-9 |
| Set Up Additional Routes | 2-9 |
| Add a Static Route | 2-10 |
| Delete a Static Route | 2-10 |
| Specify the Time Settings | 2-10 |
| Completing the Cable Connections | 2-11 |
| Completing the Configuration using MARS web interface | 2-11 |
| Licensing the Appliance | 2-11 |

| | |
|---|------|
| Licensing the 6.x Software | 2-11 |
| Verifying and Updating Network Settings | 2-14 |
| Specifying the DNS Settings | 2-15 |
| Configuring E-mail Settings for the System Administrative Account | 2-16 |
| Configuring TACACS/AAA Login Prompts | 2-17 |
| Updating the Appliance to the Most Recent Software | 2-18 |
| Next Steps | 2-18 |

CHAPTER 3

| | |
|---|------------|
| Configuring the Global Controller | 3-1 |
| Summary of Global Controller Configuration Tasks | 3-1 |
| Global Controller–Local Controller Interoperability Information | 3-2 |
| Adding Local Controllers | 3-3 |
| Topology Synchronization | 3-4 |
| Monitoring Communication between Local and Global Controllers | 3-6 |
| Connection Event and Incident Monitoring | 3-6 |
| System Rules and System Reports | 3-6 |
| Deleting Local Controllers | 3-9 |
| Importing the Security Certificates | 3-10 |
| Monitoring Local Controller Events from the Global Controller | 3-14 |
| Preparing to Add and Discover Devices | 3-15 |
| Adding Reporting Devices | 3-15 |
| Manual Configuration | 3-15 |
| Add a Device Manually | 3-15 |
| Configuring Supported Devices | 3-16 |
| L2 Discovery and Mitigation | 3-16 |

CHAPTER 4

| | |
|--|------------|
| Performing Command Line Administration Tasks | 4-1 |
| Log In to the Appliance via the Console | 4-1 |
| Reset the Appliance Administrator Password | 4-2 |
| Shut Down the Appliance via the Console | 4-3 |
| Log Off the Appliance via the Console | 4-3 |
| Reboot the Appliance via the Console | 4-4 |
| Determine the Status of Appliance Services via the Console | 4-4 |
| Stop Appliance Services via the Console | 4-6 |
| Start Appliance Services via the Console | 4-6 |
| View System Logs via the Console | 4-7 |
| Determining the Version Running on an Appliance | 4-7 |

CHAPTER 5

| | |
|---|------------|
| Upgrade Management | 5-1 |
| Upgrade Management Overview | 5-1 |
| Checklist for Upgrades of Appliance Software | 5-3 |
| Before You Begin | 5-7 |
| Verify the MARS Appliance Version and State | 5-8 |
| Verifying the MARS Appliance System Settings | 5-8 |
| Related Documents | 5-10 |
| Specify Interval for Master Catalog Polling | 5-10 |
| Specify Download Sever Settings | 5-11 |
| Select an Upgrade Package for a MARS Appliance (local) | 5-13 |
| Manage Local Upgrade Packages | 5-14 |
| Upgrading a Local Controller from the Global Controller | 5-16 |
| Schedule Package Download and Upgrades from a Global Controller | 5-17 |
| Burn an Upgrade CD-ROM | 5-18 |
| Prepare the Internal Upgrade Server | 5-19 |
| Download the Upgrade Package from Cisco.com | 5-19 |
| Specify the Proxy Settings for a MARS Appliance | 5-20 |
| Upgrade from the CLI | 5-21 |

CHAPTER 6

| | |
|---|------------|
| Backup, Recover, Restore, and Standby Server Options | 6-1 |
| Configuring and Performing Appliance Data Backups | 6-1 |
| Typical Uses of the Archived Data | 6-2 |
| Format of the Archive Share Files | 6-3 |
| Archive Intervals By Data Type | 6-4 |
| Configure the NFS Server on Windows | 6-5 |
| Install Windows Services for UNIX 3.5 | 6-6 |
| Configure a Share using Windows Services for UNIX 3.5 | 6-7 |
| Enable Logging of NFS Events | 6-8 |
| Configure the NFS Server on Linux | 6-9 |
| Configure the NetApp NFS Server | 6-9 |
| Configure Lookup Information for the NFS Server | 6-11 |
| Configure the Cygwin SFTP Server on Windows | 6-11 |
| Configure the Data Archive Setting for the MARS Appliance | 6-13 |
| Access the Data Within an Archived File | 6-15 |
| Recovery Management | 6-16 |
| Recovering a Lost Administrative Password | 6-16 |
| Downloading and Burning a Recovery DVD | 6-16 |
| Recovery the MARS Operating System | 6-17 |

| | |
|---|------|
| Re-Imaging a Local Controller | 6-18 |
| Re-Imaging a Global Controller | 6-20 |
| Restoring Archived Data after Re-Imaging a MARS Appliance | 6-22 |
| Configuring a Standby or Secondary MARS Appliance | 6-22 |
| Guidelines for Restoring | 6-23 |

APPENDIX A

| | |
|--|------|
| Troubleshooting | A-1 |
| Determine Version Information | A-1 |
| Cannot Locate License Key | A-2 |
| Cannot Recovery My Password | A-2 |
| Cannot Delete a Device from MARS | A-3 |
| Cannot Re-Add a Device to MARS | A-3 |
| Cannot Add a Device to MARS | A-3 |
| Cannot Rename Device in MARS | A-3 |
| Collect Support Information | A-3 |
| Submitting Feedback and Reporting Errors | A-4 |
| Access the GUI when the Network Is Down | A-6 |
| Troubleshooting Global Controller-to-Local Controller Communications | A-6 |
| Communications Overview | A-6 |
| Communication States | A-7 |
| Required Open Ports | A-7 |
| General Issues and Solutions | A-8 |
| List of Backend Services and Processes | A-12 |
| Error Messages | A-15 |

INDEX



Preface

Revised: September 11, 2008, OL-16776-01

This manual describes how to initialize and prepare the Cisco Security Monitoring, Analysis, and Response System Appliance (MARS Appliance) Version 6.0.x for more detailed configuration. It describes how to upgrade an existing appliance, and how to back up existing configurations and event data. This manual also details administrative tasks that you can perform from the command line interface (CLI), including disaster recovery procedures using the Recovery DVD.

Audience

This manual is for system administrators who install and configure internetworking equipment and who are familiar with Cisco IOS software. Specifically, this manual is for system administrators who will install and configure a new MARS Appliance. It is also for administrators who have existing MARS Appliances that they want to upgrade to the most recent version available under their support contract.



Warning

Only trained and qualified personnel should install, replace, or service this equipment.

Organization

This manual consists of the following chapters and appendixes:

- [Chapter 1, “Deployment Planning Guidelines,”](#) provides guidance for device placement and calculating event/second monitoring rates to determine appropriate device monitoring limits.
- [Chapter 2, “Initial MARS Appliance Configuration,”](#) provides instructions on the initial configuration of the MARS Appliance.
- [Chapter 3, “Configuring the Global Controller,”](#) instructions on adding Local Controllers to be monitored by a Global Controller.
- [Chapter 4, “Performing Command Line Administration Tasks,”](#) describes how to perform common tasks, including shutdown, restart, and monitor logs and services from the console. It also explain how to configure a Secure Shell (SSH) client to make the console connections.
- [Chapter 5, “Upgrade Management,”](#) describes how to upgrade the appliance to the latest binary and/or data package.

- [Chapter 6, “Backup, Recover, Restore, and Standby Server Options,”](#) describes how to prepare archive servers, back up data, or restore using the Recovery DVD or an archive server. It also describes how to configure a Standby server.
- [Appendix A, “Troubleshooting,”](#) identifies backend services and describes their roles in the system. It also identifies common error messages and helps you troubleshoot known issues.

Related Documentation



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.

For a complete listing of the documentation related to this version, please see the release-specific version of the *Cisco Security MARS Documentation Guide, License, and Warranty* at:

http://www.cisco.com/en/US/products/ps6241/products_documentation_roadmaps_list.html

- You can find other product literature, including white papers, data sheets, and product bulletins, at:
<http://www.cisco.com/en/US/products/ps6241/index.html>.

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>



CHAPTER 1

Deployment Planning Guidelines

Revised: September 11, 2008, OL-16776-01

This chapter presents information to assist you in deploying one or more MARS Appliances. It contains the following sections:

- [MARS Components, page 1-1](#)
- [Supporting Devices, page 1-1](#)
- [Required Traffic Flows, page 1-2](#)
- [Web Browser Client Requirements, page 1-4](#)

MARS Components

When planning a deployment, you must consider the ability of a MARS Appliance to process the traffic expected from reporting devices on your network. Which models you purchase and where you place them on your network depends on the anticipated, sustained events per second (EPS) and NetFlow flows per second (FPS) predicted for that network or segment.

For details on the supported EPS and FPS rates per model, see the [Cisco Security Monitoring, Analysis and Response System: Data Sheet](#). This datasheet also provides detailed technical specifications on the each appliance model, such as form factor, power consumption requirements, and disk type.

Supporting Devices

Supporting devices are network devices or hosts that provide network services used by MARS. The supporting devices, both optional and required, are listed in [Table 1-1](#) to help you plan your deployment.

Table 1-1 *Supporting Devices and Their Role*

| Supporting Device Type | Is It Required? | Comment |
|-------------------------|--|---|
| E-mail Server | Yes | MARS uses e-mail servers to deliver administrative reports and notifications. |
| NTP Server | Not for single device deployment. Yes for any scenario involving a Global Controller. | You must specify the timezone and UTC settings on all appliances. The timestamps applied to received messages is critical to accurate incident correlation. |
| DNS Server | Yes | MARS uses DNS to resolve the hostnames for monitored devices, which improves the readability of reports and queries. |
| Internal Upgrade Server | No | For more information on configuring and using such a server, see Checklist for Upgrades of Appliance Software, page 5-3 . |
| GUI Client | Yes | This host is one from which you run the web interface that manages the appliance. See Web Browser Client Requirements, page 1-4 . |

Required Traffic Flows

Required traffic flows identify traffic that must be allowed by gateways if they separate the MARS Appliance from a reporting device, mitigation device, or a supporting device (as listed in [Supporting Devices](#)). Also, traffic flows between a Global Controller and any monitored Local Controllers must be allowed.

The following table identifies categories of traffic flows, the protocols required, and how long they must be allowed:

Table 1-2 *Required Traffic Flows and Ports*

| Category | Protocols | Allow Only As Needed? | Comments |
|----------------|--------------------------|-----------------------|--|
| Management GUI | HTTPS/SSL (TCP port 443) | No | You cannot effectively use the appliance and block GUI-based management traffic. This traffic must be enabled for Global Controller-to-Local Controller, as well as from the MARS Appliance to the computer you are using to manage the appliance. |
| Management CLI | SSH (TCP 22) | Yes | — |

Table 1-2 Required Traffic Flows and Ports (continued)

| Category | Protocols | Allow Only As Needed? | Comments |
|--|---|-----------------------|--|
| Support Servers and Services | DNS (TCP and UDP port 53) NTP (TCP/UDP port 123) SMTP (TCP port 25) ICMP (IP level service) NFS | | SMTP is used for outgoing mail services. ICMP is useful for diagnostics and troubleshooting and is required by the dynamic vulnerability scanner. NFS is used for network-attached storage (NAS) servers to retain data archives for MARS. Because NFS ports are negotiated, it is recommended that the NAS server be located on the same network segment as the MARS Appliance. |
| Upgrade from GUI | HTTPS or FTP (TCP port 20 and 21) | Yes | Your options from within the GUI require that you |
| Upgrade from CLI | HTTPS, HTTP (TCP port 80), or FTP | Yes | At the command line, you can also upgrade from the DVD drive, which does not require any extra opened ports. |
| Discovery of reporting device or mitigation device | Telnet (TCP port 23) SSH FTP SNMP (TCP 161) | No | MARS Appliance periodically contacts the devices to ensure they are operational. |
| Monitoring of reporting device or mitigation device | HTTPS SSH SNMP Telnet FTP PostOffice (UDP port 45000) RDEP (SSL) SDEE (SSL) syslog (UDP port 514) | No | |
| Policy query to Cisco Security Manager | HTTPS | Yes | You must enable HTTPS access to the Common Services 3.0 server by the MARS Appliance.. |
| Global Controller and Local Controller data synchronization. | Proprietary (port 8444) | No | This port must remain open on the outside and inside interfaces to ensure accurate data correlation operations of the Global Controller. |

Table 1-2 Required Traffic Flows and Ports (continued)

| Category | Protocols | Allow Only As Needed? | Comments |
|----------|---|-----------------------|---|
| | NetFlow (TCP port 2055) | | You must enable Spanning Trees between switches (distribution and access switch, not the core). You can change the port on which the appliance listens for NetFlow traffic on the Admin > NetFlow Config page. |
| | OPSEC-LEA (TCP port 18184) OPSEC-CA (TCP 18210) SSLCA (TCP port 18184) OPSEC-CPMI (TCP port 18190) | | Used by Check Point devices only. CA is used for pulling a certificate for the OPSEC application. |
| | Oracle Database Listener (TCP port 1521) | | Used by Oracle only |
| | MS SQL (TCP port 1433) | | Used by FoundStone and eEye. |

Web Browser Client Requirements

The MARS web interface should be accessed *only* from a browser instance that was used to login to MARS. Avoid using browser instances spawned from the original login instance (for example, a new browser window launched with **Ctrl+N**, **File>New>New Window**, or **right-click** {link on MARS GUI}>**Open in New Window**).

Before running the user interface provided by MARS, you must prepare Microsoft® Internet Explorer 6.0 SP1 or later or Internet Explorer 7.0 to connect to the MARS Appliance. This section describes the properly configured and patched web browser.

- Configure the Browser
 - [Configuring Internet Explorer 7.0, page 1-4](#)
 - [Configuring Internet Explorer Settings 6.x, page 1-5](#)
- [Configuring Pop-Up Blockers, page 1-9](#)
- [Correcting Issues Caused by the 832894 \(MS04-004\) Security Update or the 821814 Hotfix \(IE 6.x only\), page 1-10](#)
- [Obtaining the Required Browser Plug-ins, page 1-10](#)
- [Web Browser Client Usage Guidelines and Notes, page 1-11](#)

Configuring Internet Explorer 7.0

You can use Microsoft® Internet Explorer 7.0 or later to connect to and configure the MARS Appliance. To run it with the MARS, you must configure your browser as follows:

- Set the browser's cache to check the page every visit.
- Set security level to medium (at least) to enable ActiveX controls and scripting or add the MARS Appliance URL to the Trusted sites zone with its default settings.

- Set privacy to medium (at least) to enable cookies.
- Allow pop-ups from the MARS Appliance (disable pop-up blockers for the MARS Appliance).
- Pop-up blocker must be disabled.
- Obtain the required plug-ins. For details, see [Obtaining the Required Browser Plug-ins, page 1-10](#).

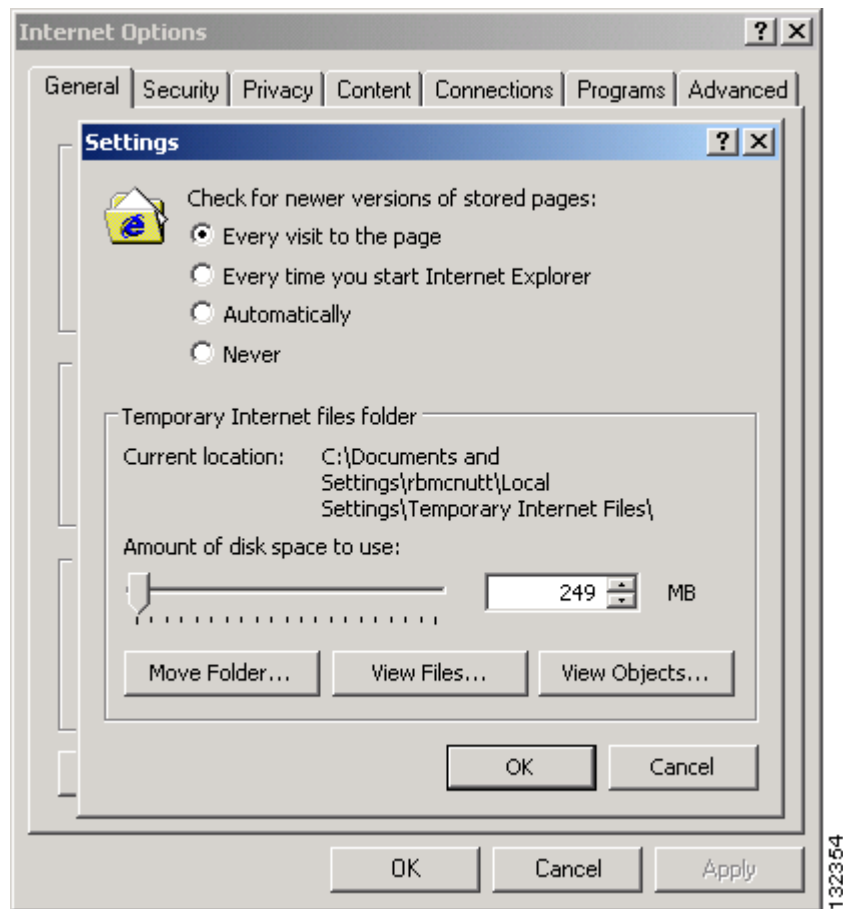
Configuring Internet Explorer Settings 6.x

You can use Microsoft® Internet Explorer 6.0 SP1 or later to connect to and configure the MARS Appliance. To run it with the MARS, you must configure your browser as follows:

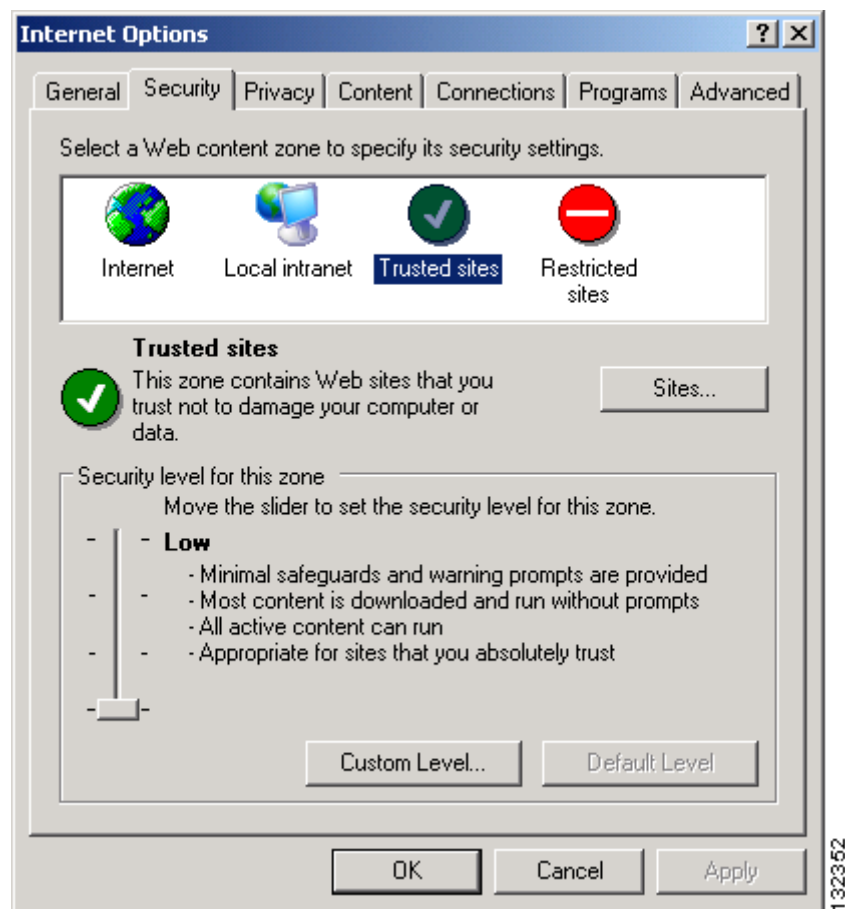
- Set the browser's cache to check the page every visit.
- Set security level to medium (at least) to enable ActiveX controls and scripting or add to the Trusted sites zone with its default settings.
- Set privacy to medium (at least) to enable cookies.
- Allow pop-ups from the MARS Appliance (disable pop-up blockers for the MARS Appliance).

To configure Internet Explorer 6.x to meet these requirements, follow these steps:

-
- Step 1** Start Internet Explorer.
- Step 2** Click **Tools > Internet Options**.
- Step 3** On the General tab under Temporary Internet Settings, click **Settings**.

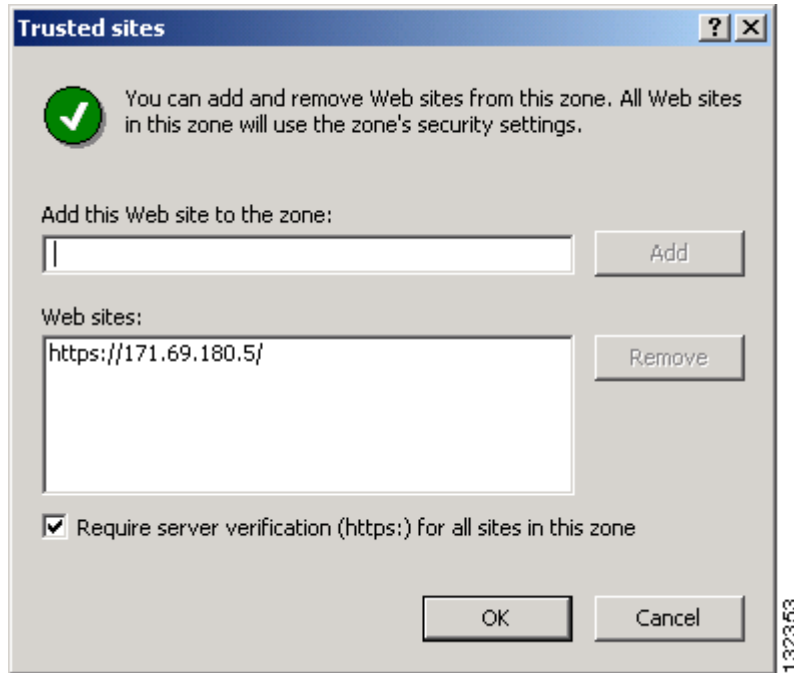
Figure 1-1 Internet Explorer Page Cache Settings

- Step 4** Click the **Every Visit to the Page** radio button.
- Step 5** Click **OK** to close the Settings dialog box and to save your changes.
- Step 6** On the Security tab under Select a Web content zone to specify its security settings, select **Trusted Sites**.

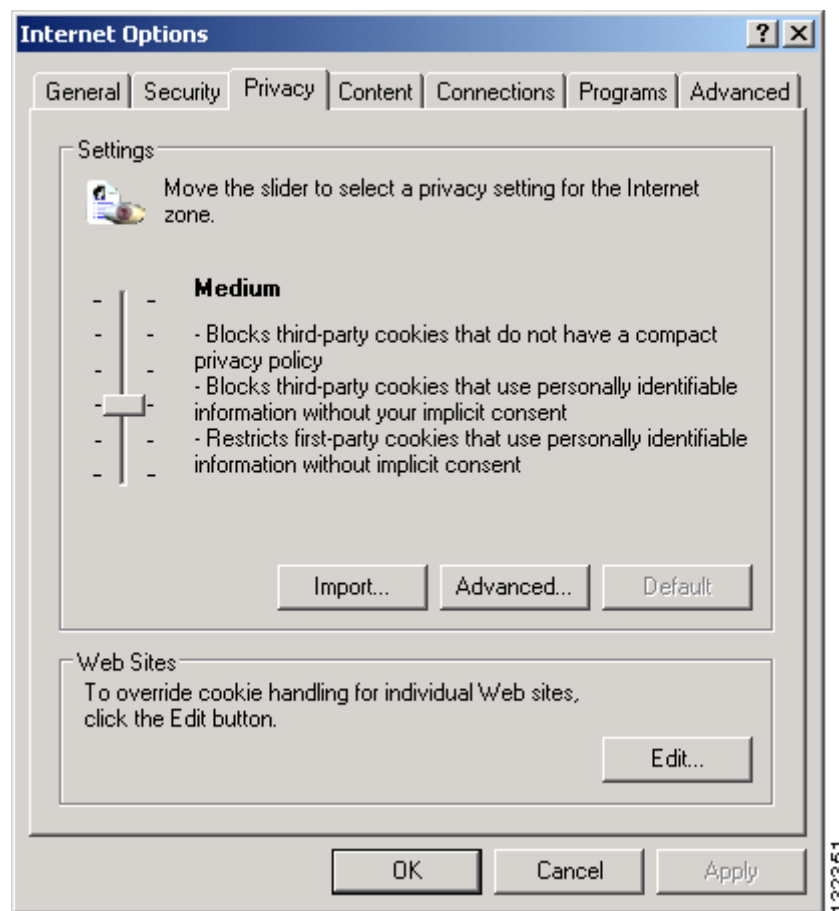
Figure 1-2 Internet Explorer Security Settings

The default security level settings for Trusted Sites is Low. If this value is not Low or Medium, use the Custom Level settings to ensure that ActiveX controls and scripting are allowed.

Step 7 With Trusted sites selected, click **Sites**.

Figure 1-3 Internet Explorer Trusted Sites

- Step 8** Enter the URL used to connect to the MARS Appliance in the Add this Web site to the zone box and click **Add**.
- Specify the full URL, preceded by https://; you can use either the DNS name or the IP address, such as https://192.168.0.1/, in the URL.
- Step 9** Click **OK** to close the Trusted sites dialog box and to save your changes.
- Step 10** On the Privacy tab under Settings, verify the selected value is **Medium**.

Figure 1-4 Internet Explorer Privacy Settings

If the selected value is not Medium, slide the bar to Medium or click Advanced to define custom settings that will enable first-party cookies.

Step 11 Click **Apply**.

Step 12 Click **OK** to close the Internet Options dialog box and to save your changes.

Configuring Pop-Up Blockers

This procedure describes how to allow access to the MARS Appliance for users running Windows XP SP2, which includes a pop-up blocker.

For information on configuring a different popup blocker to allow access to the MARS Appliance, refer to the documentation provided with the pop-up blocker product.

To enable pop-up for Internet Explorer running on Windows XP SP2, follow these steps:

Step 1 Click **Options > Toolbar Options** on the MSN toolbar.

Step 2 Select **Pop-up Blocker** under Toolbar.

In the Allow list box, enter the host ID of the MARS prefixed by https://. For example, `https://171.69.180.5/`.

**Note**

For later versions of the MSN Toolbar, you can access the Allow Lists tab by clicking the Popup Guard Settings button on Toolbar Buttons tab.

Step 3 Click **Add** to add the host to the list of sites for which pop-ups are allowed.

Step 4 Click **OK** to close the MSN Toolbar Options dialog box and to save your changes.

Correcting Issues Caused by the 832894 (MS04-004) Security Update or the 821814 Hotfix (IE 6.x only)

An issue introduced in one Internet Explorer security update, 832894, and in the 821814 hotfix can cause a “page cannot be displayed” error when you post to a site that requires authentication. If you have installed either of these updates, you must take corrective action to ensure proper operation with MARS. The following steps verify whether you have installed either update and points you to instructions provided by Microsoft to resolve the issue:

Step 1 Start Internet Explorer.

Step 2 Click **Help > About Internet Explorer**.

Step 3 Under Updated Version, look for Q832894.

If the Q832894 entry appears, you have the IE bug installed.

Step 4 If Q832894 entry appears, visit the Microsoft support web site to resolve the issue. The following knowledge base article provides specific instructions on resolving this issue:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;831167>

Obtaining the Required Browser Plug-ins

The following plug-ins are required for use with MARS:

- Adobe® SVG Viewer plug-in to view the charts, graphs, and summary page data

You can either wait for the SVG viewer to install itself when you access the Summary page for the first time, or you can download it from:

<http://www.adobe.com/svg/viewer/install/main.html>

- Adobe Reader® to view the MARS documentation

You can download the latest Acrobat Reader plug-in from:

<http://www.adobe.com/products/acrobat/readmain.html>

Web Browser Client Usage Guidelines and Notes

Familiarize yourself with the following usage guidelines and notes before using the MARS web interface:

- Avoid using the Refresh, Back, and Forward buttons in the browser. Using these buttons can lead to unpredictable behavior.
- Some pages, such as the Summary page, automatically refresh. Other pages do not. If you are viewing a page that is not automatically refreshed, you will be logged out of the user interface after a period of inactivity.
- Do not open multiple instances of the browser under the same login session. In other words, do not perform any of the following actions when viewing a page in the MARS web interface:
 - Click **File > New > Window** on the menu bar of the browser.
 - Enter **Ctrl+N**.
 - Right-click a link on the page and select **Open in New Window** on the shortcut menu.



CHAPTER 2

Initial MARS Appliance Configuration

Revised: September 5, 2008, OL-16776-01

Completing the initial configuration ensures that the MARS Appliance can communicate with other devices on the network and prepares it to monitor data from reporting devices. There are six phases to configuring the MARS Appliance. This chapter includes a checklist for initial configuration and the procedures required to complete the first five phases. The sixth and final phase of the configuration, which includes establishing administrative and user accounts, identifying the devices to monitor, and defining custom inspection rules and reports, is performed using the HTML interface and is detailed in the *User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x*.

This chapter contains the following sections:

- [Checklist for Initial Configuration, page 2-1](#)
- [Establishing a Console Connection, page 2-4](#)
- [Configuring Basic Network Settings at the Command Line, page 2-6](#)
- [Completing the Cable Connections, page 2-11](#)
- [Completing the Configuration using MARS web interface, page 2-11](#)
- [Updating the Appliance to the Most Recent Software, page 2-18](#)
- [Next Steps, page 2-18](#)

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 that the appliance is running the most recent version of software.

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

| ✓ | Task |
|---|--|
| ☐ | <p>1. Establish a console connection to the appliance.</p> <p>Initial configuration requires a console connection to access the CLI. You should establish this connection with the power turned off on the MARS Appliance. Three console connection options exist:</p> <ul style="list-style-type: none"> • A direct console connection to the appliance using a keyboard and monitor • A standard serial console connection between a computer and the appliance using a terminal emulation package • An Ethernet console connection between a computer and the appliance using a terminal emulation package <p>After you configure 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. For more information, see:</p> <ul style="list-style-type: none"> • Establishing a Console Connection, page 2-4 |
| ☐ | <p>2. Command Line Configuration: Setting the system administrative account's default password and configuring the interfaces.</p> <p>The command line configuration is separated into three tasks, each task being separated by a reboot of the appliance. The first task involves performing three to four procedures:</p> <ul style="list-style-type: none"> • Collect the information required to configure the appliance to operate optimally on your network. • Log in to the appliance and change the password associated with the system administrative account (pnadmin). • Configure the eth0 network interface, specifying the default gateway and IP address and network mask pair for that interface. • (Optional) Configure the eth1 network interface, specifying the IP address and network mask pair for that interface. <p>Each MARS Appliance has two Ethernet interfaces: eth0 and eth1. The eth0 interface is the dedicated interface used for collecting event data and logs from your network. The eth1 interface is intended for use in an out-of-band management (OOBM) network or for a console connection. Therefore, your default gateway and IP address/mask values should focus on the network connections to be used to monitor the data streams of reporting devices, and these settings should be applied to eth0.</p> <p>Note The MARS Appliance does not allow you to configure both of its interfaces on the same network.</p> <p><i>Result:</i> The default password is no longer associated with the system administrative account and the appliance is more secure. Also, the eth0 is configured to communicate on your network. When you complete the IP address configuration changes for either, the appliance reboots.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> • Configuring Basic Network Settings at the Command Line, page 2-6 • Change the Default Password of the System Administrative Account, page 2-6 • Specify the IP address and Default Gateway for the Eth0 Interface, page 2-7. • (Optional) Specify the IP Address for the Eth1 Interface, page 2-8 |

| ✓ | Task |
|---|--|
| ☐ | <p>3. Command Line Configuration.</p> <p>The second task of the CLI configuration involves setting the hostname of the appliance. The hostname identifies which appliance collects a specific log and which appliance fires an inspection rule. This unique identity is important in an environment where Global Controller is running. To complete this task, you must:</p> <ul style="list-style-type: none"> • Log in to the appliance using the system administrative account and the new password. • Set the hostname of the appliance. <p><i>Result:</i> The hostname is configured for the appliance. The appliance reboots.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> • Specify the Appliance Hostname, page 2-9. |
| ☐ | <p>4. Command Line Configuration.</p> <p>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. 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 style="list-style-type: none"> • Log in to the appliance using the system administrative account and the new password. • Set any additional static routes. • Set the clock. • Set the NTP server settings. • Set the DNS domain name. • Connect the appliance to the network (that is, plug in the Cat 5 cables.) <p><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>For more information, see:</p> <ul style="list-style-type: none"> • Specify the Time Settings, page 2-10 • Set Up Additional Routes, page 2-9 • Completing the Cable Connections, page 2-11 |

| ✓ | Task |
|---|--|
| ❏ | <p>5. Complete initial configuration using the web interface.</p> <p>After you complete the cable connections to the MARS Appliance, define the required network connection settings, and specify any additional default routes, you can start the web interface configuration process. Verify the configuration settings of your browser before configuring the MARS Appliance (see Web Browser Client Requirements, page 1-4).</p> <p>During this phase, you configure the following:</p> <ul style="list-style-type: none"> • Appliance license • Zone identification (Global Controller only) • E-mail server identification • DNS addresses • E-mail address for the system administrative account (pnadmin) • TACACS/AAA login prompt settings <p><i>Result:</i> You have configured your appliance to communicate on the network, properly correlate events, and issue system e-mails to a monitored e-mail address.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> • Completing the Configuration using MARS web interface, page 2-11 • Licensing the Appliance, page 2-11 • Verifying and Updating Network Settings, page 2-14 • Specifying the DNS Settings, page 2-15 • Configuring E-mail Settings for the System Administrative Account, page 2-16 • Configuring TACACS/AAA Login Prompts, page 2-17 |
| ❏ | <p>6. Upgrade the appliance to the most recent software version.</p> <p>The software version determines the currency of signatures, system inspection rules, features, and bug fixes. An important part of your security solution is ensuring that you maintain the most up-to-date software on the MARS Appliance. This process involves preparing an upgrade strategy and selecting a method, determining your current version, identifying the most recent version, and downloading and applying all intermediate versions of the software.</p> <p><i>Result:</i> The appliance is running the most recent version of software.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> • Checklist for Upgrades of Appliance Software, page 5-3 |

Establishing a Console Connection

Before you can perform the initial configuration of MARS Appliance, you must establish a console connection to it. You have three options for establishing an initial console connection, and four options after you complete the initial configuration. You must log in to the console using the system administrative account (pnadmin) and the password associated with that account, which is also pnadmin by default.

The three initial console connection options are:

- **Direct Console.** Directly attach a keyboard and monitor the appliance. This option provides the most console feedback of the three console connection options, and it does not require any additional software, such as a terminal emulator or SSH client.

Serial Console. Before powering on the appliance, connect a computer to the serial port using the appropriate cable. For the location of the serial port, see the backplane figure corresponding to your appliance model in the *Cisco Security MARS Hardware Installation Guide*. Configure your terminal emulation communication software (such as Hyper Terminal) to operate with the following settings:

- Baud = 9600
- Databits = 8
- Parity = None
- Stops = 1
- Flow control = None

- **Ethernet Console.** Before powering on the appliance, connect a computer to eth1 using a crossover CAT5 cable, configuring the computer's local TCP/IP settings to be on the 192.168.0.0 network. Pick an IP address other than 192.168.0.100 and 192.168.0.101, which are the default addresses assigned to eth0 and eth1, respectively. The eth1 port is reserved for administrative connections, such as the Ethernet console. For the location of the eth1 port, see the backplane figure corresponding to your appliance model in the *Cisco Security MARS Hardware Installation Guide*. Configure your terminal emulation communication software (such as Hyper Terminal) to operate with the following settings:

- Baud = 9600
- Databits = 8
- Parity = None
- Stops = 1
- Flow control = None

**Tip**

You can achieve a boost in web interface performance by configuring eth1 to be the interface by which the web interface is accessed. Because you can define the default gateway for eth0 only, you must define static routes for eth1 that ensure the administrative traffic is properly routed.

- **SSH Console.** After you complete the initial configuration as outlined in [Checklist for Initial Configuration, page 2-1](#), you can connect to the appliance from any host on your network using a SSH client. The only constraint is that the host be able to route network traffic to the appliance. Configure the SSH client to operate with the following options:
 - Hostname = Hostname or the IP address assigned to eth0 during the initial configuration.
 - Username = padmin
 - Port = 22
 - Terminal = vt100

To establish a console connection to the MARS Appliance, follow these steps:

- Step 1** Select from among the direct, serial, or ethernet console connection options and configure according to the information provided under that description.
- Step 2** Power on the MARS Appliance and the console, and if required by the option, open your terminal emulation communication software on the console.

The login prompt appears.

- Step 3** Enter **pnadmin** as the username and the password associated with that account.
By default, the password is pnadmin.



Note

If you are logging in to the appliance for the first time, you are prompted to change the password associated with this account. In doing so, you can skip [Change the Default Password of the System Administrative Account, page 2-6](#).

The `[pnadmin]$` prompt appears. You can now perform the initial configuration.

Configuring Basic Network Settings at the Command Line

The first time you boot the appliance and whenever you re-image it, you must configure the MARS Appliance. Before you begin to configure the appliance, ensure you have the following information:

- Network hostname of the appliance
- Administrative username and password
- IP, netmask, and gateway addresses you will assign to the MARS Appliance
- The IP addresses of one or more DNS servers that the appliance will use to resolve hostnames (configured in the web interface)
- Whether you will be using NTP synchronization and, if yes, the address of the NTP server
- The time, date, and timezone in which the appliance operates

To configure the MARS Appliance, follow these steps:

- [Change the Default Password of the System Administrative Account, page 2-6](#)
- [Specify the IP address and Default Gateway for the Eth0 Interface, page 2-7](#)
- (Optional) [Specify the IP Address for the Eth1 Interface, page 2-8](#)
- [Specify the Appliance Hostname, page 2-9](#)
- [Specify the Time Settings, page 2-10](#)
- [Set Up Additional Routes, page 2-9](#)

Change the Default Password of the System Administrative Account

Good security practices suggest that you now change the default password. We suggest using strong passwords for the MARS appliances.



Note

The first time you log in to the appliance using a console connection, you are prompted to change the password. The password you are changing is the password for the system administrative account, pnadmin.

To change the password associated with the pnadmin account, follow these steps:

- Step 1** Establish a console connection to the MARS Appliance; for options and details see [Establishing a Console Connection, page 2-4](#).



Note If the MARS Appliance is not configured (that is, it is new or has been re-imaged), the system displays the system information—including the software version.

- Step 2** Log in using the system administrative account and password (pnadmin/pnadmin).
The system displays the [pnadmin]\$ prompt.

- Step 3** Confirm that the following information is displayed above the [pnadmin]\$ prompt:

```
Last login: Mon May  2 10:22:34 2005 from <host_address>
```

```
CS MARS - Mitigation and Response System
```

```
? for list of commands
```

```
[pnadmin]$
```

- Step 4** At the [pnadmin]\$ prompt, enter **passwd**.



Note When you boot the system for the first time, it is not configured. Logging in as pnadmin allows you to configure the system.

The system displays the `New password:` prompt.

- Step 5** At the `New password:` prompt, enter the new password.

Passwords are case sensitive. They can contain up to 64 alphanumeric characters and special characters (!, @, #, etc.). However, a password cannot contain spaces, single quotes, double quotes, or parenthesis.

The system displays the `Retype new password:` prompt.

- Step 6** At the `Retype new password:` prompt, re-enter the new password.

The system displays the [pnadmin]\$ prompt.

Specify the IP address and Default Gateway for the Eth0 Interface

Before you can connect to the appliance and administer it using the web interface or a SSH client, you must configure the appliance so that it can be reached by other hosts on your network.

Before you specify the interface settings, verify that eth0 is *not* connected to the network.

- Step 1** Establish a console connection to the MARS Appliance; for options and details, see [Establishing a Console Connection, page 2-4](#).

- Step 2** Log in using the system administrative account and the new password specified in [Change the Default Password of the System Administrative Account, page 2-6](#).

The system displays the [pnadmin]\$ prompt.

- Step 3** At the [pnadmin]\$ prompt, enter **ifconfig eth0 <ip_address> <net_mask>**, where *ip_address* is the IP address value for this appliance and *net_mask* is the netmask value for the IP address.

The system displays the following message on the console:

```
IP addresses change will cause the system to reboot.
Do you want to proceed?
```

Step 4 To accept the net settings and reboot the appliance, enter **yes**.

The system displays the following message on the console:

```
Broadcast message from root (pts/0) <DATE>...
The system is going down for reboot NOW !!
```



Note

It can take several minutes for the appliance to reboot before you can log in again.

Step 5 After the reboot operation completes, repeat Steps 1 and 2 and then continue with [Step 6](#).

Step 6 At the [pnadmin]\$ prompt, enter **gateway** <gateway_address>, where *gateway_address* is the IP address of the default gateway for the network to which you plan to attach eth0.

Specify the IP Address for the Eth1 Interface

If you chose to use eth1 as an administrative interface (SSH or web interface), you must configure it so it can be reached by other hosts on your network. .

Before you specify the interface settings, verify that eth1 is *not* connected to the network.

To specify the IP address and default gateway address, follow these steps:

Step 1 Establish a console connection to the MARS Appliance; for options and details, see [Establishing a Console Connection, page 2-4](#).

Step 2 Log in using the system administrative account and the new password specified in [Change the Default Password of the System Administrative Account, page 2-6](#).

The system displays the [pnadmin]\$ prompt.

Step 3 At the [pnadmin]\$ prompt, enter **ifconfig eth1** <ip_address> <net_mask>, where *ip_address* is the IP address value for this appliance and *net_mask* is the netmask value for the IP address.

The system displays the following message on the console:

```
IP addresses change will cause the system to reboot.
Do you want to proceed?
```

Step 4 To accept the net settings and reboot the appliance, enter **yes**.

The system displays the following message on the console:

```
Broadcast message from root (pts/0) <DATE>...
The system is going down for reboot NOW !!
```



Note

It can take several minutes for the appliance to reboot before you can log in again.

Specify the Appliance Hostname

After you have the basic connection settings, you must specify the hostname of the appliance. To do this, you must use the console connection.

To specify the hostname, follow these steps:

-
- Step 1** Establish a console connection to the MARS Appliance; for details, see [Establishing a Console Connection, page 2-4](#).
- Step 2** Log in using the system administrative account and the new password specified in [Change the Default Password of the System Administrative Account, page 2-6](#).
- The system displays the [pnadmin]\$ prompt.
- Step 3** At the [pnadmin]\$ prompt, enter **hostname** <name>, where *name* is the hostname value for this appliance.

**Tip**

The name can contain up to 15 letters and numbers, but it cannot contain spaces.

The system displays the following message on the console:

```
Hostname change will cause the system to reboot.  
Do you want to proceed?
```

- Step 4** To accept the new hostname and reboot the appliance, enter **yes**.

The system displays the following message on the console:

```
Broadcast message from root (pts/0) <DATE>...  
The system is going down for reboot NOW !!
```

**Note**

It can take several minutes for the appliance to reboot before you can log in again.

Set Up Additional Routes

If MARS cannot access certain devices or resources (such as the Internet) through the default gateway, you must add a static route to reach such resources. You can define static routes to subnets or hosts. Adding or deleting static routes can only be performed from the CLI using the **route** command. See [Cisco Security MARS Command Reference 6.x, page 1-1](#), for more information.

**Caution**

Do not define or modify the gateway IP address using the **route** command (changes are not persistent). Instead, use the **gateway** command.

Before you can edit the routing table, you must establish a console connection to the MARS Appliance; for options and details, see [Establishing a Console Connection, page 2-4](#). The following examples show how to add or delete a static route from the routing table.

Add a Static Route

This command permanently changes the MARS routing table.

To add a route to the network `192.168.x.x`, using gateway `10.1.1.1` via `eth0`, enter:

```
route add -net 192.168.0.0 netmask 255.255.0.0 gw 10.1.1.1 dev eth0
```

To add a route to the host at `192.168.0.101`, using gateway `10.1.1.1` via `eth0`, enter:

```
route add -host 192.168.0.101 gw 10.1.1.1 dev eth0
```

Delete a Static Route

To delete a route to subnet `192.168.0.0/16`, enter:

```
route del -net 192.168.0.0 netmask 255.255.0.0
```

To delete a host at `192.168.0.101`, enter:

```
route del -host 192.168.0.101
```

Specify the Time Settings



Caution

You must configure NTP on the Global Controller and on each Local Controller to ensure that rules fired by the Local Controller are properly propagated to the Global Controller. For more information on configuring NTP, see [ntp, page 1-27](#).

After you have the basic connection settings, you must specify the time, date, and timezone of the appliance. To do this, you must use the console connection and do the following:

-
- Step 1** Access the command line interface of the appliance.
- Step 2** Enter **timezone set** to specify the timezone in which the appliance is running.
- This command displays a menu system that enables you to select the appropriate timezone based on continent/country/region or using the POSIX TZ format. When configuring a Global Controller/Local Controller hierarchy, you should ensure that each Local Controller is set to the same timezone as the reporting devices that it monitors. In addition, the Global Controller and all Local Controllers must be set to the same universal time (also referred to as UTC or GMT).
- Step 3** To specify the current time and date in accordance with the specified timezone, do one of the following:
- Identify the NTP servers as follows:
 - a. Enter **ntp server** to identify the server.
 - b. Enter **ntp sync** to force a synchronization with the server.
 - Manually specify the date and time for this appliance as follows:
 - a. Enter **date** to specify the date in *mm/dd/yyyy* format.
 - b. Enter **time** to specify the time in *hh:mm:ss* format.

- Step 4** Enter **reboot** to reboot the appliance and re-initialize all the processes using the changed time/date settings.
-

Completing the Cable Connections

If you are using a console connection to eth0 or eth1, you must now disconnect that console and connect the appliance to the network using a crossover cable. However, if you are using a non-Ethernet console connection, you can continue with [Completing the Configuration using MARS web interface, page 2-11](#).

Completing the Configuration using MARS web interface

Before you can configure MARS to monitor the reporting devices, you must use the web interface to configure the appliance with some basic information. This information includes enabling the appliance license, updating the e-mail domain, identifying the e-mail gateway, specifying DNS addresses, and identifying the e-mail account to be used for administrative notifications. After you complete this part, you can update the appliance to the most recent software version. This part comprises the following:

- [Licensing the Appliance, page 2-11](#)
- [Verifying and Updating Network Settings, page 2-14](#)
- [Specifying the DNS Settings, page 2-15](#)
- [Configuring E-mail Settings for the System Administrative Account, page 2-16](#)
- [Configuring TACACS/AAA Login Prompts, page 2-17](#)

Licensing the Appliance

How you license your appliance depends on the model number and the software support you are running. Your appliance comes with a *Software License Claim Certificate*, which you use to generate your license key using a web browser.

Licensing the 6.x Software

Adding the license file is only performed using the web interface; there is not no CLI support. In the 5.x releases, you are able upgrade a MARS 110R to a MARS 110 by purchasing and applying an additional license.

**Note**

The license key that you apply to a Global Controller does not propagate to the monitored Local Controllers. Each MARS Appliance has a unique license key.

To provision the license on 5.x software, follow these steps:

- Step 1** Locate the *Software License Claim Certificate* document that came with your product.

- Step 2** Following the instructions on the claim certificate, log on to the specified website, and obtain the license authorization key/file. The Product Authorization Key (PAK) number found on the *Software License Claim Certificate* is required for the registration process. After registering, retain the document for future reference.
- Step 3** Once you have stored the file on your local computer, verify the file has a .lic extension. If not, rename the file to have that extension. MARS prevents you from uploading a file with a different extension.
- Step 4** Open your web browser and enter one of the following URL syntaxes in the address bar:
- **https://<machine_name>/**
 - **https://<ip_address>/**

where *machine_name* is the name of the appliance as defined in [Specify the Appliance Hostname, page 2-9](#), and *ip_address* is the address assigned to the interface to which you are attempting to connect (either eth0 or eth1), as configured in [Specify the IP address and Default Gateway for the Eth0 Interface, page 2-7](#), or [Specify the IP Address for the Eth1 Interface, page 2-8](#).

You will be prompted to accept the security certificate before you can proceed. After you accept the certificate, the login page appears.

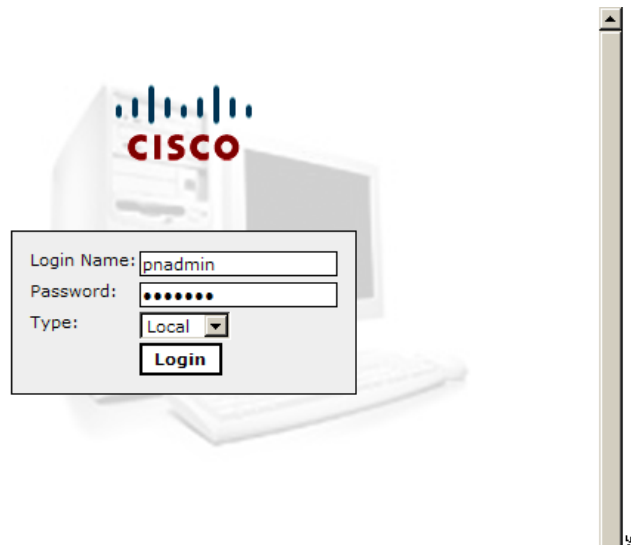
**Note**

SSL only works with the Cisco Systems self-signed certificates.

**Note**

You will be prompted to install the Adobe SVG control if not previously installed.

Figure 2-1 MARS Login Page



- Step 5** When you see the login page, enter the system administrative account (pnadmin) and the password as defined in either [Establishing a Console Connection, page 2-4](#), or [Change the Default Password of the System Administrative Account, page 2-6](#).
- Step 6** Select **Local** from the Type list because pnadmin is the local system administrative account, and click **Login**.

The *Local* versus *Global* distinction refers to the type of account you are using to log in to this appliance. Typically, you log in using an account that is defined on the Local Controller, which corresponds to the Local option in the Type list. If you are logging in using an account that is defined on the

Global Controller, select Global. When you chose to manage a Local Controller from a Global Controller, the administrative accounts defined for the Global Controller are pushed down to the Local Controller.

**Note**

The first time you log in, expect performance to be a little slow due to first-time caching and compilation.

If the MARS license key is not configured, the License Key dialog prompts you to enter this key.

Figure 2-2 Click the License Key Link

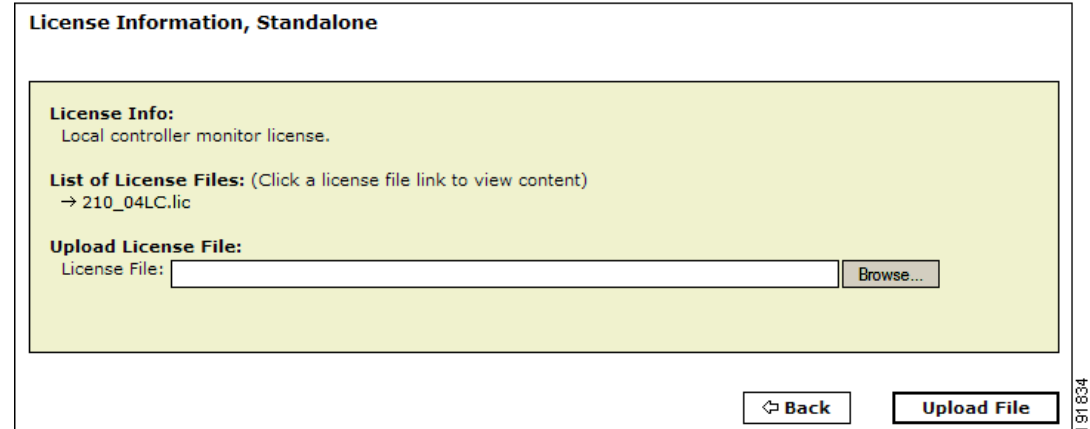


- Step 7** Click the link that directs you to load the license key file on the System Maintenance > License Key, Upgrade, and Certificates > Set License page.

You must load this key to activate the MARS Appliance before you can use it.

The License Information page displays.

Figure 2-3 Import the License Key



- Step 8** Click **Browse** under Upload License Files, select the .lic file on your local computer, and click **Open**. The license key file is uploaded appears under List of License Files. The license key information field is populated based on the information found in the license file.

- Step 9** To view the content of an uploaded license file, click the link of the license filename under the List of License Files.

**Note**

You cannot edit the content of the license file from this page

Verifying and Updating Network Settings

To complete the configuration of the appliance, you must enter basic configuration information that can only be set using the web interface. Specifically, you must designate its network zone (if it is a Global Controller) and enter e-mail gateway information, which is used by the appliance to deliver e-mail notifications.

To configure the necessary settings, follow these steps:

Step 1 Select **Admin > System Setup > Configuration Information**.

The Device Configuration page displays.

Figure 2-4 Entering Configuration Information (Global Controller example)

CS-MARS Device Config

→ Name:

→

| Interface Name | IP Address | | | | Net Mask | | | | Default Gateway | | | |
|----------------|------------|-----|---|-----|----------|-----|-----|---|-----------------|---|---|---|
| eth0 | 10 | 2 | 3 | 181 | 255 | 255 | 255 | 0 | 10 | 2 | 3 | 1 |
| eth1 | 192 | 168 | 1 | 100 | 255 | 255 | 255 | 0 | | | | |

→ Zone:

Name:

Description:

→ Mail Gateway:

IP:Port :

Email domain name: (ex: Enter 'domain1' for user@domain1)

Email Format: ☒ Full graphics ☐ Minimal graphics (Recommended for Lotus Notes clients)

Step 2 Verify the following information is correct:

- *Name*
Identifies the hostname for this appliance. This value serves not only as the hostname of the appliance, but the web interface uses this name in topologies, incidents, rules, queries, and reports.



Note

The MARS *cannot* have spaces in its hostname. The name can contain up to 15 letters and numbers.

- *Interface Name*
The two network interfaces for the MARS are eth0 and eth1. See the backplane figure corresponding to your appliance model in the *Cisco Security MARS Hardware Installation Guide* for more information.
- *IP Address*
Identifies the IP address for each interface. These interfaces must reside on different subnets.

- *Net Mask*
Identifies the network mask values for eth0 and eth1.
- *Default Gateway*
Identifies the IP address for the default gateway for the eth0 interface.

**Note**

Changing the appliance's name, IP addresses, or netmask information on this page reboots the appliance after you click **Update**.

- Step 3** (Global Controller only) In the Zone field, enter the name for a geographical or virtual zone where the Global Controller resides. One Local Controller can operate in a single zone.
- Step 4** In the IP:Port field under Mail Gateway, enter the IP address and port on which your e-mail gateway listens. You can enter an IP address, or if the DNS is resolved, you can use the gateway name. This appliance uses the e-mail gateway to send e-mail notifications. The port number is usually 25 for SMTP.
- Step 5** In the E-mail domain name field under Mail Gateway, enter the domain name from which e-mail notifications will originate.
- This value is the fully qualified domain name, such as `example.com`.
- When rule notifications are sent from the appliance, the messages are delivered from the sender: `notifier.<hostname>@<e-mail_domain>`, where *hostname* is the hostname for the appliance and *e-mail_domain* is the domain name specified in this field.
- When report notifications are sent from the appliance, the messages are delivered from the sender: `<type>.scheduler.<hostname>@<e-mail_domain>`, where *type* is either local or global (depending on whether the report was defined at the global or local level), *hostname* is the hostname for the appliance, and *e-mail_domain* is the domain name specified in this field.
- Step 6** Click **Submit** to save your changes.

Specifying the DNS Settings

The local TCP/IP stack that resides on the appliance uses DNS services just as any host on the network does. In addition, MARS uses DNS to resolve the IP addresses into hostnames for events that it studies. This mapping enables you to study events by hostname or by IP address.

To specify the DNS settings for the appliance, follow these steps:

- Step 1** Select **Admin > System Setup > Configuration Information**.
- Step 2** Scroll down past the Device Config group to the DNS Config group.

Figure 2-5 Domain Name Server Information

DNS Config

→ DNS Address

Primary DNS:

Secondary DNS:

Tertiary DNS:

DNS Search Path

Search Domain:

Add

Delete

Back

Update

132962

- Step 3** In the Primary, Secondary, and Tertiary DNS address fields, enter any DNS addresses necessary.
- Step 4** In the Search Domain field, enter the domain and click **Add**.
- Step 5** Click **Update** to save your changes.



Note

If the DNS configuration is changed from the web interface, you must perform a pntstop and then a pntstart operation for the new DNS information to be used by the MARS Appliance. For information on performing these two operations, see [Stop Appliance Services via the Console, page 4-6](#) and [Start Appliance Services via the Console, page 4-6](#).

Configuring E-mail Settings for the System Administrative Account

One of the required settings for MARS is the e-mail address for the system administrative account, pnadmin. The MARS Appliance uses this e-mail address to deliver import notifications and reports about system status.

To specify the e-mail address for the system administrative account, follow these steps:

- Step 1** Select **Management > User Management**.
- Step 2** Select the check box next to Administrator (pnadmin), and click **Edit**.
- Result:* The User page appears.

- Step 3** In the Email field, enter the e-mail alias to be used for this account.
- Step 4** Update any other information as needed.
- Step 5** Click **Submit**.

Configuring TACACS/AAA Login Prompts

By default, MARS knows what the default device login prompt looks like. When attempting to connect to a reporting device or mitigation device, MARS validates the prompt to avoid login failures. However, if you use a TACACS-based AAA server to manage the administrative access to your reporting devices and mitigation devices, you must describe the login prompts for username and password so that MARS can recognize them.

Many servers provide the ability to develop custom prompts to avoid providing information about the devices on their networks. This technique, known as security through obscurity, allows you to hide the specifics about network devices from hackers and others. The value of this technique is that it is more difficult to identify the device type and operating system version, which are used to identify weaknesses of a given device. Using a custom prompt makes all devices appear to be the same, and since it is custom, it is more difficult to probe with automated device recognition tools.

To specify your TACACS/AAA prompt settings, follow these steps:

- Step 1** Select **Admin > System Parameters > TACACS/AAA Server Prompts**.

- Step 2** In the Default Login Prompt field, enter the text displayed at the prompt when requesting the username to access the reporting device.
- Step 3** In the Default Password Prompt field, enter the text displayed at the prompt when requesting the password associated with a username.
- Step 4** Click **Submit** to save your changes.

The specified settings are used globally by MARS to recognize prompts by the TACACS/AAA server. In the event that neither the TACACS/AAA server prompt or the default device prompt is recognized, MARS does not attempt to connect to the device and an error message is generated.

Updating the Appliance to the Most Recent Software

After you complete the initial configuration, you need to verify that the appliance is running the most recent version of available software. For more information and procedures on updating the software, see [Checklist for Upgrades of Appliance Software, page 5-3](#).

When the software update is complete, you can identify the reporting devices to monitor, as discussed in [Next Steps, page 2-18](#).

Next Steps

If you are configuring a Global Controller for the first time, you must identify the Local Controllers that you want to monitor. For information on preparing the Global Controller, see [Summary of Global Controller Configuration Tasks, page 3-1](#).

After you have successfully performed the procedures in this guide, your MARS Appliance is installed and initially configured. The next step is to use a browser and the web interface to fully configure your MARS Appliance to provide the STM services you want from this installation.

This configuration includes:

- Defining additional administrative accounts
- Identifying the reporting devices and mitigation devices
- Defining custom inspection rules
- Defining custom reports
- Tuning false positives

For information on configuring devices to monitor, creating inspection rules, and other parameters, see the *User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x*.



CHAPTER 3

Configuring the Global Controller

This chapter contains the following topics:

- [Summary of Global Controller Configuration Tasks, page 3-1](#)
- [Global Controller–Local Controller Interoperability Information, page 3-2](#)
- [Adding Local Controllers, page 3-3](#)
- [Importing the Security Certificates, page 3-10](#)
- [Monitoring Local Controller Events from the Global Controller, page 3-14](#)
- [Preparing to Add and Discover Devices, page 3-15](#)
- [Adding Reporting Devices, page 3-15](#)
- [Configuring Supported Devices, page 3-16](#)
- [L2 Discovery and Mitigation, page 3-16](#)

Once you have performed the configuration tasks described in this chapter, a Global Controller administrator can create, edit, or delete user-defined settings and rules on the Global Controller and its monitored Local Controllers. These settings and rules include:

- Rules
- Reports and queries
- User, IP, and service management

Summary of Global Controller Configuration Tasks

To configure the Global Controller, you must perform several tasks before you can monitor the events and incidents reported by Local Controllers:

1. Configure the Global Controller to operate on your network. For more information on configuring the Global Controller to connect to your network, see the [Chapter 2, “Initial MARS Appliance Configuration.”](#)
2. Divide your network topology into locally controlled zones. For each zone identified, install and configure a Local Controller.
3. Add the reporting and mitigation devices in a zone to the Local Controller that monitors that zone. Also, configure the SNMP read-only community string settings for those devices to enable network discovery.

4. Add the zones to be monitored into Global Controller. Each zone is represented by a single Local Controller. By adding a Local Controller to the Global Controller, you are indicating that the Global Controller should monitor that local zone.



Note You can only add reporting devices to an active Local Controller.

5. Import the security certificate from each Local Controller into the Global Controller and vice versa. Sharing the security certificates among the appliances enables secure communications between a Local Controller and the Global Controller.
6. When a Global Controller and Local controller are separated by a firewall, open the following ports on both the inside and outside interfaces of the firewall to ensure proper operation of the Global Controller:

| Port | Function |
|------|---|
| 22 | Secure Shell (SSH) |
| 443 | Hyper Text Transport Protocol with Secure Sockets Layer (HTTPS) |
| 8444 | Cisco Proprietary data synchronization with Local Controller |

Global Controller–Local Controller Interoperability Information

Feature History for MARS Appliance GC–LC Interoperability

| Release Version | Description |
|-----------------|---|
| 4.3.1 / 5.3.1 | Introduced interoperability for LCs running different MARS release versions than the GC |

To interoperate, a Global Controller and a Local Controller must be running compatible releases of the MARS operating systems. A Global Controller cannot add a Local Controller running an incompatible release. [Table 3-1](#) lists which Local Controllers (20R, 20, 50, 100E, 100, 200, 110, 110R, 210) can interoperate with which Global Controllers (GCM, GC, GC2R, GC2).

Local Controllers reporting to the same Global Controller can be running different releases. [Table 3-2](#) lists the compatible releases required for a Global Controller to interoperate with a Local Controller.

The GC2R and the GCM are designed to operate only with Local Controllers 20R, 20, and 50.

Table 3-1 Global Controller to Local Controller Interoperability Matrix

| | 20R | 20 | 50 | 100E | 100 | 200 | 110 | 110R | 210 |
|-------------|-----|-----|-----|------|-----|-----|-----|------|-----|
| GCM | Yes | Yes | Yes | No | No | No | No | No | No |
| GC | Yes | Yes | Yes | Yes | Yes | Yes | No | No | No |
| GC2R | Yes | Yes | Yes | No | No | No | No | No | No |
| GC2 | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |

Table 3-2 Release Requirements for Global Controller –Local Controller Interoperability

| Release Versions—Global Controller ¹ | Release Versions—Local Controllers |
|---|---|
| 5.3.1 | 4.3.1 or 5.3.1 |
| 4.x.x | Local Controller must run identical release version |

1. Release 5.x operates only on Global Controllers GC2R and GC2, and on Local Controller 110R, 110, and 210.
Release 4.x operates only on Global Controllers GC and GCM, and on Local Controllers 100E, 100, and 200.

Adding Local Controllers

Follow these steps to add a Local Controller to the Global Controller:

- Step 1** Click **ADMIN > System Setup > Local Controller Management** to display the Zone Controller Information page, as shown in [Figure 3-1](#).

Figure 3-1 Zone Controller Information Page

The screenshot shows the Cisco MARS web interface. At the top, there's a navigation bar with tabs: SUMMARY, INCIDENTS, QUERY / REPORTS, RULES, MANAGEMENT, ADMIN (selected), and HELP. Below this is a sub-navigation bar with: System Setup, System Maintenance, User Management, System Parameters, and Custom Setup. The main header area shows 'Sep 5, 2006 12:25:03 PM PDT' and 'ADMIN | CS-MARS Global Controller: gc60 v4.2'. There are also links for 'Login: Global: Administrator (pnadmin)', 'Logout', and 'Activate'.

The main content area is titled 'Zone Controller Information'. It includes a 'Page Refresh Rate' dropdown set to '15 minutes'. Below this are buttons: Edit, Delete, Add, Back, Topo Sync Start/Stop, Suspend/Resume, and Details....

| | Zone Name | Device Name | Zone Model | Zone Address | Version | Description | Status |
|--------------------------|-----------|-------------|------------|--------------|---------|-------------|---|
| <input type="checkbox"/> | LC133 | pnmars | CS-MARS 20 | 10.1.1.133 | 4.2.1 | LC133 | Active (last checked: Tue Sep 05 12:25:03 PDT 2006) |

At the bottom right, there's a pagination control showing '1 to 1 of 1' and '25 per page'.

- Step 2** Click **Add**.
A pop-up window appears in which you can add a Local Controller to the Global Controller.

Figure 3-2 Local Controller Information Page

The screenshot shows a 'Local Controller Information' pop-up window. It has three input fields: 'Zone Name' with the value 'HQ_Local_Zone', 'Zone Description' with the value 'Headquarters Zone', and 'LC IP Address' with the value '10.2.3.66'. At the bottom of the window are two buttons: 'Cancel' and 'Submit'.

Step 3 Enter values for the following settings:

- **Zone Name.** Enter a name for this zone. This name is used to uniquely identify the networks within this zone relative to other zones. For example, many companies use the same private network addresses behind NATed gateways. The zone combined with the network address allows you to reuse the same network address on your private networks.
- **Zone Description.** Enter a description of the zone
- **LC IP Address.** Enter the IP address of the Local Controller that monitors this zone.

Step 4 Click **Submit** to save the values.

Before the Global Controller can communicate with the Local Controller, you must import the security certificate into the Global Controller. For more information, see [Importing the Security Certificates, page 3-10](#).

Topology Synchronization

For the Global Controller to display a summarized and merged view of topology for its Local Controllers, topology data from all the Local Controllers must be pushed to the Global Controller. When you add a Local Controller to a Global Controller, the topology synchronization process begins and completes automatically.

When synchronized with Local Controllers, the Global Controller contains all the security and monitoring information of the Local Controllers (as displayed on **Admin > System Maintenance > Security and Monitor Devices**) and can display the combined topological maps of the Local Controllers with the following constraints:

- Devices common to Local Controllers are merged in the Global Controller topology. If you have a router listed on different Local Controllers, it only shows up once in topology graphs.
- Networks common to Local Controllers are not merged in the Global Controller topology, but are displayed as separate topologies even if they are the same network.

Topo Sync Start/Stop

When you change Local Controller topology or it otherwise becomes out-of-sync, you can re-synchronize the Local Controller and Global Controller by clicking **Topo Sync Start/Stop** on the Zone Controller Information Page. The **Status** field reports the current state of the synchronization process. [Table 3-3](#) lists and describes all possible status messages.

An out-of-sync condition can occur when unexpected errors or events (device, software, network, etc.) disrupt communication between the Local and Global Controllers.

Suspend/Resume

The **Suspend/Resume** button toggles the communication link on and off between the Global Controller and the Local Controller. When suspended, the Local Controller cannot communicate with the Global Controller.



Note

Incident, topology, and other information cannot be uploaded to the Global Controller when the Local Controller communication is suspended.

Table 3-3 Local Controller Status Messages on Zone Controller Page

| Status Field Values | Description and Action |
|---|---|
| Active (last checked: <i>Time_and_Date_last_checked</i>) | The Local Controller is online, connected, and synchronized with the Global Controller. |
| Suspended | Communications between the Local Controller and the Global Controller have been manually halted with the Suspend/Resume button. To re-establish communication, select the Local Controller and click Suspend/Resume . |
| Synchronizing (<i>progress</i>) | The Global Controller and Local Controller are comparing and updating their topology information tables. |
| Deleting in progress | The Global Controller is purging the selected Local Controller configuration and data from its database. If the Global and Local Controllers can communicate, the Local Controller is purging Global Controller configurations to change from monitor to standalone mode. |
| Not Responding (last checked: <i>Time_and_Date_last_checked</i>) | The Local Controller cannot be detected on the network. Check network status and connections. |
| Local Controller is online but is not responding (last checked: <i>Time_and_Date_last_checked</i>) | The Local Controller can be detected on the network, but does not respond. The problem or delay may clear, the status can return to Active. |
| Zone has standalone license | The Local Controller model indicated is not supported by the Global Controller. |
| Global controller license does not allow adding model PNMARS-100 for monitoring | The Local Controller model indicated is not supported by the Global Controller. |
| Global controller license does not allow adding model PNMARS-100X for monitoring | The Local Controller model indicated is not supported by the Global Controller. |
| Global controller license does not allow adding model PNMARS-200 for monitoring | The Local Controller model indicated is not supported by the Global Controller. |
| Zone version is different | The Global and Local Controllers are operating with different software versions. Update one or the other or both as appropriate. |
| Global license is Local Controller license | Enter the correct Global Controller license in the Global Controller at Admin > System Maintenance > Set License Key . |
| Global certificate not in LC or local certificate not on GC | Copy the Global Controller security certificate to the Local Controller, and the Local Controller security certificate to the Global Controller at Admin > System Maintenance > Certificates |

Monitoring Communication between Local and Global Controllers

Communication status between the Local and Global Controller is displayed on the Global Controller Zone Information Page, as shown in [Figure 3-1](#), with the status messages described in [Table 3-3](#).

Feature History for MARS Appliance GC–LC Communication Monitoring

| Release Version | Description |
|-----------------|--|
| 4.3.1 / 5.3.1 | Events, Rules, and Reports introduced to monitor GC–LC communication |

In summary, communication problems between the Global Controller and Local Controllers are typically caused by one or more of 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

Monitoring the connection to the Global Controller from the Local Controller is accomplished by using syslogs, system rules and system reports designed to detect typical communication failure events.

Connection Event and Incident Monitoring

Every two minutes, a MARS process runs on the Local Controller to check the connection status, certificate information, and MARS release versions of itself and the Global Controller.

Syslogs are generated according to the following algorithm:

1. If the same error is found on three consecutive 2-minute checks, a syslog is generated as described in [Table 3-3](#) for Event IDs 1000059, 1000062, and 1000064.
2. If the same error is discovered in the next three consecutive 2-minute checks, a “continues to fail” syslog is generated, as described in [Table 3-3](#) for Event IDs 1000061, 1000063, and 1000065.
3. If the same error is detected in every subsequent 2-minute check for two hours, the “continues to fail” syslog reporting interval is lengthened to every eighteen minutes from every six minutes.
4. Whenever a discovered error is corrected (not detected), a “recovered” syslog is generated, as described in [Table 3-3](#) for Event ID 1000066.

The Local Controller sends the syslog messages to itself through the eth0 interface.

System Rules and System Reports

There are three system rules and two system reports of the Local Controller that can alert MARS users of communication issues with the Global Controller, as described in [Table 3-5](#) and [Table 3-6](#) respectively.

Table 3-4 Local Controller Events and Syslog Messages for Local Controller –Global Controller Communication

| Event ID | Event Description and Raw Message | Device Event ID | Event Groups |
|----------|--|------------------------|--------------------------|
| 1000059 | CS-MARS LC failed to communicate with GC due to connectivity issue | PN-MARS: MARS-2-350050 | OperationalError/CS-MARS |
| | OperationalStatusChange/CS-MARS | | |
| | %MARS-2-350050 LC for zone '<LC_zone>' at '<LC_IP_address>' failed to communicate with GC at <GC_IP_address>' due to connectivity issue for 3 times in the last 6 consecutive minutes. LC last successfully connected to GC at <date_time>. | | |
| 1000061 | CS-MARS LC continues to fail to communicate with GC due to connectivity issue | PN-MARS: MARS-2-350051 | Info/Misc/CS-MARS |
| | OperationalError/CS-MARS | | |
| | %MARS-2-350051 LC for zone '<LC_zone>' at '<LC_IP_address>' continues to fail to communicate with GC at <GC_IP_address>' due to connectivity issue for <m> times in the last <n> consecutive minutes. LC last successfully connected to GC at <date_time>. | | |
| 1000062 | CS-MARS LC failed to communicate with GC due to certificate mismatch | PN-MARS: MARS-2-350052 | OperationalError/CS-MARS |
| | OperationalStatusChange/CS-MARS | | |
| | %MARS-2-350052 LC for zone '<LC_zone>' at '<LC_IP_address>' failed to communicate with GC at <GC_IP_address>' for 3 times in the last 6 consecutive minutes due to certificate mismatch. LC last successfully matched the certificates with GC at <date_time>. | | |
| 1000063 | CS-MARS LC continues to fail to communicate with GC due to certificate mismatch | PN-MARS: MARS-2-350053 | Info/Misc/CS-MARS |
| | OperationalError/CS-MARS | | |
| | %MARS-2-350053 LC for zone '<LC_zone>' at '<LC_IP_address>' continues to fail to communicate with GC at <GC_IP_address>' for <m> times in the last <n> consecutive minutes due to certificate mismatch. LC last successfully matched the certificates with GC at <date_time>. | | |
| 1000064 | CS-MARS LC failed to communicate with GC due to incompatible software/data versions | PN-MARS: MARS-2-350054 | OperationalError/CS-MARS |
| | OperationalStatusChange/CS-MARS | | |
| | %MARS-2-350054 LC for zone '<LC_zone>' at '<LC_IP_address>' failed to communicate with GC at <GC_IP_address>' for 3 times in the last 6 consecutive minutes due to incompatible software/data versions. LC version is <x1.y1.z1>. GC version is <x2.y2.z2>. LC last successfully had compatible software/data versions with GC at <date_time>. | | |
| 1000065 | CS-MARS LC continues to fail to communicate with GC due to incompatible software/data versions | PN-MARS: MARS-2-350055 | Info/Misc/CS-MARS |
| | OperationalError/CS-MARS | | |
| | %MARS-2-350055 LC for zone '<LC_zone>' at '<LC_IP_address>' continues to fail to communicate with GC at <GC_IP_address>' for <m> times in the last <n> consecutive minutes due to incompatible software versions. LC version is <x1.y1.z1>. GC version is <x2.y2.z2>. LC last successfully had compatible software/data versions with GC at <date_time>. | | |
| 1000066 | CS-MARS Communication from LC to GC has recovered | PN-MARS: MARS-2-350056 | Info/Misc/CS-MARS |
| | OperationalStatusChange/CS-MARS | | |
| | %MARS-2-350056 Communication has recovered from LC for zone '<LC_zone>' at '<LC_IP_address>' to GC at <GC_IP_address>'. Communication was unsuccessful for <this_number_of> minutes. | | |

Table 3-5 Local Controller System Rules for Local Controller –Global Controller Communication

| System Rule | Rule Description |
|--|---|
| System Rule: CS-MARS LC-GC Communication Failure - Connectivity Issue | <p>This rule fires if there is one or more repeated connectivity failure messages. Potentially, this could be a transient failure that may correct itself. The rule is a 3-offset rule as follows:</p> <p>(CS-MARS LC failed to communicate with GC due to connectivity issue</p> <p>FOLLOWED-BY</p> <p>CS-MARS LC continues to fail to communicate with GC due to connectivity issue)</p> <p>OR</p> <p>CS-MARS LC continues to fail to communicate with GC due to connectivity issue</p> <p>Each offset has a count of 1 and a time range of 10 minutes.</p> |
| System Rule: CS-MARS LC-GC Communication Failure - Certificate Mismatch | <p>This rule is a one offset rule that matches against the event:</p> <p>CS-MARS LC failed to communicate with GC due to certificate mismatch</p> <p>The count is 1, the time range is 1 minute.</p> |
| System Rule: CS-MARS LC-GC Communication Failure - Incompatible Versions | <p>This rule is a one offset rule that matches against the event:</p> <p>CS-MARS LC failed to communicate with GC due to incompatible software/data versions</p> <p>The count is 1, the time range is 1 minute</p> |

Table 3-6 Local Controller System Reports for Local Controller –Global Controller Communication

| System Report | Report Description |
|--|---|
| Activity: CS-MARS LC-GC Communication Failures (Total View) | <p>Report scheduled for every hour.</p> <p>Query Type: Custom Columns ranked by Time, with “ANY” in all columns except Query, where event type matches any one of the communication failure events listed in Table 3-3 (Event IDs 1000059–1000065).</p> <p>The custom columns are ordered as Source Address, Event Type Set, Time Range and Raw Message.</p> |
| Activity: CS-MARS LC-GC Communication Recovered (Total View) | <p>On-demand report with a time range of 1 hour.</p> <p>Query Type: Custom Columns ranked by Time, with “ANY” in all columns except Query, where event type matches the event “CS-MARS Communication from LC to GC has recovered” (Event ID 1000066 in Table 3-3)</p> <p>The custom columns are ordered as Source Address, Event Type Set, Time Range, and Raw Message.</p> |

Deleting Local Controllers

To delete a Local Controller from the Global Controller and return the Local Controller to Standalone mode, do the following steps:

- Step 1** Click **ADMIN > System Setup > Local Controller Management**, to display the Zone Controller Information page, as shown in [Figure 3-3](#).

Figure 3-3 Zone Controller Information Page

The screenshot displays the 'Zone Controller Information' page in the Cisco MARS interface. At the top, there is a navigation bar with tabs for SUMMARY, INCIDENTS, QUERY / REPORTS, RULES, MANAGEMENT, ADMIN, and HELP. Below this, a breadcrumb trail shows 'System Setup > System Maintenance > User Management > System Parameters > Custom Setup'. The page title is 'Zone Controller Information'. A 'Page Refresh Rate' dropdown is set to '15 minutes'. Below this, there are buttons for 'Edit', 'Delete', and 'Add'. A table lists the zone controllers:

| Zone Name | Device Name | Zone Model | Zone Address | Version | Description | Status |
|-----------|-------------|------------|--------------|---------|-------------|---|
| LC1 | LC1 | CS-MARS S0 | 10.2.3.91 | 4.2.2 | zone_LC1 | Active (last checked: Tue Sep 05 14:23:01 PDT 2006) |
| LC2 | LC2 | CS-MARS 20 | 10.2.3.92 | 4.2.2 | zone_LC2 | Active (last checked: Tue Sep 05 14:23:01 PDT 2006) |

Below the table, there are buttons for 'Edit', 'Delete', and 'Add', and a 'Back' button. A pagination bar shows '1 to 2 of 2' and '25 per page'. The footer contains copyright information: 'Copyright © 2003, 2006 Cisco Systems, Inc. All rights reserved.' and a 'Feedback' link.

- Step 2** Click the checkbox of the Local Controller to delete, and click **Delete**.

A Yes/No confirmation dialog box appears. Click **Yes** to remove configuration info and data from the Global and Local Controllers.

If the status of the Local Controller is **Not Responding**, a Continue/Cancel dialog box appears. Because the Global Controller cannot communicate with the Local Controller, clicking **Continue** removes only the Local Controller data from the Global Controller. To remove the Global Controller configuration information from the Local Controller, you must execute a **pnreset -s** CLI command on the Local Controller as explained in the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/command/reference/cref1.html#wp1071420



Note

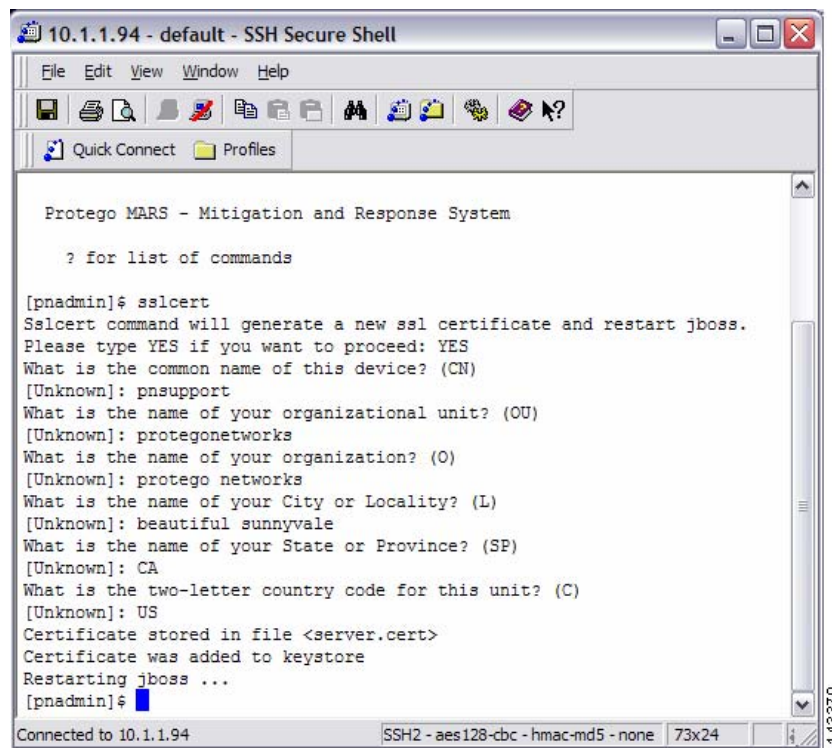
If you do not remove the Global Controller configuration from the Local Controller, errors may occur when the Local Controller attempts to contact the Global Controller. Moreover, the Local Controller cannot be added to a Global Controller until it is reset.

The duration of the deletion process varies with the amount of data to be deleted. A duration of many minutes is possible.

Importing the Security Certificates

Security certificates are used for secure communications between a web browser and the Global Controller, as well as between the Global Controller and any Local Controllers that are managed by the Global Controller. Every Global Controller comes with a default certificate which is unique to each Global Controller. However, users could choose to modify the default certificate using the `sslcert` CLI command. For more information on using the `sslcert` command, see [sslcert](#), page 1-91 in the *Cisco Security MARS Initial Configuration and Upgrade Guide, Release 6.x*.

Figure 3-4 Changing the Default Security Certificate



If you wish to install the certificate to an Internet Explorer browser, you must do it during the Global Controller login process.

When the Security Alert pop up appears, choose:

-
- Step 1** View Certificate.
 - Step 2** Install Certificate. Then click **Next**.
 - Step 3** Select *Automatically Select the Certificate Based on the Type of Certificate*. Then click **Next**.
 - Step 4** Complete the Certificate Import process by clicking **Finish**.
 - Step 5** Select **Yes** to add the certificate to the Root Store.

Figure 3-5 Global Controller Login Security Alert

The security certificate is used for communication between a Global Controller and any Local Controllers that are managed by the Global Controller.

Although Global Controller and Local Controllers have default security certificates, the Global Controller certificate will need to be exported to all the Local Controllers manually. And all Local Controllers certificates will need to be exported to Global Controller.

To install a Global Controller security certificate on to Local Controllers, follow these steps:

-
- Step 1** From the Global Controller, select **Admin > System Maintenance > Certificates**.
- Step 2** Highlight the certificate, and press **Ctrl+C** to copy it.

Figure 3-6 Copy the Global Controller Security Certificate

System Setup | System Maintenance | User Management | Oct 22, 2004 10:35:50 AM PDT

ADMIN | PN-MARS Global Controller: pnmars32 v3.1 Login: Global: Administrator (pnadmin) :: Logout :: Activate

Global Controller pnmars32 Certificate:

```

-----BEGIN CERTIFICATE-----
MIICrDCCAhUCBEFu9igwDQYJKoZIhvcNAQEEBQAwwZwwCzAJBgNVBAYTA1VTMRMwEQYDVQ
QIEwpsDzZ29uZXR3b3Jrcy5jb20wHhcNMDE0MjE1NjU2WhcNMDE0MjE1NjU2WjCB
DELMAKGA1UEBhMCVVMxEzARBgNVBAgTCkNhbmG1mb3JuaWEuXETAPBgNVBAcTCE1pbHBpdGFzMR0wGwYDVQ
QKEwRQcm90ZWdvIE51dHdvcmVzIE1uYzEkMCIGA1UECzMBTmV0d29yaYBTZW50MSAwH
gYDVQQDEXd3d3cucHJvdGVnb25ldHdvcmVzLmNvbTCBnzANBgkqhkiG9w0BAQFAA
OBjQAwGyKCyYEA0rmkOYZmHQIX9doxGM3sG3fIPoPlao22c8sFRKOnLUSfDHoXygW
IOZ4mZqwer9047FmwH55HXQVBoN85jJxpz+9OgOIY1xNiJwehJoa6DsDpmD3tRR9W9
ILX7g3wpzYw9a8BYTpMO8XpRLEnPYr4eHyP/u7OeqF1D+PGnHdghUCAwEAATANBgkqhkiG9w0BA
QQFAAOBgQB/rtrIFvCSNsJo
-----END CERTIFICATE-----

```

Export Instructions

Local Controllers:

| | Zone |
|--------------------------|------|
| <input type="checkbox"/> | LC31 |
| <input type="checkbox"/> | LC34 |

Back Add/Edit Certificate

- Step 3** Navigate to Local Controller **Admin > System Maintenance > Certificates**.
- Step 4** Paste the Global Controller certificate into the **Global Controller Certificate** box.
- Step 5** Repeat the process for all every Local Controller that the Global Controller is monitoring.

Figure 3-7 Apply the Global Controller Certificate to the Local Controller

System Setup | System Maintenance | User Management | Oct 22, 2004 10:35:50 AM PDT

ADMIN | PN-MARS Global Controller: pnmars32 v3.1 Login: Global: Administrator (pnadmin) :: Logout :: Activate

Global Controller Certificate:

```

-----BEGIN CERTIFICATE-----
MIICrDCCAhUCBEFu9igwDQYJKoZIhvcNAQEEBQAwwZwwCzAJBgNVBAYTA1VTMRMwEQYDVQ
QIEwpsDzZ29uZXR3b3Jrcy5jb20wHhcNMDE0MjE1NjU2WhcNMDE0MjE1NjU2WjCB
DELMAKGA1UEBhMCVVMxEzARBgNVBAgTCkNhbmG1mb3JuaWEuXETAPBgNVBAcTCE1pbHBpdGFzMR0wGwYDVQ
QKEwRQcm90ZWdvIE51dHdvcmVzIE1uYzEkMCIGA1UECzMBTmV0d29yaYBTZW50MSAwH
gYDVQQDEXd3d3cucHJvdGVnb25ldHdvcmVzLmNvbTCBnzANBgkqhkiG9w0BAQFAA
OBjQAwGyKCyYEA0rmkOYZmHQIX9doxGM3sG3fIPoPlao22c8sFRKOnLUSfDHoXygW
IOZ4mZqwer9047FmwH55HXQVBoN85jJxpz+9OgOIY1xNiJwehJoa6DsDpmD3tRR9W9
ILX7g3wpzYw9a8BYTpMO8XpRLEnPYr4eHyP/u7OeqF1D+PGnHdghUCAwEAATANBgkqhkiG9w0BA
QQFAAOBgQB/rtrIFvCSNsJo
-----END CERTIFICATE-----

```

Back Submit

To install a Local Controller security certificate on to the Global Controller, follow these steps:

- Step 1** From the Local Controller, select **Admin > System Maintenance > Certificates**.
- Step 2** Highlight the certificate and press **Ctrl+C** to copy it.

Figure 3-8 Copy the Local Controller Security Certificate

Step 3 From the Global Controller, select **Admin > System Maintenance > Certificates**.

Step 4 Select the specific zone from which this certificate was copied.

Figure 3-9 **Select the Appropriate Local Controller**

Local Controllers:

| | Zone |
|--------------------------|------|
| <input type="checkbox"/> | LC31 |
| <input type="checkbox"/> | LC34 |

[← Back](#) [Add/Edit Certificate](#)

Step 5 Paste the Local Controller certificate to the **Global Controller Certificate** box.

Step 6 Repeat the process from all Local Controllers that are monitored by this Global Controller.

System Setup

System Maintenance

User Management

Oct 22, 2004 10:41:16 AM PDT

ADMIN | PN-MARS Global Controller: pnmars32 v3.1 Login: Global: Administrator (pnadmin) :: Logout :: Activate

Local Controller LC31 Certificate:

-----BEGIN CERTIFICATE-----
MIICeDCCAhuCEBfUuwDQYJKoZIhvcNAQEEBQAwwGZmxwCzAJBgNVBAYTA1VTMRMWEQQYDVQQIEwpD
YWxpZm9ybmlhMREwDwYDVQQHEWhNaXxwaXRhcEEdMBsGA1UEChMUUHJvdGVnbvBOZXR3b3JrcyBJ
bmMxJDAlBgNVBAStTG05ldHdvcmVudWU2VjdwIydHkgRGVwYXNjbWVudDEGEGBA1UEAxMXd3d3LnBy
b3Rl229uZXR3b3Jrcy5jb20wHhcNMMDQxMDEMDAxNjQ0WHcNMTkxMDEyMDAxNjQ0WjCBNDLMAGK
A1UEBHMCMVVMezARBgNVBAgtCnNhbg1mb3JuaWEuXETAPBgNVBACTE1pbHBpdGFzMROwGwYDVQQK
ExRQcm90ZWdvIE5ldHdvcmVudWU2VjdwIzdHkgRGVwYXNjbWVudDEGEGBA1UEAxMXd3d3LnByb3Rl
ZW50MSAwHgYDVQQDExd3d3LnByb3RlZW5ldHdvcmVudWU2VjdwIzdHdvcmVudLmNvbTCBnzANBgqhkkiG9w0BAQEFAAOB
jQAwGykCgYEA07HrCqV1TiJhxSNBEJC0Y8zJIEyL+q4InQ2U4AmyPzOKfb6YnFwNt0h/28nlpBTc
j/OUSZBZYdrIeU+zSyob9AQfobWTKHU1zDZzaXZ1qcJDO4ksGcWMDTfm1uvB15sEXCPvvxzfoGuG
19moSrBGX6aRnpwBQyaD6/5jWqKTN8CAweAATANBgqhkkiG9w0BAQQFAAOBggCA2IxSWSCA1T/8

Back

Submit

The various Local Controllers send summarized information to the Global Controller, which in turn compiles and collates it. There may be a reason you want to suspend, or temporarily hold back, information being sent from one of the Local Controllers. For example, if several of the Local Controller zones are compromised and sending many events at once, you may want to focus on isolating problems on one Local Controller at a time.

- Step 1** In the Zone Controller Information page, select the Local Controller you want to suspend.
- Step 2** Click the **Suspend/Resume** button.

Follow the same procedure to resume output from the affected Local Controller.

Before configuring the Global Controller to recognize reporting devices, be aware of the levels of operation supported by a Local Controller. To learn more about the levels of operation for the Local Controller s, see [Levels of Operation, page 3-1](#) in the *User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x*

Adding Reporting Devices

After you have added the Global Controller's configuration information and rebooted it, you need to configure the third-party devices that report to the Global Controller. All of the event information that passes through these devices is distilled down and sessionized to the information that the Global Controller presents to you. The more information that you can provide for these devices, the clearer the picture you'll get when using the Global Controller.



Note

For a list of devices supported by the Global Controller, see the [Configuring Supported Devices, page 3-16](#).

Manual Configuration

In general, you have two choices for adding devices that you want to monitor into your Global Controller. You can create a seed file or you can add each device manually. Seed file support is limited to a few device types; see [Configuring Supported Devices, page 3-16](#).

When manually configuring devices, select the devices that are most interesting to you. Once added, you can come back and edit them as necessary. Manual configuration is also useful when you add or change a single security device on your network. See [Configuring Supported Devices, page 3-16](#) for more information about configuring individual devices.



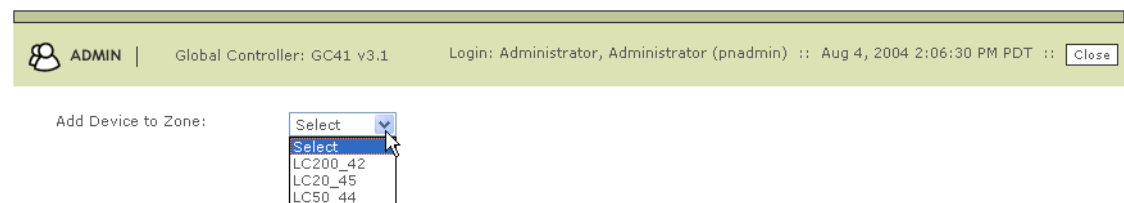
Note

Remember that you do not have to add all of the devices configuration information at once. You can start by adding the device's name and its access IP address. You can always return later, when the Global Controller starts to report to you, and provide more details.

Add a Device Manually

Step 1 Click **Admin > Security and Monitor Devices > Add**.

Figure 3-11 *Selecting the Local Controller Zone*




Step 2 Select the Local Controller **Zone** from the pull-down menu. This determines which Local Controller monitors the device. *You are then automatically logged into the Local Controller you have selected. A pop-up window appears.*

Figure 3-12 Entering the Device on the Local Controller

Note:

1. Enter the reporting IP (the IP address where events originated from) to ensure that the system processes the events.
2. * denotes a required field.

Device Type: 

→ *Device Name:

→ *Reporting IP:

Step 3 Select the device from the pull-down menu.

Step 4 Enter the information needed to communicate with the device.

Step 5 Click the **Submit** button.

Newly added devices on the Local Controller are automatically discovered by the Global Controller.

For more information on installing individual devices, see [Preparing to Add and Discover Devices](#), page 3-15.

Configuring Supported Devices

For most of the security and monitoring devices that you have report to Global Controller, set up and configuration is three-part. You need to:

- Open communication channels to the device.
- Add the appropriate communication information to the Global Controller.
- Make sure that firewalls and routers sitting between the Global Controller and the reporting device are configured to let event traffic pass.

For devices that use agents, modules, or sensors, you need to perform a couple of extra steps.

L2 Discovery and Mitigation

For information on L2 device discovery and mitigation, see [Layer 2 Discovery and Mitigation](#), page 3-32 in the *User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x*.



CHAPTER 4

Performing Command Line Administration Tasks

Revised: August 28, 2008, OL-16776-01

This chapter describes details basic administrative tasks that you perform using a console connection to the MARS Appliance.

This chapter contains the following procedures:

- [Log In to the Appliance via the Console, page 4-1](#)
- [Reset the Appliance Administrator Password, page 4-2](#)
- [Shut Down the Appliance via the Console, page 4-3](#)
- [Log Off the Appliance via the Console, page 4-3](#)
- [Reboot the Appliance via the Console, page 4-4](#)
- [Determine the Status of Appliance Services via the Console, page 4-4](#)
- [Stop Appliance Services via the Console, page 4-6](#)
- [Start Appliance Services via the Console, page 4-6](#)
- [View System Logs via the Console, page 4-7](#)

For other MARS Appliance configuration and administration tasks, see the document roadmap for this release: [Cisco Security MARS Documentation Guide and Warranty](#).

Log In to the Appliance via the Console

After the MARS Appliance boots, the console service starts and prompts the user to log in. Successful login launches a command line application (shell) that operates the CLI.

To log in to the MARS Appliance via a console connection, follow these steps:

-
- Step 1** Establish a console connection to the MARS Appliance. For options and details, see [Establishing a Console Connection, page 2-4](#).
- Step 2** At the `login:` prompt, enter the MARS Appliance administrator name.
- Step 3** At the `password:` prompt, enter the MARS Appliance password.

Result: The system prompt appears in the following form:

```
Last login: Tue Jul  5 05:57:31 2005 from <host>.<domain>.com
```

```
Cisco Security MARS - Mitigation and Response System
```

? for list of commands

[pnadmin]\$



Note

There is only one set of MARS Appliance login credentials (administrator name and password) that have the console connection privilege.



Tip

To exit the console connection, enter **exit** at the command prompt.

Reset the Appliance Administrator Password

There is always a single set of MARS Appliance administrator credentials consisting of the administrator name *pnadmin* and a corresponding password. Unlike other MARS administrative accounts, this unique administrative account is granted all privileges and cannot be deleted.

This procedure details how to reset the password after you log in with the existing credentials. If you do not have the existing MARS Appliance administrator login credentials with which to log in, the only method of recovery is to re-image the appliance, which resets the password to the factory defaults. For information on resetting the administrator login and password without first logging in, see [Recovery Management, page 6-16](#).

To reset the MARS Appliance administrator login credentials, follow these steps:

Step 1 Log in to the MARS Appliance. For more information, see [Log In to the Appliance via the Console, page 4-1](#).

Step 2 At the system prompt, type **passwd** and then press **Enter**.

Result: The MARS Appliance displays the following prompt:

New password:

Step 3 Type the new password, and then press **Enter**.



Note

The new password should not contain the administrator account name, must contain a minimum of 6 characters, and it should include at least 3 character types (numerals, special characters, upper case letters, and lowercase letters). Each of the following examples is acceptable: 1PaSsWoRd, *password44, Pass*word.

The MARS Appliance displays the following prompt:

Retype new password

Step 4 Type the new password again, and then press **Enter**.

Result: The MARS Appliance displays the command prompt, and the password is changed.

Shut Down the Appliance via the Console

You can shut down an appliance remotely via a console connection. However, to power up the appliance, you must have physical access to the device.

**Caution**

Powering off the MARS Appliance by using only the power switch may cause the loss or corruption of data. Use this procedure to shut down the MARS Appliance.

Summary Steps**1. shutdown**

To use the console to shut down 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, page 4-1](#).

Step 2 At the system prompt, type **shutdown**, and then press **Enter**.

Result: The following message appears and the MARS Appliance powers off.

```
[pnadmin]$ shutdown
```

```
Broadcast message from root (pts/0) (Fri Mar 28 14:38:54 2008):
```

```
The system is going down for system halt NOW!
```

```
[pnadmin]$ Last login: Fri Mar 28 14:59:11 2008
```

Log Off the Appliance via the Console

Logging off via the console closes the administrative session at the appliance. Good security practices recommend logging off when you are not using the console.

Summary Steps**1. exit**

To log off the MARS Appliance via the console, follow these steps:

Step 1 At the system prompt, type **exit**.

Step 2 Press **Enter**.

Result: The console connection closes, and the `login:` prompt reappears.

Reboot the Appliance via the Console

From time to time, you may need to manually reboot the appliance. For example, if a service seems to be hung, rebooting may resolve the issue. Rebooting ensures that the services are shut down safely before the appliance restarts.

Summary Steps**1. reboot**

To reboot the MARS Appliance via the console, follow these steps:

Step 1 Log in to the MARS Appliance. For more information, see [Log In to the Appliance via the Console, page 4-1](#).

Step 2 At the system prompt, type **reboot**, and then press **Enter**.

Result: The MARS Appliance displays the following message:

```
[pnadmin]$ reboot
```

```
Broadcast message from root (pts/0) (Fri Mar 28 15:33:31 2008):
```

```
The system is going down for reboot NOW!
```

```
[pnadmin]$
```

The MARS Appliance reboots. When the reboot is finished, the `login:` prompt reappears.

Determine the Status of Appliance Services via the Console

You can use the console connection to obtain system and service status information.

Summary Steps**1. pnstatus****Detailed Steps**

To determine the status of the MARS Appliance's services, follow these steps:

Step 1 Log in to the MARS Appliance. For more information, see [Log In to the Appliance via the Console, page 4-1](#).

Step 2 At the system prompt, type **pnstatus**, and then press **Enter**.

The system displays list of services and status information. Possible states are:

- **RUNNING.** The service is operational.
- **STOPPED.** The service is not running.

**Note**

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

Examples

The expected results for **pnstatus** run on a Global Controller:

```
Last login: Tue Jul 15 08:39:14 2008 from <hostname>
```

CS MARS - Mitigation and Response System

? for list of commands

```
[pnadmin]$ pnstatus
```

| Module | State | Uptime |
|-----------------------|---------|-------------|
| DbIncidentLoaderSrv | STOPPED | |
| KeywordQuerySrv | STOPPED | |
| autoupdate | RUNNING | 11-03:47:01 |
| csdam | STOPPED | |
| csiosips | STOPPED | |
| csips | STOPPED | |
| cswin | STOPPED | |
| device_monitor | STOPPED | |
| discover | STOPPED | |
| graphgen | RUNNING | 10:20:31 |
| pnarchiver | RUNNING | 11-03:47:02 |
| pndbpurger | STOPPED | |
| pnesloader | STOPPED | |
| pnmac | STOPPED | |
| pnparser | STOPPED | |
| process_event_srv | STOPPED | |
| process_inlinerep_srv | STOPPED | |
| process_postfire_srv | STOPPED | |
| process_query_srv | STOPPED | |
| securesyslog | RUNNING | 11-03:47:02 |
| superV | RUNNING | 11-03:47:02 |

The expected results for **pnstatus** run on a Local Controller:

Last login: Tue Jul 15 08:11:56 2008 from <hostname>

CS MARS - Mitigation and Response System

? for list of commands

```
[pnadmin]$ pnstatus
```

| Module | State | Uptime |
|-----------------------|---------|-------------|
| DbIncidentLoaderSrv | RUNNING | 41-19:20:54 |
| KeywordQuerySrv | RUNNING | 41-19:20:54 |
| autoupdate | RUNNING | 41-19:20:54 |
| csdam | RUNNING | 41-19:20:54 |
| csiosips | RUNNING | 41-19:20:54 |
| csips | RUNNING | 41-19:20:54 |
| cswin | RUNNING | 41-19:20:54 |
| device_monitor | RUNNING | 41-19:20:54 |
| discover | RUNNING | 41-19:20:54 |
| graphgen | RUNNING | 10:17:26 |
| pnarchiver | RUNNING | 3-08:19:55 |
| pndbpurger | RUNNING | 41-19:20:54 |
| pnesloader | RUNNING | 41-19:20:54 |
| pnmac | RUNNING | 41-19:20:54 |
| pnparser | RUNNING | 22:01:45 |
| process_event_srv | RUNNING | 41-19:20:54 |
| process_inlinerep_srv | RUNNING | 41-19:20:54 |
| process_postfire_srv | RUNNING | 41-19:20:54 |
| process_query_srv | RUNNING | 41-19:20:54 |
| securesyslog | RUNNING | 41-19:20:54 |
| superV | RUNNING | 41-19:20:55 |

Stop Appliance Services via the Console

You can stop all MARS Appliance services from the console. To list the services and their status, you can use the **pnstatus** command. For more information, see [Determine the Status of Appliance Services via the Console, page 4-4](#).

To stop all services on 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, page 4-1](#).
 - Step 2** Type **pnstop**.
 - Step 3** Press **Enter**.

Result: The system immediately shows the message:

```
Please Wait . . .
```

Followed by the return of the prompt, indicating the command has completed.

- Step 4** To verify the status of the services, enter **pnstatus**.
The superV service does not stop. This service monitors and restarts the other services as needed.
-

Start Appliance Services via the Console

If the services are stopped, you can manually start all MARS Appliance services from the console. To list the services and their status, you can use the **pnstatus** command. For more information, see [Determine the Status of Appliance Services via the Console, page 4-4](#).

Summary Steps

1. **pnstart**

To start all stopped MARS services, follow these steps:

-
- Step 1** Log in to the MARS Appliance. For more information, see [Log In to the Appliance via the Console, page 4-1](#).
 - Step 2** Type **pnstart**.
 - Step 3** Press **Enter**.
Result: The system prompt disappears and then returns, indicating the services are restarted.
 - Step 4** To verify the status of the services, enter **pnstatus**.
-

View System Logs via the Console

This section details the procedure for running the **pnlog show** command. This command displays the log status and can be used by support personnel for analysis.

For more information on the **pnlog** command, see [pnlog show, page 1-53](#). The syntax for the **pnlog show** command is as follows:

```
pnlog show <gui|backend|cpdebug>
```

These options do a running output of a particular log file in the backend. There are three different logs that you can view: the web interface logs, the backend logs (shows logs for processes that the **pnstatus** command reports on), and CheckPoint debug logs. Use Ctrl+C or ^C to stop this command.

When using **cpdebug**, you should have **pnlog setlevel** set to more than 0, which is the default value and turns off the CPE Debug messages.

To generate a .cab file of log and system Registry information, follow these steps:

-
- | | |
|---------------|---|
| Step 1 | Log in to the MARS Appliance. For more information, see Log In to the Appliance via the Console, page 4-1 . |
| Step 2 | Type pnlog show and the appropriate argument. |
| Step 3 | Press Enter . <i>Result:</i> The console begins scrolling the output of the executed command. |
| Step 4 | To stop the output at any time, press Ctrl+C . <i>Result:</i> The system returns to the system prompt. |
-

Determining the Version Running on an Appliance

Before you upgrade an appliance, you must determine the version you are running. You can determine this in one of two ways:

- **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.

The format of the version appears as **x.y.z (build_number) data_version**, for example, **6.0.1 (2992) 30**.

Result: You have identified the version running on your appliance and know whether you must contact Cisco support or continue with this checklist.



CHAPTER 5

Upgrade Management

Revised: September 5, 2008, 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 5-21](#)

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 product and data package whether running a standalone Local Controller or managing a set of Local Controller via 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 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.
2. 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.
3. 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 6-16. <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>3.4.1 (1922)</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>4. Determine the medium for upgrading.</p> <p>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 style="list-style-type: none"> • 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. • 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. • 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>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><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>For more information, see:</p> <ul style="list-style-type: none"> • Download the Upgrade Package from Cisco.com, page 5-19 • Burn an Upgrade CD-ROM, page 5-18 • Prepare the Internal Upgrade Server, page 5-19 • Specify Download Sever Settings, page 5-11 • Select an Upgrade Package for a MARS Appliance (local), page 5-13 • 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 either a proxy server or a direct connection to the Internal Upgrade Server or 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 provide them at the command line during 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 5-21 • 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)

Detailed Steps

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 checklist.

Related Documents

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

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 pages 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/ld"/> The system periodically checks this location for a new package catalog.</p> <p>Package Polling Interval: <div> <div>NEVER</div> <div> NEVER Every 1 hour Every 2 hours Every 3 hours Every 6 hours Every 12 hours Every day Every 2 days Every 3 days Every 4 days Every 5 days Every 6 days Every 7 days Every 8 days Every 9 days Every 10 days Every 11 days Every 12 days Every 13 days Every 14 days </div> </div> Indicates how often the Catalog polling URL is checked.</p> <p><input type="button" value="Save Changes"/></p> | | | |

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 Server 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 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 | <div></div> |

Install

Upgrade Status Logs

| 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 proxy information is not provided and you attempt to download an upgrade for that appliance, the MARS Appliance attempts to connect to Internal Upgrade Server and 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> <div> <input type="button" value="Import Package"/> <input type="button" value="Delete"/> <input type="button" value="View Release Notes"/> </div> <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.

Close Import View Release Notes

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 | <div></div> |
| <input type="checkbox"/> | LC-26 | 10.89.178.26 | Active | 6.0.1 | <div></div> |

Install

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 |

☐ Install Now
 ☐ Schedule Install

Today
 02/20/08
 1:30 AM

Cancel
 Submit

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

The Internal Upgrade Server requirements vary based on the upgrade option you selected and the version running on your appliance.

**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 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.

For CLI-based upgrades of version 2.5.1 or later, the Internal Upgrade Server must be configured to meet the following requirements:

- Be an FTP, HTTP, or HTTPS server
- Require user authentication
- Accept connections from the MARS Appliance
- Connections pass through a proxy server that also uses authentication

For web interface-based upgrades of releases 3.4.1 or later, the Internal Upgrade Server must be configured to meet the following requirements:

- Be an HTTPS or FTP server
- Require user authentication
- Accept connections from the MARS Appliance
- Connections pass through a proxy server that also uses authentication. In addition, the proxy server setting must be configured in the web interface before the upgrade.

Download the Upgrade Package from Cisco.com

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

- Top-level page: <http://www.cisco.com/cgi-bin/tablebuild.pl?topic=279644034>
- Upgrade files: <http://www.cisco.com/cgi-bin/tablebuild.pl/cs-mars>
- Recovery images: <http://www.cisco.com/cgi-bin/tablebuild.pl/cs-mars-recovery>
- Supporting files: <http://www.cisco.com/cgi-bin/tablebuild.pl/cs-mars-misc>

**Note**

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

For information on obtaining a Cisco.com 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 specify the proxy settings. This procedure describes how to specify the proxy settings with the assumption that you will upgrade the appliance from the user interface associated with that appliance. 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:

10

1

1

23

Proxy Port:

8080

Proxy User:

user

Proxy Password:

Back

Clear Settings

Submit

132536

- 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** 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. MARS requires that proxy servers enforce inline user authentication. Therefore, you must specify a username and password pair to authenticate to the proxy server.

- Step 5** In the Proxy Password field, specify the password associated with the username you just provided.
- Step 6** Click **Submit** to save your changes.

Upgrade from the CLI

You can connect to the Internal Upgrade Server and complete the upgrade using HTTP or HTTPS, or you can download the upgrade package onto an FTP server and perform the upgrade. For more information on the upgrade command, see [pnupgrade, page 1-64](#).

To upgrade using the CLI, follow these steps:

-
- Step 1** Log in to the appliance via the console port or SSH connection.
- Step 2** Enter your MARS login name and password.
- Step 3** To verify that the appliance is running the prerequisite version, run the CLI command:

```
version
```

The appliance must be running the supported prerequisite version. If it is not, you must follow the upgrade path to reach that version.

- Step 4** Do one of the following:



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 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, run the CLI command:

```
pnupgrade cdrom://package/pn-ver.pkg
```

Where *package* is the path on the CD where you have stored the *.pkg file and where *[ver]* is the version number of the package file to which you want to upgrade, such as 3.3.4.

- To upgrade from an internal HTTP or HTTPS server, run the CLI command:

```
pnupgrade https://upgrade.myhttpserver.com/upgrade/packages/  
pn-ver.pkg [user] [password]
```

— or —

```
pnupgrade http://upgrade.myhttpserver.com/upgrade/packages/  
pn-ver.pkg [user] [password]
```

Where *upgrade.myhttpserver.com/upgrade/packages* is the server name and path where you have downloaded the other *.pkg file, and where *ver* is the version number, such as 3.3.4, and *[user]* and *[password]* are your Internal Upgrade Server login name and password.

- To upgrade from your FTP server after you have downloaded the file, run the CLI command:

```
pnupgrade ftp://upgrade.myftpserver.com/upgrade/packages/  
pn-ver.pkg [user] [password]
```

Where *upgrade.myftpserver.com/upgrade/packages* is the server name and path where you have downloaded the other *.pkg file, and where *[ver]* is the version number, such as 3.3.4, *[user]* and *[password]* are your Internal Upgrade Server login name and password.

- To upgrade from the Internal Upgrade Server through a proxy server, run the CLI command:

```
pnupgrade proxyServerIP:proxyServerPort [proxyUser:proxyPassword]  
https://upgrade.myhttpserver.com/upgrade/packages/pn-ver.pkg [user] [password]
```

Where the variables are defined as follows:

- `proxyServerIP:proxyServerPort` identifies the IP address/port pair that connects to the proxy server residing between your appliance and the Internal Upgrade Server.
- `proxyUser:proxyPassword` identifies the username and password pair required for the appliance to authenticate to the proxy server.
- `upgrade.myttppserver.com/upgrade/packages` is the server name and path where you have downloaded the *.pkg file.
- `ver` is the version number, such as 3.3.4.
- `[user]` and `[password]` are 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.



CHAPTER 6

Backup, Recover, Restore, and Standby Server Options

Revised: September 3, 2008, OL-16776-01

This chapter describes the backup and recovery components of MARS, as well as how to configure a secondary standby server.

- [Configuring and Performing Appliance Data Backups, page 6-1](#)
- [Recovery Management, page 6-16](#)
- [Configuring a Standby or Secondary MARS Appliance, page 6-22](#)
- [Guidelines for Restoring, page 6-23](#)
- [Configure the Cygwin SFTP Server on Windows, page 6-11](#)

Configuring and Performing Appliance Data Backups

You can archive data from a MARS Appliance and use that data to restore the operating system (OS), system configuration settings, dynamic data (event data), or the complete system. The appliance archives and restores data to and from an external network-attached storage (NAS) system using the network file system (NFS) or Secure FTP (SFTP) protocols. While you cannot schedule when the data backup occurs, the MARS Appliance performs a configuration backup every morning at 2:00 a.m. and events are archived every hour. The configuration backup can take several hours to complete.

When archiving is enabled, dynamic data is written twice: once to the local database and once to the archive server. As such, the dynamic data that is archived includes only the data that is received or generated *after* you enable the data archive setting. Therefore, we recommend that you enable archiving before configuring your appliance to receive audit events from reporting devices.

You can use the same server to archive the data for more than one MARS Appliance; however, you must specify a unique directory in the path for each appliance that you want archive. If you use the same base directory, the appliances overwrite each others' data, effectively corrupting the images.



Note

For the complete list of supported NFS and SFTP servers, see:

- http://www.cisco.com/en/US/products/ps6241/products_device_support_tables_list.html

Each MARS Appliance seamlessly archives data using an expiration date that you specify. When the MARS internal storage reaches capacity, it automatically purges the data in the oldest partition of the local database, roughly 10% of the stored event and session data. The data in the NFS or SFTP file share has a life span specified in days. Therefore, to keep a year's worth of data, you would specify 365 days as the value for the Remote Storage Capacity (in Days) field. All data older than 365 days is purged from the archive file.

When planning for space requirements, use the following guidance: Estimate 6 GB of storage space for one year's worth of data, received at a sustained 10 events/second. This estimate assumes an average of 200 Bytes/event and a compression factor of 10, both realistic mean values. In addition to capacity planning, plan the placement of your archive server to ensure a reliable network connection that can transmit 10 MB/second exists between the archive server and the MARS Appliance. You should consider using the eth1 interface to avoid high-traffic networks that might introduce latency and to ensure that the backup operation is not competing with other operations in the MARS Appliance. Also, define a default route to the archive server on the MARS Appliance and that you verify any intermediate routers and firewalls allow for multi-hour NFS or SFTP connections to prevent session timeouts during the backup operation.

**Note**

Data archiving is local to a given appliance. When you configure data archiving on a Global Controller, you are archiving the data for that appliance; you cannot configure the Global Controller to archive data from Local Controllers that it monitors.

For more information on the uses and format of the archived data, see the following topics:

- [Typical Uses of the Archived Data, page 6-2](#)
- [Format of the Archive Share Files, page 6-3](#)
- [Archive Intervals By Data Type, page 6-4](#)
- [Guidelines for Restoring, page 6-23](#)
- [pnrestore, page 1-57](#)

To configure data archiving, you must perform the following procedures:

1. Configure the NFS server or SFTP server
 - [Configure the NFS Server on Windows, page 6-5](#)
 - [Configure the NFS Server on Linux, page 6-9](#)
 - [Configure the NetApp NFS Server, page 6-9](#)
 - [Configure the Cygwin SFTP Server on Windows, page 6-11](#)
2. (NFS only) [Configure Lookup Information for the NFS Server, page 6-11](#)
3. [Configure the Data Archive Setting for the MARS Appliance, page 6-13](#)

Typical Uses of the Archived Data

While the primary use of an archive is to restore the appliance in response to a catastrophic software failure, the archived data provides the following alternate uses:

- Use **Admin > System Maintenance > Retrieve Raw Messages** to analyze historical raw messages from periods that exceed the capacity of the local database. The data returned from raw message retrieval is simply the audit message provided by the reporting device. The raw message is just the message as sent by the reporting device, such as a syslog message. For more information, see [Retrieving Raw Messages, page 12-3](#).
- Manually view the archived event records, which are compressed using gzip. Viewing the data in this manner is faster than retrieving raw messages from either the local database or the archive. However, the record format is more complicated than the simple raw event returned by the Retrieve Raw Messages operation. It includes all the data necessary to restore the incidents and dependent data, including the raw message and the system data required to correlate that message with the session, device type, five tuple (source IP, destination IP, protocol, source port, and destination port), and all other data points. For more information, see [Format of the Archive Share Files, page 6-3](#) and [Access the Data Within an Archived File, page 6-15](#).
- Image a standby or secondary MARS Appliance to either swap into the network in the event of a hardware failure or to access full query and report features for historical time periods. For more information, see [Configuring a Standby or Secondary MARS Appliance, page 6-22](#), and [Guidelines for Restoring, page 6-23](#).

Format of the Archive Share Files

The MARS archive process runs daily at 2:00 a.m., and it creates a dated directory for its data. You cannot specify a different time to archive the data.

The `pnos` directory is where the operating system backup is stored.

```
06/12/2005 11:32p <DIR> .
06/12/2005 11:32p <DIR> ..
07/09/2005 01:30a <DIR> pnos      <-- OS Backup Directory
07/08/2005 04:49p <DIR> 2005-07-08<-- Daily Data Backup Directory
07/10/2005 12:09a <DIR> 2005-07-10
07/11/2005 12:12a <DIR> 2005-07-11
07/12/2005 12:12a <DIR> 2005-07-12
07/13/2005 12:16a <DIR> 2005-07-13
07/14/2005 02:02a <DIR> 2005-07-14
07/15/2005 02:02a <DIR> 2005-07-15
07/16/2005 02:02a <DIR> 2005-07-16
07/17/2005 02:02a <DIR> 2005-07-17
07/18/2005 02:02a <DIR> 2005-07-18
07/19/2005 02:02a <DIR> 2005-07-19
07/19/2005 09:46p <DIR> 2005-05-26
07/20/2005 07:16a <DIR> 2005-05-27
07/20/2005 07:17a <DIR> 2005-07-20
07/22/2005 12:13a <DIR> 2005-07-22
07/21/2005 12:09a <DIR> 2005-07-21
07/23/2005 12:15a <DIR> 2005-07-23
      0 File(s)          0 bytes
     58 Dir(s)    4,664,180,736 bytes free
```

Within each daily directory, subdirectories are created for each data type. The following example identifies the directory type in the comments.

Directory of D:\MARSBackups\2005-07-08

```
07/08/2005 04:49p <DIR> .
07/08/2005 04:49p <DIR> ..
07/08/2005 04:49p <DIR> CF<-- Configuration Data
07/08/2005 05:00p <DIR> IN<-- Incident Data
07/08/2005 05:16p <DIR> AL<-- Audit Logs
```

```

07/08/2005 05:16p      <DIR>          ST<-- Statistics Data
07/08/2005 05:16p      <DIR>          RR<-- Report Results
07/08/2005 05:49p      <DIR>          ES<-- Raw Event Data
          0 File(s)          0 bytes
          8 Dir(s)    4,664,180,736 bytes free

```

The .gz filename in the raw event data directory identifies the period of time that the archived data spans in a YYYY-MM-DD-HH-MM-SS format. The filename includes the following data [dbversion]-[productversion]-[serialno]_[StartTime]_[EndTime].gz. The following examples illustrate this format:

```

ix-5248-524-1171238692_2007-02-12-00-04-46_2007-02-12-01-04-51.gz
rm-5248-524-1171238692_2007-02-12-00-04-46_2007-02-12-01-04-51.gz

```

**Note**

Files starting with “ix” are index files and those starting with “rm” contain the raw messages.

Directory of D:\MARSSBackups\2005-07-08\ES

```

07/08/2005 05:49p      <DIR>          .
07/08/2005 05:49p      <DIR>          ..
07/08/2005 05:49p          34,861 es-3412-342_2005-07-08-16-49-52_2005-07-08-17-49-47.gz
07/08/2005 05:49p          31,828 rm-3412-342_2005-07-08-16-49-52_2005-07-08-17-49-47.gz
07/08/2005 06:49p          49,757 es-3412-342_2005-07-08-17-49-49_2005-07-08-18-49-40.gz
07/08/2005 06:49p          48,154 rm-3412-342_2005-07-08-17-49-49_2005-07-08-18-49-40.gz
07/08/2005 07:49p          24,420 es-3412-342_2005-07-08-18-49-45_2005-07-08-19-49-52.gz
07/08/2005 07:49p          22,346 rm-3412-342_2005-07-08-18-49-45_2005-07-08-19-49-52.gz
07/08/2005 08:50p          44,839 es-3412-342_2005-07-08-19-49-47_2005-07-08-20-50-04.gz
07/08/2005 08:50p          41,534 rm-3412-342_2005-07-08-19-49-47_2005-07-08-20-50-04.gz
07/08/2005 09:50p          58,988 es-3412-342_2005-07-08-20-49-55_2005-07-08-21-50-06.gz
07/08/2005 09:50p          54,463 rm-3412-342_2005-07-08-20-49-55_2005-07-08-21-50-06.gz
07/08/2005 10:50p         130,604 es-3412-342_2005-07-08-21-49-58_2005-07-08-22-50-08.gz
07/08/2005 10:50p          85,437 rm-3412-342_2005-07-08-21-49-58_2005-07-08-22-50-08.gz
07/08/2005 11:50p         114,445 es-3412-342_2005-07-08-22-49-55_2005-07-08-23-50-10.gz
07/08/2005 11:50p          58,240 rm-3412-342_2005-07-08-22-49-55_2005-07-08-23-50-10.gz
07/09/2005 12:50a        110,556 es-3412-342_2005-07-08-23-50-02_2005-07-09-00-50-14.gz
07/09/2005 12:50a          53,977 rm-3412-342_2005-07-08-23-50-02_2005-07-09-00-50-14.gz
          16 File(s)          964,449 bytes
          2 Dir(s)    4,664,164,352 bytes free

```

The following is an example of the data found in the configuration data directory.

Directory of D:\MARSSBackups\2005-07-08\CF

```

07/08/2005 04:49p      <DIR>          .
07/08/2005 04:49p      <DIR>          ..
07/08/2005 02:02a          2,575,471 cf_2005-07-08-02-02-02.pna
          1 File(s)          2,575,471 bytes
          2 Dir(s)    4,664,164,352 bytes free

```

Archive Intervals By Data Type

MARS archives data either daily or in near real time based on the type of data. Therefore, all the data in the MARS internal storage (local database) should be in the archive server storage as well, give or take a day's worth of specific types of data.

MARS data consists of four types:

1. configuration data, such as topology and device settings, which is archived daily

2. audit trails of MARS web interface activity and MARS report results, which are archived daily
3. MARS statistics, such as charts in Summary/Dashboard, which are archived hourly
4. dynamic and event data, such as events, sessions, and incidents, which are archived quickly so they do not tax the MARS Appliance's local storage.

Configuration data, audit trails, and static data is written to database first. During archival time, data is written to local files and archived from those files. However, dynamic and event data is written in parallel to both the database and to local files. Therefore, even if the data has been archived, it is likely to still be in the database.

In other words, dynamic and event data is initially stored in two locations: the archive server and MARS database. Later, when the MARS database partition becomes full, the database purge operation occurs to make room for new events—but those events and incidents were archived prior to the purge operation.

**Note**

Once data is purged from the MARS local database, it can not be queried. Queries and reports operate only on the data in the MARS database.

To account for temporarily unavailable archive servers, the files for all data types are stored locally on the MARS Appliance for one day before they are purged. When you enable archiving in the web interface, you must also define the parameters for retaining the data in the archive server. As a result, MARS performs simple data maintenance on the archive server by purging data outside the range specified in the Remote storage capacity in Days field of the Data Archiving page. For example, the storage capacity value is 365 days, then all data older than one year is purged from the archive server.

Refer to [Table 6-1](#) for the archive interval for each type of data.

Table 6-1 *Archive Interval Description(4.3.1 and 5.2.4 and later)*

| Archive Folder and Data Type Description | Archive Interval | Max. Interval (in minutes) | Schedule |
|---|--|----------------------------|-----------------|
| AL: Audit log information | Once per day at 2:00 a.m. | n/a | Daily at 2 a.m. |
| CF: Configuration information | Once per day at 2:00 a.m. | n/a | Daily at 2 a.m. |
| ES: Events, sessions, and raw messages | Every 10 minutes or when 3 MB (compressed) file size is reached, whichever threshold is met first. | 10 minutes | n/a |
| IN: Incidents | Immediately | 1 minute ¹ | n/a |
| RR: Report results | Once per day at 2:00 a.m. | | n/a |
| ST: Statistical data/counters information | Hourly. | | n/a |

1. If event rate is higher, archive interval for real time can be shorter than Max Interval.

Configure the NFS Server on Windows

Windows Services for UNIX (WSU) allows an NFS mount to be created on a Windows file server. This option is convenient and is often useful in a lab environments or when UNIX expertise is unavailable. The following URLs support the configuration of this complimentary download from Microsoft Corporation:

Windows Services for UNIX 3.5 Download

<http://www.microsoft.com/windowsserversystem/sfu/downloads/default.msp>

System Requirements for WSU 3.5

<http://www.microsoft.com/windowsserversystem/sfu/productinfo/sysreqs/default.msp>

Microsoft Windows Services for UNIX 3.5 Reviewer's Guide

<http://www.microsoft.com/windowsserversystem/sfu/techinfo/revguide.msp>

Performance Tuning Guidelines for Microsoft Services for Network File System

<http://www.microsoft.com/technet/interopmigration/unix/sfu/perfnfs.msp>

To install and configure the WSU 3.5 to operate with a MARS Appliance, perform the following tasks:

- [Install Windows Services for UNIX 3.5, page 6-6](#)
- [Configure a Share using Windows Services for UNIX 3.5, page 6-7](#)

Install Windows Services for UNIX 3.5

To configure the NFS server on a Windows server, follow these steps:

-
- Step 1** Log in to the Windows server using an account with either local or domain-level administrative privileges.



Note If you install the services using an account without administrative privileges, the archive process fails.

- Step 2** Download the Windows Services for UNIX 3.5.
- Step 3** To install the Windows Services for UNIX, double-click **SFU35SEL_EN.exe**.
- Step 4** Enter the folder where the program files should be extracted in the Unzip to folder field, and click **Unzip**.
We recommend defining a new folder, not using the temp folder under the local profile. The unzip process can take several minutes.
- Step 5** Open the folder where you extracted the files, and double-click **SfuSetup.msi**.
- Step 6** Click **Next** to continue.
The Customer Information panel appears.
- Step 7** Enter values for the User name and Organization fields, and click **Next**.
The License and Support Information panel appears.
- Step 8** Select the **I accept the agreement** option, and click **Next**.
- Step 9** Select the **Custom Installation** option, and click **Next**.
- Step 10** At a minimum, you must select **Entire feature (including any subfeatures if any) will be installed on local hard drive** for the following components Under Windows Services for UNIX in the Components list, and then click **Next**:
- **NFS** (This option includes the Client for NFS and Server for NFS subfeatures.)
 - **Authentication tools for NFS** (This option includes the User Name Mapping, Server for NFS Authentication, and Server for PCNFS subfeatures.)

**Note**

This procedure assumes that you have selected **Entire feature will not be available** for all components other than NFS and Authentication tools for NFS.

The Security Settings panel appears.

- Step 11** Verify that the Change the default behavior to case sensitive check box is *not selected*, and then click **Next**.

As the MARS Appliance does not use a special account for NFS authentication, you do not need to change the default settings.

- Step 12** The User Name Mapping panel appears.

- Step 13** Verify that the Local User Name Mapping Server and Network Information Service (NIS) options are selected, and then click **Next**.

A second User Name Mapping panel appears.

- Step 14** Enter values for the following fields, and then click **Next**:

- **Windows domain name.** We recommend accepting the default value, which is the local host name.
- (Optional) **NIS domain name**
- (Optional) **NIS server name**

The Installation Location panel appears.

- Step 15** Enter the desired installation location and click **Next**.

The Installing panel appears, presenting the progress of the installation. When the installation completes, the Completing the Microsoft Windows Services for UNIX Setup Wizard panel appears.

- Step 16** Click **Finish** to complete the installation and close the Setup Wizard.

- Step 17** Reboot the computer.

You have successfully installed the required NFS components. Now you must define and configure a share to be used by the MARS Appliance for backups and archiving. For more information, see [Configure a Share using Windows Services for UNIX 3.5, page 6-7](#).

Configure a Share using Windows Services for UNIX 3.5

Configuring the share involves identifying the folder to share and specifying the correct permissions and access.

To configure WSU 3.5 as an NFS server for a MARS Appliance, follow these steps:

- Step 1** Start Windows Explorer on the Window host where you installed WSU 3.5.

- Step 2** Create the folder where you want the MARS archives to be stored.

An example folder is *C:\MARSBackups*.

- Step 3** Right-click on the folder you created and click the **NFS Sharing** tab.

- Step 4** Select the **Share this folder** option, and enter a name in the Share name field.

An example share name can be the same as the folder name, *MARSBackups*.

- Step 5** Select the **Allow Anonymous Access** check box.

As the Windows server cannot directly authenticate the MARS Appliance, you *must* select this option.

Step 6 Click **Permission**.

The NFS Share Permissions dialog box appears.

Step 7 Select **ALL MACHINES** under Name, and then select **No Access** from the Type of Access list.

Step 8 Click **Add**.

Step 9 Enter the IP address of the MARS Appliance, and click **OK**.

Step 10 Select the IP address of the MARS Appliance, then select **Read-Write** from the Type of Access list. Ensure that **ANSI** is selected from the Encoding list.

Step 11 Click **OK** to save your changes and close the NFS Share Permissions dialog box.

Step 12 Click **Apply** to enable your changes.



Note

If the Apply does not work, you did not reboot the server after installing WSU 3.5. To work around this issue, you must reboot the server and repeat this procedure.

Step 13 From the DOS command window, enter the following commands:

```
cd <PathToParentOfShareFolder>
```

```
cacls <ShareFolderName> /E /G everyone:F
```

These commands modify the shared folder the permissions so that **Everyone** has local filesystem access to the folder. Example usage:

```
cd C:\archive
cacls MARSBackups /E /G everyone:F
```

Step 14 Click **Start > Control Panel > Administrative Tools > Local Security Policy**

Step 15 Under Local Security Policy > Security Options, double-click **Network Access: Let Everyone permissions apply to anonymous users**, select **Enabled**, and click **OK**.

This option equates the Anonymous user to the Everyone user.

You have completed the NFS configuration settings for the Windows server. To enable logging for debug purposes, continue with [Enable Logging of NFS Events, page 6-8](#). Otherwise, continue with [Configure the Data Archive Setting for the MARS Appliance, page 6-13](#).

Enable Logging of NFS Events

For troubleshooting purposes, you can enable NFS Server logging on a Windows host that is running the Microsoft Windows Services for UNIX 3.5.

To enable NFS server logging on the Windows host, follow these steps:

Step 1 Click **Start > All Programs > Services for UNIX Administration > Services for UNIX Administration**.

Step 2 Under Services for UNIX, select **Server for NFS**.

Step 3 Specify the folder where you want the log file to appear under Log events in this file:

By default the log file appears in C:\SFU\log directory.

- Step 4** Verify that all the check boxes are selected.
 - Step 5** Click **Apply** to save your changes.
 - Step 6** Continue with [Configure the Data Archive Setting for the MARS Appliance, page 6-13](#).
-

Configure the NFS Server on Linux

NFS is supported natively on Linux file systems, which requires that you have a Linux box. Because a Linux file server can be built inexpensively, it is highly recommended that a file server be built and dedicated for MARS archived data.

This section presents an example configuration as guidance for configuring your NFS to archive the data for a MARS Appliance. For each MARS Appliance that you want to archive for a given NFS server, you must set up a directory on the NFS server to which the appliance can read and write. The following procedure identifies the steps required to accomplish this task.

To prepare a Linux NFS Server for archiving from a MARS Appliance, follow these steps:

-
- Step 1** Log in to the NFS server using an account with root permissions.
 - Step 2** Create a directory for archiving data.

For example:

```
mkdir -p /archive/nameOfYourMARSBoxHere
chown -R nobody.nobody /archive
chmod -R 775 /archive
```



Note

Mode 770 works only for MARS Appliances running the same software generation (4.x or 5.x). Use 775 to support a mixed environment of 4.x to 5.3.x software and when performing migrations from 4.x to 5.3.x. Due to difference of UID/GID between the 4.x to 5.x releases, you must allow r-x so an appliance running 5.3.x can import from files exported by a 4.x appliance.

- Step 3** In the /etc/exports file, add the following line:

```
/archive/nameOfYourMARSBoxHere MARS_IP_Address(rw)
```
 - Step 4** Restart the NFS service.

```
/etc/init.d/nfs restart
```
-

Configure the NetApp NFS Server

The NetApp NFS server differs from other Linux/UNIX NFS servers in that NetApp restricts the functionality of the shell environment running on the server. As such, you must use an external UNIX/Linux administrative host to change the permissions and ownership of the exported NFS directory.

Before You Begin

- To perform the tasks in this procedure, you must configure an external Linux/UNIX administrative host. For information on configuring such a host, refer to the documentation for your Network Appliance server.

To prepare the NetApp NFS server so that the MARS Appliance can archive to it, follow these steps:

Step 1 If you have not exported a directory on the NetApp NFS appliance, and perform the following task from the NetApp's web GUI.

- a. Connect to the NetApp administrative host (http://hostname/na_admin/).
- a. Click **FileView**, then click **NFS** on the menu in the left pane.
- b. If the exported directory already exists, click **Manage Exports** under NFS. Otherwise, click **Add Export** under NFS.
- c. Select the following options on the NFS Export Wizard page, and click **Next**:
 - Read-Write Access
 - Root-Access
 - Security

The NFS Export Wizard - Path page appears.



Note If you are using a temporary NetApp administrative host, you can disable the host's access to the exported directory. To do so, do not select the Root-Access option. This configuration disables access by the host to the exported NFS directory.

- d. Enter the path to the desired export directory in the Export Path field, and click **Next**.
The NFS Export Wizard - Read-Write Access page appears.
- e. Click **Add**, and enter the IP address of the MARS Appliance in the Host to Add field, and click **OK**.
- f. Click **Add**, and enter the IP address of the NetApp administrative host in the Host to Add field, click **OK**, and then click **Next**.
The NFS Export Wizard - Root Access page appears.
- g. Click **Add**, then enter the IP address of the NetApp appliance (or the IP address of the Linux/Unix server to serve this purpose) in the Host to Add field, click **OK**, and then click **Next**.
The NFS Export Wizard - Security page appears.
- h. Select the **Unix Style** option, and click **Next**.
The NFS Export Wizard - Commit page appears.
- i. Verify that the settings are correct, and then **Commit**.

Step 2 To change the permissions of the exported directory, enter the following commands on the NetApp administrative host:

```
mount NetAppIP:/PathToExport /mnt/YourMountPoint
```

```
chown nobody.nobody /mnt/YourMountPoint
```

```
chmod 775 /mnt/YourMountPoint
```

**Note**

Mode 770 works only for MARS Appliances running the same software generation (4.x or 5.x). Use 775 to support a mixed environment of 4.x to 5.3.x software and when performing migrations from 4.x to 5.3.x. Due to difference of UID/GID between the 4.x to 5.x releases, you must allow r-x so an appliance running 5.3.x can import from files exported by a 4.x appliance.

Step 3 To verify that `/mnt/YourMountPoint` directory is writable by anyone, enter the following command:

```
ls -l /mnt
```

Step 4 To unmount the directory, enter the following command:

```
umount /mnt/YourMountPoint
```

Step 5 Configure the MARS Appliance to use the path as archiving directory as described in [Configure the Data Archive Setting for the MARS Appliance, page 6-13](#).

Configure Lookup Information for the NFS Server

**Note**

These common guidelines apply to NFS servers running on either Linux or Windows.

Many services in the current Linux system, such as ssh and the NFS server, use nslookup to obtain the hostname of the client. If the nslookup operation fails, the connection may fail or take a long time to finish the negotiation.

For the pnarchive and pnrestore operations to succeed, the NFS server must obtain the hostname of the MARS Appliance using its IP address. You can ensure that it obtains this information by doing one of the following:

- Add the NFS client (MARS Appliance) info in `/etc/hosts` file on the NFS server. The hosts file is located at `WINDOWS\system32\drivers\etc\` on Windows servers.
- Add the MARS Appliance information to your DNS server.

During a typical restore process, the MARS Appliance is first re-imaged from the DVD, upgraded to the correct version of software, and then the restore operation is performed. During the DVD re-image process, the name of the appliance is changed to the factory default, which is **pnmars**. If you do not wish to change the name of the appliance *before* you attempt to restore it from the NFS server, you must ensure add an entry for **pnmars** to the DNS server or in the `/etc/hosts` file on the NFS server so that during the restore operation, the NFS server can perform an IP address-to-hostname lookup for the MARS Appliance.

After the restore operation completes, the MARS Appliance will be restored to the name saved in the archived OS package. You should have included this name already in the DNS server or `/etc/host` file of the NFS server. Otherwise, this archive/restore operations may not function properly.

Configure the Cygwin SFTP Server on Windows

Cisco Security MARS supports SFTP servers as a storage medium for archiving or for data migration from 4.x to 6.0.1. This topic presents the steps require to configure Cygwin and OpenSSH on Windows. It targets Cygwin SFTP server on Windows XP.

**Note**

You must be logged in using an account with Administrator privileges on the Windows host to perform the tasks in this section.

Install the following packages as part of Cygwin:

- cygwin 1.5.25-12
- cygrunsrv 1.34-1
- openssh 5.0p1-1
- tcp_wrappers 0-7.6-4
- zlib 1.2.3-2

Once these packages are installed, perform the following steps:

Step 1 To CYGWIN as a System variable in Windows, right-click My Computer and select **Properties** on the shortcut menu.

Step 2 Click the **Advanced** tab, and then click **Environment Variables**.

Step 3 Do the following:

- Set value of CYGWin variable to **ntsec tty**
- Add **;%cygwin%\bin** to end of PATH System variable.

Step 4 From a Command Prompt shell, enter the following command:

cygwin

Result: The Cygwin command prompt appears.

Step 5 At the Cygwin command prompt, enter the following command:

ssh-host-config -y

Step 6 You are prompted to enter the value of environment variable CYGWIN.

ntsec tty

Step 7 To verify the sshd service is installed, enter the following command:

cygrunsrv -L

Step 8 To start sshd, enter the following command:

cygrunsrv -S sshd

Step 9 To verify that sshd is running, enter the following command:

sftp <username>@localhost

Where *username* is the administrative account used to install Cygwin.

Step 10 Enter the password for the administrative user account.

Step 11 Enter the following command:

pwd

The working directory should be `/home/<username>`.



Note

When performing a migration from a MARS Appliance (or configuring the archive settings in the web interface), use the Windows user account used to install Cygwin to authenticate to the SFTP server. For details on performing the migration, see the **pnexp** and **pnimp** commands in the [Migrating Data from Cisco Security MARS 4.x to 6.0.1](#) document.

Configure the Data Archive Setting for the MARS Appliance

You can archive the data and the system software that is running on a MARS Appliance to a remote server. This data archival includes operating system (OS) and upgrade/patch data, system configuration settings, and dynamic data, such as system logs, incidents, generated reports, and the audit events received by the appliance. The feature provides a snapshot image of the appliance.



Note

While complete system configuration data is archived, the dynamic data that is archived includes only the data that is received or generated *after* you enable the data archive setting. Therefore, we recommend that you enable archiving before configuring your appliance to receive audit events from reporting devices.

Using archived data, you can restore your appliance in the event of a failure, as long as the data is not corrupted. In this capacity, data archiving provides an alternative to re-imaging your appliance with the Recovery DVD.

Before You Begin

You must set up the NFS server correctly to archive the appliance's data. See [Configure the NFS Server on Windows, page 6-5](#) or [Configure the NFS Server on Linux, page 6-9](#).

You must configure the basic network settings for the appliance.

To configure the data archive settings for a given MARS Appliance, follow these steps:

Step 1 Select **Admin > System Maintenance > Data Archiving**.

Step 2 Specify values for the following fields:

- **Archiving Protocol**—Select either NFS or SFTP
- **Remote Host IP**—enter the IP address of the remote server.
- **Remote Path**—Enter the export path on the remote SFTP server, NFS server, or a NAS system where you want to store the archive files.

For example, `/MARSTBackups` would be a valid value for a Windows host with an NFS share named `MARSTBackups`. The forward slash is required to resolve the UNC share name.

- **Remote storage capacity in Days**—enter one of the following values:
 - The maximum number of days for which you want the archive server to retain data. The server keeps your data for the number of days previous to the current date.
 - The number of days of data that the archive server can maximally retain. In other words, you are identifying the upward capacity of the archive server.

- **Username**—(SFTP only) Enter the Windows user account used to install Cygwin to authenticate to the SFTP server.
- **Password/Re-enter password**—(SFTP only) Enter the password associated with the account specified in the Username field.

Data ArchivingStatus: **Running** ([less info](#))Archiving Service: **Enabled**Remote Server: **Available** (Click  to check remote host current status)

Remote Server Settings (* denotes required field)

| | |
|-------------------------------------|----------------------------|
| → *Archiving Protocol: | SFTP |
| → *Remote Host IP: | 10 . 2 . 3 . 7 |
| → *Remote Path: | /storage/jonla/5_3_5/PNARQ |
| → *Remote Storage Capacity in Days: | 10 |
| → *Username: | |
| → *Password: | |
| → *Re-enter password: | |

Data ArchivingStatus: **Running** ([less info](#))Archiving Service: **Enabled**Remote Server: **Available** (Click  to check remote host current status)

Remote Server Settings (* denotes required field)

| | |
|-------------------------------------|----------------------------|
| → *Archiving Protocol: | NFS |
| → *Remote Host IP: | 10 . 2 . 3 . 7 |
| → *Remote Path: | /storage/jonla/5_3_5/PNARQ |
| → *Remote Storage Capacity in Days: | 10 |

Step 3 Click **Start** to enable archiving for this appliance.**Note**

After starting archiving, if you see an error message such as “invalid remote IP or path,” your archive server is not correctly configured. If you receive these messages, consult [Configure the NFS Server on Windows, page 6-5](#), [Configure the NFS Server on Linux, page 6-9](#), or [Configure the Cygwin SFTP Server on Windows, page 6-11](#).

Result: A status page appears. Click **Back** to return to the Data Archiving page.

Step 4 If you need to change any values on this page, enter the value and click **Change**.

**Tip**

To stop archiving data, return to the Data Archiving page and click **Stop**.

Access the Data Within an Archived File

You can access the event data in an archived file allows to review the events contained therein. You may want to perform this task to look at a particular time range of events or to perform post processing on the data.

**Tip**

For other options on accessing archived data, see [Typical Uses of the Archived Data, page 6-2](#)

To access the data within an archived file, follow these steps:

Step 1 Perform the following command at the command line interface of the archive server:

```
cd <archive_path>
```

where *archive_path* is the remote path value specified in [Configure the Data Archive Setting for the MARS Appliance, page 6-13](#).

Step 2 To select the archive to review, enter the following command:

```
cd <YYYY-MM-DD>
```

where *YYYY-MM-DD* is the date that the archive file was created.

Step 3 To view the list of archive files for the selected data, enter the following command:

```
cd ES ls -l
```

Step 4 To extract the data from the archive file, enter the following command:

```
gunzip <filename>
```

where *filename* is the name of the file to extract. The list of available files are based on a timestamp for when they were created.

Step 5 To view the file's contents, enter the following command:

```
vi <filename>
```

You can use any text editor or run scripts against the data in these files. However, you should not change the contents of these zipped files or leave extracted data or additional files in the archive folders. MARS cannot process new or extracted files when performing a restore operation.

Recovery Management

MARS Appliance functionality includes two procedures that you can perform using the MARS Appliance Recovery DVD-ROM. The approach you should take to recover your appliance depends upon whether or not you have archived data that you want to recover as well. Two decisions affect how you will recover your MARS Appliance:

- **Re-Image a Global Controller or Local Controller.** The procedure for recovering an appliance is unique to the role that the appliance has in the STM system. Global Controllers require an additional operation on each monitored Local Controller.
- **Archived Data.** If you have been archiving data for the appliance that you wish to recover, there is an additional step following recovery of the appliance.



Caution

The recovery process erases the MARS Appliance hard disk drive. You permanently lose all configuration and event data that you have not previously archived or backed up. If possible, write down your license key before you re-image the appliance. You must provide this license key during the initial configuration following any re-image operation, and it is not restored as part of archived data.

The procedures, detailed in this section, are as follows:

- [Recovering a Lost Administrative Password, page 6-16](#)
- [Downloading and Burning a Recovery DVD, page 6-16](#)
- [Recovery the MARS Operating System, page 6-17](#)
- [Re-Imaging a Local Controller, page 6-18](#)
- [Re-Imaging a Global Controller, page 6-20](#)
- [Restoring Archived Data after Re-Imaging a MARS Appliance, page 6-22](#)

Recovering a Lost Administrative Password

If you lose the password associated with the *pnadmin* account, you cannot recover the password. You must re-image the appliance, which resets the password to the factory defaults, as described in [Re-Imaging a Local Controller, page 6-18](#), and [Re-Imaging a Global Controller, page 6-20](#). If you have configured the MARS Appliance to archive data, as described in [Configuring and Performing Appliance Data Backups, page 6-1](#), you can also recover the configuration and event data using the procedure in [Restoring Archived Data after Re-Imaging a MARS Appliance, page 6-22](#).

Downloading and Burning a Recovery DVD

If you do not have the MARS Appliance Recovery DVD-ROM that shipped with your MARS Appliance or you want to use a new image to expedite the post recovery upgrade process, you can download the current recovery image from the Cisco.com software download pages dedicated to MARS. You can access these pages at the following URLs, assuming you have a valid Cisco.com account and that you have registered your SMARTnet contract number for your MARS Appliance.

- Recovery images: <http://www.cisco.com/cgi-bin/tablebuild.pl/cs-mars-recovery>

After you download the ISO image, for example, *csmars-6.0.1.iso*, you must burn that file on to a DVD-ROM. The files are typically 1.42 GB or larger.

The following guidelines are defined:

- Use DVD+R, DVD+RW, or DVD-R and the correct media for either of those standards.
- Do not burn the DVD at a speed higher than 4X.
- To make a bootable DVD, you must burn the *.iso file onto the DVD using the bootable ISO DVD format; just copying the file to DVD does not make it bootable. Do not copy the *.iso file to a DVD; instead, you must extract it onto the DVD using your burner software. Most DVD burner software has a burn image function that extracts the files and makes the DVD bootable.

Recovery the MARS Operating System

For MARS 25, 55, 110, 210, GC2, and their variant models, the MARS operating system (OS) is stored separate from the MARS application and event data. It is stored on a flash disk-on-module (DOM) drive in the appliance. With the OS and application separation, if the MARS application hangs due to a RAID failure, you can login from a remote host and still retrieve log and trace data to assist in identifying the root cause of the failure.

The flash drive corrupts when, for example, system libraries or executable files are missing or are the wrong sizes as reported during a consistency checks or when the previous configuration is lost. When a corruption occurs, you will see symptoms like a failure to boot or to deploy the previous configuration, not able to execute certain commands, failures during the file system consistency check, or errors reporting missing files.

If the flash becomes corrupted, you can restore the OS using a Recovery DVD. For information on creating a Recovery DVD, see [Downloading and Burning a Recovery DVD, page 6-16](#). The recovery operation restores the MARS OS without prompting for installation option information, such as the model or role (Global Controller vs. Local Controller). The flash drive is also stores the system configuration data (IP addresses, DNS configuration settings, host name, and license file). During an OS recovery, the daily backup of the configuration data is copied from the hard drive to the flash drive so you configuration can be reapplied, eliminating any appliance configuration or licensing.

Before You Begin

- Ensure that the release number of the Recovery DVD matches the operating system running on your appliance. Issues may result if a DVD of an earlier release is used to recover a appliance running a newer release. The DVD does not checks the versions to prevent this issue.
- During the OS recovery operation, the system configuration data is copied from the hard drive to the flash drive. The system configuration data is created as part of the daily backup operation and is created nightly at 2:00 A.M. If your appliance has not been running long enough to back up the system configuration, then the OS is restored but the configuration is not.
- If you changed your system network settings (DNS, IP address, or hostname) after the last nightly backup, you must manually (using the [ifconfig, page 1-23](#), [hostname, page 1-19](#), and the [dns, page 1-11](#) commands) correct the settings once the OS recovery operation completes.

To recovery the operating system for your MARS Appliance, follow these steps:

-
- | | |
|---------------|--|
| Step 1 | Connect your monitor to the MARS Appliance's VGA port and your keyboard to the PS/2 keyboard port. (To view a diagram of the MARS Appliance VGA and serial ports, refer to the backplane figure corresponding to your appliance model in the <i>Cisco Security MARS Hardware Installation Guide</i> .) |
| Step 2 | Disconnect any connected network cables from the eth0 and eth1 ports. |
| Step 3 | Put the Recovery DVD in the MARS Appliance DVD-ROM drive. |

Step 4 Do one of the following:

- Log in to the MARS Appliance as pnadmin and reboot the system using the **reboot** command
- Power cycle the MARS Appliance

Result: The following message displays on the console:

```
Please Choose A MARS Model To Install...
1. Distributed Mars - Local Controller
2. Distributed Mars - Global Controller
3. Mars Operating System Recovery
4. Quit
```

Step 5 Using the arrow keys, select **3. Mars Operating System Recovery** at the Recover menu and press **Enter**.

Result: The OS binary download to the appliance begins. This process takes approximately 15 minutes. After the image download is complete, the Recovery DVD is ejected and the following message appears on the console:

```
Please remove the installation CD and press Reboot to finish the installation.
```

Step 6 Remove the Recovery DVD from the MARS Appliance.**Step 7** Press **Enter** to restart the MARS Appliance.

Result: The MARS Appliance reboots and synchronizes the configuration information between the flash drive and the hard drive.

Step 8 Reconnect any network cables to the eth0 and eth1 ports.

Because the OS recovery does not affect configuration data or event data, the system should be accessible with no further configuration requirements.

Re-Imaging a Local Controller

Use the MARS Appliance Recovery DVD-ROM to re-image the Local Controller if necessary. This operation destroys all data and installs a new image. In addition to preparing the device and later restoring any archived data, you must also perform three time-consuming appliance recovery phases:

- Image downloading from the CD (about 30 minutes)
- Image installation after the download (about 90 minutes)
- Basic system configuration (about 5 minutes)

**Caution**

Performing this procedure destroys all data stored on the MARS Appliance.

Before You Begin

- (Models 20/20R, 50, 100/100e, 200, GC/GCm) Write down your license key before you re-image the appliance. You must provide this license key during the initial configuration following the re-image operation.
- (Models 25/25R, 55, 110/110R, 210, GC2/GC2R) You must provide the license file during the initial configuration following the re-image operation.

To re-image your Local Controller, follow these steps:

-
- Step 1** Connect your monitor to the MARS Appliance VGA port and your keyboard to the PS/2 keyboard port. (To view a diagram of the MARS Appliance VGA and serial ports, refer the backplane figure corresponding to your appliance model in the *Cisco Security MARS Hardware Installation Guide*.)
- Step 2** Disconnect any connected network cables from the eth0 and eth1 ports.
- Step 3** Put the Recovery DVD in the MARS Appliance DVD-ROM drive.
- Step 4** Do one of the following:
- Log in to the MARS Appliance as pnadmin and reboot the system using the **reboot** command
 - Power cycle the MARS Appliance

Result: The following message displays on the console:

```
Please Choose A MARS Model To Install...
1. Distributed Mars - Local Controller
2. Distributed Mars - Global Controller
3. Mars Operating System Recovery
4. Quit
```

- Step 5** Using the arrow keys, select **1. Distributed MARS — Local Controller** at the Recover menu and press **Enter**.
- Step 6** (100/100e or 110/110R only) Do one of the following:
- If you are re-imaging a MARS 100 or 100e, the following message appears on the console.

```
Please Choose Which MARS 100 Model To Install...
1. MARS100
2. MARS100E
3. Quit
```

Using the arrow keys, select the proper model based on the license you purchased and press **Enter**.

- If you are re-imaging a MARS 110 or 110R, the following message appears on the console.

```
Please Choose Which MARS 110 Model To Install...
1. MARS110
2. MARS110R
3. Quit
```

Using the arrow keys, select the proper model based on the license you purchased and press **Enter**.

Result: The image download to the appliance begins. This process takes approximately 15 minutes. After the image download is complete, the Recovery DVD is ejected and the following message appears on the console:

```
Please remove the installation CD and press Reboot to finish the installation.
```

- Step 7** Remove the Recovery DVD from the MARS Appliance.
- Step 8** Press **Enter** to restart the MARS Appliance.

Result: The MARS Appliance reboots, performs some configurations, including building the Oracle database. The configurations that occur after the first reboot take a significant amount of time (between an hour and an hour and a half), during which there is no feedback; this is normal system behavior.

- Step 9** Reconnect any network cables to the eth0 and eth1 ports.



Note

After re-imaging the appliance, you must once again perform initial configuration of the MARS Appliance. For detailed instructions, see [Chapter 2, “Initial MARS Appliance Configuration.”](#)

Step 10 After the initial configuration is complete, do one of the following:

- Add any devices to be monitored to the Local Controller. For more information, see *User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x*.
- Recover the previously archived data using the procedure in [Restoring Archived Data after Re-Imaging a MARS Appliance, page 6-22](#)

Re-Imaging a Global Controller

Use the MARS Appliance Recovery DVD ROM to re-image the Global Controller if necessary. This operation destroys all data and installs a new image. In addition to preparing the device and later restoring any archived data, you must also perform four time-consuming appliance recovery phases:

- Purge all Global Controller data from each monitored Local Controller. (See [Before You Begin, page 6-20](#).)
- Image downloading from the CD (about 30 minutes)
- Image installation after the download (about 45 minutes)
- Basic system configuration (about 5 minutes)

To re-image your Global Controller, follow these steps:



Caution

Performing this procedure destroys all data stored on the MARS Appliance.

Before You Begin

- (Models 20/20R, 50, 100/100e, 200, GC/GCm) Write down your license key before you re-image the appliance. You must provide this license key during the initial configuration following the re-image operation.
- (Models 25/25R, 55, 110/110R, 210, GC2/GC2R) You must provide the license file during the initial configuration following the re-image operation.
- Before you can re-image a Global Controller, you must purge the data that the Global Controller pushed down to the Local Controllers that it monitors. For each Local Controller that is monitored by the Global Controller that you want to recover, execute the following command at the command line interface of each Local Controller.

```
pnreset -g
```

This command clears the global inspection rules and user accounts from the Local Controller, which prepares it to be managed by the re-imaged Global Controller. However, it does not remove the global user groups; instead they are renamed (appended with a date) and converted to local user groups. You can edit or delete these empty groups after the reset. Because user groups are often used as recipients for rule notifications, they are not deleted to avoid invalidating the Action definition of such rules.

Step 1 After you have executed the **pnreset -g** command on each Local Controller as described in [Before You Begin, page 6-20](#), connect your monitor to the MARS Appliance VGA port and your keyboard to the PS/2 keyboard port. (To view a diagram of the MARS Appliance VGA and serial ports, refer to the backplane figure corresponding to your appliance model in the *Cisco Security MARS Hardware Installation Guide*.)

Step 2 Disconnect any connected network cables from the eth0 and eth1 ports.

Step 3 Put the Recovery DVD in the MARS Appliance DVD-ROM drive.

Step 4 Do one of the following:

- Log in to the MARS Appliance as pnadmin and reboot the system using the **reboot** command
- Power cycle the MARS Appliance

Result: The following message displays on the console:

```
Please Choose A MARS Model To Install...
1. Distributed Mars - Local Controller
2. Distributed Mars - Global Controller
3. Mars Operating System Recovery
4. Quit
```

Step 5 Using the arrow keys, select **2. Distributed MARS — Global Controller** at the Recover menu and press **Enter**.

Result: The image download to the appliance begins. After the image download is complete, the Recovery DVD is ejected and the following message appears on the console:

```
Please remove the installation DVD and press Reboot to finish the installation.
```

Step 6 Remove the Recovery DVD from the MARS Appliance.

Step 7 Press **Enter** to restart the MARS Appliance.

Result: The MARS Appliance reboots, performs some configurations, including building the Oracle database. The configurations that occur after the first reboot take a significant amount of time, during which there is no feedback; this is normal system behavior.

Step 8 Reconnect any network cables to the eth0 and eth1 ports.



Note

After re-imaging the appliance, you must once again perform initial configuration of the MARS Appliance. For detailed instructions, see [Chapter 2, “Initial MARS Appliance Configuration.”](#)

Step 9 After the initial configuration is complete, do one of the following:



Note

You cannot add or monitor a Local Controller using the Global Controller until the Global Controller is running the same MARS software version as the Local Controllers it will be used to monitor.

- Add all Local Controllers back into the Global Controller. All devices and topology information are pulled up from each Local Controller into the Global Controller. For more information, see *User Guide for Cisco Security MARS Local and Global Controllers, Release 6.x*.
- **(Recommended)** Recover the previously archived data using the procedure described in [Restoring Archived Data after Re-Imaging a MARS Appliance, page 6-22](#).

Restoring Archived Data after Re-Imaging a MARS Appliance

When you restore a MARS Appliance using archived data, you are restoring the system to match the data and configuration settings found in the archive. The configuration data includes the operating system, MARS software, license key, user accounts, passwords, and device list in effect at the time the archive was performed.



Caution

The version of MARS software running on the appliance to be restored must match the version recorded in the archive. For example, if the data archive is for version 4.1.4, you must reimage the MARS Appliance to version 4.1.4, not older or newer, before using the **pnrestore** command to recover the system configuration and events.

For additional information on how the archives are restored, see [Guidelines for Restoring, page 6-23](#).



Note

If you choose to restore from your archived data, you must re-enter all devices on the Local Controller that are missing from the archive file. To restore existing cases, you must restore incident and session data. See [pnrestore, page 1-57](#), for more information on types of data and restore modes.

If you have archived your data and you have recovered your MARS Appliance as described in either [Re-Imaging a Local Controller, page 6-18](#), or [Re-Imaging a Global Controller, page 6-20](#), perform the following steps:

Step 1

When the recovery process is complete, restore the MARS Appliance from the last archived data by executing the following command:

```
pnrestore -p <ArchiveServerIP>:/<archive_path>
```

Where *ArchiveServerIP* is the value specified in the Remote Host IP field and *archive_path* is the value specified in the Remote Path field in the settings found in the web interface at **Admin > System Maintenance > Data Archiving**. You must identify the archive server by IP address, separated by a `:` and then the pathname *ArchiveServerIP:/archive_path*. For more information on these settings, see [Configure the Data Archive Setting for the MARS Appliance, page 6-13](#).

Step 2

When the restore operation completes, you may need to delete, re-enter, and re-discover all the devices that are missing from the MARS archive file.

Configuring a Standby or Secondary MARS Appliance

You cannot run queries and reports or perform incident investigation over archived data directly. To perform any kind of investigation using archived data, you must restore that data to a MARS Appliance. Therefore, we recommend that you configure a secondary appliance for this purpose. The reason to use a separate appliance to study old data is that you must restore the period data to the appliance, and the restore re-images all configuration and event data based on the archive settings for the defined period.

To restore to a secondary appliance, you must restore to an appliance of the same model or higher. For example, you can restore an image from a MARS 20 to a MARS 20, MARS 50, MARS 100, or MARS 100e; however, you *cannot* restore a MARS 50 to a MARS 20. Restoring to a secondary appliance differs from restoring to the actual appliance that performed the archive. The following issues must be addressed when restoring to a secondary appliance:

- You must purchase a new license key for the secondary appliance. Each license key is associated with the serial number of the appliance to which it is assigned.
- You must enter that new license key on the restored image before you can log into the secondary appliance.
- When restoring the image to the secondary appliance, you need to take the primary appliance off the network or perform the operation behind a gateway that can perform NAT. When the secondary appliance comes up and you are on the same network, you receive an IP address conflict error, because the IP address assigned to the secondary appliance exactly matches that of the primary.

Because a single image of the complete system configuration data is archived and updated daily, no matter what period you select from an archive, the system configuration data includes the most recent changes. In other words, selecting a period that is 365 days old affects only the event data. The system configuration that is restored mirrors that of the most current archive.

For more guidance, see [Guidelines for Restoring, page 6-23](#).

Guidelines for Restoring

When you do restore to an appliance, keep in mind the following guidelines:

- The version of MARS software running on the appliance to be restored must match the version recorded in the archive. For example, if the data archive is for version 4.1.4, you must reimage the MARS Appliance to version 4.1.4, not older or newer, before using the **pnrestore** command to recover the system configuration and events.



Caution

The **pnrestore** command does not check to ensure that the same version requirement is met, and it will attempt to restore an incorrect version match.

- All restore operations take a long time. Time varies based on the options you select. See [pnrestore, page 1-57](#).
- A restore of configuration data only takes less time.
- A restore operation does not allow for incremental restores of event data only. It always performs a complete reimage of the harddrive in the target appliance.
- All configuration information, including the license key, IP addresses, hostname, stored certificates and fingerprints, user accounts, passwords, and DNS settings, are always restored.
- If restoring to an appliance other than the one that created the archive, see [Configuring a Standby or Secondary MARS Appliance, page 6-22](#).
- When restoring to an appliance different from the one that archived the data, you must enter the license key assigned to the serial number of the new appliance before you access the restored data.
- A restore is performed from the day you specify forward until the archive dates are exhausted. The date argument of the **pnrestore** command should be the name of the daily data backup directory that identifies the start of the time range to be restored. See [Format of the Archive Share Files, page 6-3](#).
- To restore a specific range of days, we recommend temporarily moving the unwanted days at the end of the range out of the archive folder. This technique of trimming out unwanted days can also speed up the restore, although you do lose the dynamic data from those dates.
- If the data contained in the selected restore range of the archive exceeds the capacity of the local database on the target MARS Appliance, the MARS Appliance automatically purges the data in the oldest partition of the local database and then resumes the restore operation. As such, you should

select a reasonable range of dates when performing the restore. Nothing is gained from restoring ranges that exceed the local database limits, and the overall restore operation is slowed by the intermittent purging of the oldest partition until the most current date is restored.

- Mode 5 of the **pnrestore** command restores from a backup in the local database; you cannot use it to restore from a NFS or SFTP archive. As such, you do not need to have archiving enabled to perform this restore operation. The configuration data is backed up every night on the appliance. Beware that if you upgrade to a newer release and attempt a restore before that configuration has been backed up, the restore will fail. See [pnrestore, page 1-57](#), for more information on types of data and restore modes.
 - If a Global Controller requires re-imaging, you should perform a **pnrestore** operation to recover the data after it is reimaged (assuming you have archived it). This approach is recommended because:
 - All global data defined on the Global Controller and propagated to each managed Local Controller is not pushed back to the Global Controller, so restoring it from an archived configuration file is the only method of recovering these configuration settings and accounts.
 - Incidents and report results that were pushed to the Global Controller before it was reimaged are not pushed back after reimaging. When running on a Global Controller, the archive operation only archives reports, which can be restored. However, all old incidents are permanently lost on the Global Controller, as they are not archived.
 - Regardless of how the Global Controller is restored, re-image or restore, the Local Controllers must be cleaned of Global Controller configuration data, which is accomplished by performing a **pnreset -g** operation on each Local Controller.
 - The **pnreset -g** operation must be completed on each Local Controller before attempting to restore the Global Controller.
-



APPENDIX A

Troubleshooting

Revised: September 11, 2008, OL-16776-01

This appendix presents information that is helpful when troubleshooting the MARS Appliance. It lists expected services and error messages for each supported MARS Appliances. It explains how to collect and send support information to assist Cisco support in debugging such services are required. This appendix also provides guidance on retrieving lost license keys and running the web interface using a console connection. It includes the following topics:

- [Determine Version Information, page A-1](#)
- [Cannot Locate License Key, page A-2](#)
- [Cannot Recovery My Password, page A-2](#)
- [Cannot Delete a Device from MARS, page A-3](#)
- [Cannot Re-Add a Device to MARS, page A-3](#)
- [Cannot Add a Device to MARS, page A-3](#)
- [Cannot Rename Device in MARS, page A-3](#)
- [Collect Support Information, page A-3](#)
- [Access the GUI when the Network Is Down, page A-6](#)
- [Troubleshooting Global Controller-to-Local Controller Communications, page A-6](#)
- [List of Backend Services and Processes, page A-12](#)
- [Error Messages, page A-15](#)

Determine Version Information

Feature Modification History

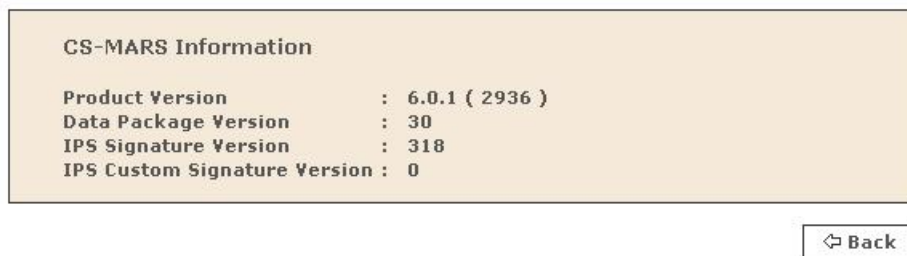
| Release | Modification |
|--------------|---|
| 4.3.1, 5.3.1 | Separates dynamic IPS signature version information. Introduced requirement to maintain identical IPS signature versions between Global Controller and managed Local Controllers. |
| 6.0.1 | Separates product package from data package version information. |

The software version information provide four versions:

- **Product version.** Identifies the version of system binaries running on the appliance.
- **Data package version.** Identifies the data package (signature updates, rules, reports, event types, and event type groups, etc.) version running on the appliance.
- **IPS signature version.** Identifies the latest Cisco IPS signature package is installed on the appliance.
- **IPS custom signature version.** Identifies the latest version of custom Cisco IPS signatures installed on the appliance.

The dynamic IPS signature updates 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.

To view this information, click **Help >About** on each appliance.



To obtain just the product and data package details, you can enter **version** at the command line interface.

```
[pnadmin]$ version
6.0.1 (2936) 30
[pnadmin]$
```

Cannot Locate License Key

For newer models of the MARS Appliance, the license key and serial numbers are both located on the exterior of the appliance. For information on locating the license key and serial number, see [License Key, page 1-2](#) for details on locating the license key in Generation 2 hardware or [License Key, page 2-2](#) for locating the license key in Generation 1 hardware.

If you cannot locate your license key, contact the Cisco Licensing Team at licensing@cisco.com. You will need to provide the following information in the e-mail:

- Customer name
- Serial number of the MARS Appliance

Cannot Recovery My Password

See [Recovering a Lost Administrative Password, page 6-16](#).

Cannot Delete a Device from MARS

See [Delete a Device](#), page 3-15.

Cannot Re-Add a Device to MARS

If you cannot re-add a device to MARS, the device is likely already defined in one capacity or another. See [Delete a Device](#), page 3-15.

Cannot Add a Device to MARS

If you cannot add a device to MARS, the device has likely been defined during a topology discovery operation. You can address this issue by first deleting the device, and then adding it. See [Delete a Device](#), page 3-15.

Cannot Rename Device in MARS

You cannot directly rename a device. To do so you must first delete the device and then re-add it. See [Delete a Device](#), page 3-15.

Collect Support Information

As long as your appliance is running, you can provide Cisco support with log information that can assist in diagnosing any issues you are having with the appliance. Three options exist for collecting and sending this information:

- **Collect Summary Status from the MARS Database.** You can use the `get_mars_summary_info.sh` script to gather high-level statistics about a MARS Appliance's configuration and topology.

```
[pnadmin]$ script get_mars_summary_info.sh
Collecting MARS summary info from the DB in HTML format
Started at Fri Aug 24 11:08:58 PDT 2007
Use 'pnlog mailto' command to include it in the logs This may take several minutes to
complete. Use Ctrl+C in case you need to interrupt.
Completed at Fri Aug 24 11:10:20 PDT 2007 [pnadmin]$
```

After running the script, use the **pnlog mailto** command to e-mail the logs to yourself. You will see the files `get_mars_summary_info.html` and `get_mars_summary_info.run.log` in the log file named `error-logs.tar.gz` received with the other logs.

- From the CLI, you can use the **pnlog mailto** command. For more information on using this command, see [pnlog](#), page 1-48.
- In the GUI, you can use the **Help > Feedback** option. For more information on using this option, see [Submitting Feedback and Reporting Errors](#), page A-4

Both options require that the appliance is connected to a network that can reach your SMTP server, and that the appliance is configured properly to send e-mail to that server. You can specify the e-mail gateway settings either on the Admin > System Setup > Configuration Information page or as an option the command line using the **pnlog mailto** command.

The **pnlog mailto** command packages and delivers the following information in a file named `error-logs.tar.gz`:

- C++ process logs
- System logs
- Java (GUI) logs
- Upgrade logs
- Current version
- Current model
- List of running processes

No passwords or network information is included in the `error-logs.tar.gz` file.

Submitting Feedback and Reporting Errors

If you receive an error in the web interface and the system recovers, a pink page appears allowing you to report the error to Cisco.



You can use either the Report Error button or the Feedback button that appears on every page to send feedback and error log files to the Cisco TAC. When you select the Feedback button, an e-mail message is sent to the e-mail address associated with the user account with which you are logged into the MARS web interface. You can forward this e-mail as needed. If you log in using an account that does not have an e-mail address associated with it, you will be prompted to enter an e-mail address.

The Report Error button allows you to send the error logs and information related to the triggering error. The error log facilitates debugging the error, and therefore it is the recommended option. However, this option requires that you provide a valid TAC case number to which the error log is attached.

TAC Case Number:

If this is a new case, please create a Cisco TAC Service Request by clicking here.

Email Log to TAC:
☒

Message:

Please describe what actions produced the error:

If you do not already have a valid case number, you are redirected to the Cisco TAC web site so you can create a new TAC case and obtain a valid case number.

[Logged In](#) | [Profile](#) | [Contacts & Feedback](#) | [Help](#) | [Site Map](#) | [Select a Location / Language](#)

HOME

TECHNICAL SUPPORT & DOCUMENTATION

TOOLS & RESOURCES

TAC Service Request Tool

Products & Services | Ordering | Technical Support & Documentation | Learning & Events | Partners

Tools & Resources

TAC Service Request Tool

Welcome to the TAC Service Request Tool.

The TAC Service Request Tool allows you to:

- Open severity 3 and 4 service requests and, after you describe your service request online, the tool recommends resources that may provide a solution immediately.
- Check the current status of open service requests
- Update open service requests with your own notes
- Attach files to open service requests
- View service requests closed within the last 18 months

If you have a severity 1 or 2 network-down emergency, open your service request by [telephone](#).

[Create a new TAC Service Request](#)

[Query a TAC Service Request](#)

Cisco Security MARS Initial Configuration and Upgrade Guide, Release 6.x

OL-16776-01

A-5

Access the GUI when the Network Is Down

While console connections enable you to perform basic network settings for an appliance, you must use the GUI to perform the majority of the configuration for the appliance. If you cannot connect to the appliance from hosts on your network, you can access the GUI using a computer by connecting a crossover cable to one of the Ethernet ports in the appliance.

To access the GUI using a console connection, follow these steps:

-
- Step 1** With the appliance running, connect a Cat 5 crossover cable to your computer's Ethernet port.
- Step 2** Connect the Cat 5 crossover cable to the MARS Appliance's eth1 port. See [Physical Descriptions—MARS 25R, 25, 55, 110R, 110, 210, GC2R, and GC2, page 1-1](#) or [Physical Descriptions—MARS 20R, 20, 50, 100E, 100, 200, GCm, and GC, page 2-1](#).
- Step 3** Configure the computer's local TCP/IP settings to be on the same network as one of the Ethernet interfaces in the MARS Appliance. Pick an IP address other than the one used by the appliance on that interface.

It is possible that you specified the interface address for eth1 when you configured the interfaces using a console connection in [Specify the IP address and Default Gateway for the Eth0 Interface, page 2-7](#), and [Specify the IP Address for the Eth1 Interface, page 2-8](#). However, the factory default setting for eth1 is 192.168.0.101.



Tip

You can use eth0 also; however, you must specify an address for your computer that works with the network settings that you specified in [Specify the IP address and Default Gateway for the Eth0 Interface, page 2-7](#).

Troubleshooting Global Controller-to-Local Controller Communications

The following sections provide information to assist in troubleshooting communications issues between a Global Controller and the Local Controllers it manages.

- [Communications Overview, page A-6](#)
- [Communication States, page A-7](#)
- [Required Open Ports, page A-7](#)
- [General Issues and Solutions, page A-8](#)

Communications Overview

A Global Controller and Local Controller can communicate if they are running on the same version of software. A version mismatch causes all communications to stop. For more information on configuring the communications, see [Configuring the Global Controller, page 3-1](#).

When a Global Controller and Local Controller communicate, several types of data are synchronized:

- **Topology.** Topology configuration data includes the list of monitored devices, their interfaces, routes, and network groups. This data is sent from a Local Controller to the Global Controller every 30 seconds.
- **Configuration.** Configuration data includes custom parser definitions, event types, inspection rules, report definitions, and user accounts and roles that are defined on the Global Controller. This data is sent from the Global Controller to Local Controller every 30 seconds.
- **Report data.** Report result data is sent from a Local Controller to the Global Controller every 10 minutes. If a backlog exists on the Local Controller (for example, due to a communications failure), a block of report data is picked up 30 seconds after the previous block transmission completes until the backlog is clear.



Note For each schedule report (whether global or just a default system report), data is collected every 10 minutes and sent to the Global Controller, regardless of whether a report is scheduled within that interval.

- **Incident/firing event data.** This data is sent from the Local Controller to Global Controller every two minutes.



Note When a backlog exists in report data, the most recent data is sent first, allowing MARS to stay current with incoming data and to clear the backlog over time.

Communication States

When troubleshooting the communications, first verify that the Local Controller and Global Controller are communicating properly. From the web interface of the Global Controller, view the device state on the Admin > System Setup > Local Controller Information page. Understanding the communication state can assist you in diagnosing issues.

The key states to check for when troubleshooting communications issues are as follows:

- **Active.** This state indicates that communications are operational. If you made a recent change, wait a minute for the system to process the change and then re-visit the page to obtain the updated state.



Note After adding a new Local Controller, the page briefly indicates the Active state even though you have not added the certificates. Re-visit the page to obtain the correct state.

- **Certificate Errors.** This state indicates the certificates are not configured correctly. If this state appears, validate the certificates on both the Local Controller and Global Controller. See [Importing the Security Certificates, page 3-10](#)
- **Synchronizing (progress).** This state results from triggering a full topology synchronization. A status indicator allows you to monitor the progress.

For a complete list of states and their meanings, see [Table 3-3 on page 3-5](#).

Required Open Ports

When a Global Controller and Local Controller are separated by a firewall, open the following ports on both the inside and outside interfaces of the firewall to ensure proper operation of the Global Controller:

| TCP Port | Function |
|----------|---|
| 22 | Secure Shell (SSH) used by Local Controller for topology and device discovery |
| 443 | Hyper Text Transport Protocol with Secure Sockets Layer (HTTPS) use for user interface access |
| 8444 | Cisco Proprietary data synchronization between a Global Controller and Local Controllers. |

General Issues and Solutions

The following symptoms and solutions address many synchronization errors.

**Tip**

Deleting and re-adding a Local Controller is rarely, if ever, the solution. This change also causes a full re-synchronization of topology data, resulting in an even longer downtime (possibly days). You should only delete a Local Controller if you want to permanently remove that Local Controller from the Global Controller.

| Symptom | Possible Resolution |
|--|---|
| Local Controller/Global Controller communications fail. | Beginning with the 4.3.1 and 5.3.1 releases, the dynamic IPS signature updates 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. To determine the version of MARS software and the IPS signature version, click Help >About on each appliance. |
| Local Controller/Global Controller communications does not appear to work but the state is Active. | <p>This issue can result from a backlog of data caused by a temporary disconnect of the Local Controller and Global Controller. Data synchronizes over time; therefore, the solution is to wait to verify the issue is correctly diagnosed. See Data is not synchronizing and the Local Controller and Global Controller were disconnected., page A-9</p> <p>Possible causes:</p> <p>A recent network outage caused a communication disconnect. The symptoms appear if the Local Controller receives a lot of data because, in such cases, the backlog can be large.</p> <p>A high usage MARS Appliance may not have adequate bandwidth between Local Controller/Global Controller to ensure that the system stays synchronized.</p> |
| Data is not synchronizing and the Local Controller and Global Controller were disconnected. | <p>If a Local Controller\Global Controller pair is disconnected for a long period of time, the report and incident data will take a long time to transfer to the Global Controller. For each global report, data is gathered every 10 minutes and then transferred to the Global Controller. If the connectivity to the Global Controller is down, the Local Controller queues up pending data transfers. When connectivity is restored, it begins sending the report data.</p> <p>Configuration and topology data does not take as long as report and incident data, and it should synchronize in a reasonable amount of time.</p> <p>Note Communication link speeds vary; a saturated link could slow synchronization greatly relative to a lab environment.</p> |

| Symptom | Possible Resolution |
|--|---|
| A change in the Global Controller, such as adding a new global report or inspection rule, does not appear on a managed Local Controller. | <p>Verify Activate was clicked.</p> <p>You must click Activate for Local Controller-based topological changes to be pushed to the Global Controller</p> |
| No incidents appear in the Global Controller | <p>This issue can result from a time synchronization mismatch. Make sure the Local Controller and Global Controller have the system times set properly as a time skew can cause incidents to not appear in the Summary page.</p> |
| I deleted a Local Controller from the Global Controller when there were communication problems. How do I restore the Local Controller? | <p>If the Local Controller was deleted from a Global Controller when communications were failing, use the pnreset -s command to reset the Local Controller to standalone mode. Then, you can add it to the Global Controller again.</p> <p>For more information, see pnreset, page 1-54.</p> |
| A replacement Global Controller appliance has been restored. How do I restore communications with the Local Controllers? | <p>Use the pnreset -g command on each Local Controller. This command removes the Global Controller data from a Local Controller, leaving Local Controller-specific data untouched. This option keeps the Global Controller connectivity information on the Local Controller intact, enabling the Local Controller to reconnect as soon as the Global Controller is restored (to purge this information, use the -s option). For more information, see pnreset, page 1-54.</p> <p>Note Use this option only when a Global Controller recovery is required.</p> |

| Symptom | Possible Resolution |
|---|--|
| The topology diagram is missing a device or other information. | <p>To verify the issue is not the result of a slow link or catch up due to network downtime, add new device as a test. If the test device replicates after clicking Activate and waiting a few minutes, but the missing data still does not replicate, there could be an issue processing the transaction log.</p> <p>To manually re-synchronize the topology data, perform the following steps from the Global Controller web interface:</p> <ol style="list-style-type: none"> 1. Click Admin > Local Controller Management. 2. Select the Local Controller that has the issues and click the Topo Sync Start/Stop button. <p>The entire topology is copied from the Local Controller to the Global Controller. The size of this data set depends on the topology, but in very large cases, this operation can take several days. See Topology Synchronization, page 3-4.</p> <p>On the Local Controller Management page, the status indicates that data is being processed. As long as it is moving, progress is being made so continue to wait.</p> <p>Note Deleting and re-adding the Local Controller restarts this process and is not recommended</p> |
| A topology change does not appear, the state is Active, and a reasonable amount of time has passed. | <p>Initiate a full topology synchronization to re-push all topology.</p> <p>Note The time required to perform a full topology synchronization is not trivial; use this process only if topology data is missing on the Global Controller but more recent topology data has been transferred from the same Local Controller.</p> |

| Symptom | Possible Resolution |
|--|---|
| Configuration data (users, report definitions, rules, and event types) does not replicate from a Global Controller to Local Controller | <p>If the servers were disconnected, this symptom can result because it takes time to clear the backlog created during the downtime.</p> <p>To diagnose, create a new piece of data, such as a new user, and then click Activate. If, after a few minutes, the new user data replicates but the originally missing data does not, MARS has encountered an issue replaying that log. No configuration synchronization mechanism exists; therefore, you should follow your technical support escalation process.</p> |
| None of the previous suggestions correct the error. | <p>Use the pnlog command to collect log data and submit it to technical support to identify exceptions that may have caused the error. See Collect Support Information, page A-3.</p> |

List of Backend Services and Processes

You can obtain status on the following services and processes by entering **pnstatus** at the command line or by selecting Admin > System Maintenance > View Log Files to view backend system logs generated by the appliance. [Table A-1](#) lists the services and processes and provides a description of their role within MARS.



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.

Table A-1 MARS Services and Processes Descriptions

| Service/Process Name | Description |
|----------------------|--|
| ANOMALY service | The ANOMALY service performs statistical analysis of flows and other variables obtained via SNMP MIBs such as per-interface bandwidth, per-interface errors, and firewall connections. This service detects statistically significant anomalies in the data. In case of a detected anomaly, the ANOMALY service inserts a MARS generated “anomaly detected” event into the system. |
| autoupdate | The backend process that pulls and processes the IPS signature updates. |
| csdam | <p>This backend process was responsible for DTM and the management of IOS IPS signatures. It uses the IOS command line interface (CLI) over SSH or Telnet to issue SDF updates and retrieve current configuration information from the managed Cisco IOS IPS routers.</p> <p>Note This process was removed in 6.0.1.</p> |

Table A-1 MARS Services and Processes Descriptions (continued)

| | |
|---------------------|---|
| csiosips | This backend process uses SDEE to pull alerts from IOS IPS devices using SDEE. The alerts pulled are then processed and passed on to pnparser from where they enter the system as all other events do. This process, introduced in version 4.2.2, replaces the former process named pniosips_srv. |
| csips | This backend process uses RDEP to pull alerts from IDS 4.0 devices and SDEE to pull alerts from IPS 5.0 devices. The alerts pulled are then processed and passed on to pnparser from where they enter the system as all other events do. This process, introduced in version 4.2.2, replaces the two former processes named pnids40_srv and pnids50_srv. |
| cswin | This backend process uses MS-RPC to pull alerts from Windows devices. The alerts pulled are then processed and passed on to pnparser from where they enter the system as all other events do. This process was introduced in version 4.2.2. |
| DbIncidentLoaderSrv | This process stores event/session data for fired incidents into the database after process_postfire_srv has performed false positive analysis. |
| device_monitor | The PNMONITOR service acts as a software watchdog for JBOSS and SUPERV. The operating system watches the health of PNMONITOR service. |
| device_monitor | This process uses SNMP to monitor the resources usage on the reporting devices and raises device anomalies (MARS events) when the usage exceeds the defined thresholds. The resources studied include CPU, memory, number of connections, and bandwidth used. |
| discover | The DISCOVERY service discovers the Layer 3 and Layer 2 network topology, NAT and ACL configuration from firewalls and routers. The service parses this information and stores it in the database in a unified vendor and device neutral form. |
| GC Exchange service | The Global Controller Exchange service communicates with the Global Controller and synchronizes the information between the two systems. The information that needs to be synchronized is: <ul style="list-style-type: none"> • Network topology discovered by the MARS appliances, • Report results generated by a MARS appliance • Incidents generated at a MARS appliance • Global objects (for example, networks, services, rules, reports, and queries) created at a Global Controller |
| graphgen | The GRAPHGEN service creates network topology graphs, hotspot topology graphs, and topological attack paths for display by the web browser. The service also generates appropriate vendor and device-specific mitigation commands based on its derived knowledge about the attack path and all devices along the attack path. |
| GUI service | The GUI service provides the code used to display web pages that serve as the web interface for MARS. The service uses a JBOSS/Tomcat application server framework. |

Table A-1 *MARS Services and Processes Descriptions (continued)*

| | |
|-----------------------|---|
| KeywordQuerySrv | Based on a keyword query across raw messages, this backend process scans through local index and data files to identify and retrieve matching raw messages. The results are then stored in the database. This process was introduced in 5.2.4. |
| LOADER service | The LOADER service efficiently stores the events and incidents into the database and compresses the data to be stored for archival purposes. |
| LOGIC service | The LOGIC service correlates the parsed events according to a set of inspection rules. The inspection rules may be built in (that is, system defined) or defined by the user. Whenever a correlation rule is satisfied, the LOGIC service creates an incident containing the set of events satisfying the rule and forwards the incident for further analysis to process_postfire_srv. |
| pnarchiver | The pnarchiver service archives data stored in the database to an offline store via NFS. Both configuration data and dynamic events and incident data are archived. The archiving is done for both system recovery and forensics. |
| pndbpurger | The pndbpurger service deletes old data from the database to make room for new data. |
| pnesloader | This process stores event and session data in the database after pnparsr has parsed and sessionized the recoeved data. |
| pnmac | This backend process retrieves the mac addresses for the IP addresses found in sessions and incidents. It uses the STP information provided by the switches to which the sources and destinations are connected. MARS uses this data to perform port blocks or suggest the CLI commands required to block traffic from these MAC addresses. |
| pnparsr | The pnparsr service receives and parses events, SNMP MIBs and traffic flow logs generated by the reporting devices. It also uses network topology information to sessionize flows. The sessionization process involves grouping flows and other events for the same Layer 7 session that arrives within a small time frame. The network topology information is used to normalize the NAT-ed flows. Events belonging to the same session are assigned a session identifier. |
| process_event_srv | This process is the rule processing engine. Compiles rules, receives events, computes the incidents that need to be fired and passes them on for notification and false positive analysis to process_postfire_srv. |
| process_inlinerep_srv | The INLINE REPORT service performs in-memory computation of certain reports—this avoids the huge I/O penalty associated with database server computing these reports. |

Table A-1 MARS Services and Processes Descriptions (continued)

| | |
|----------------------|---|
| process_postfire_srv | <p>The process_postfire_srv service analyzes the incidents generated by the LOGIC service to determine whether they are false positives, identifies valid incidents that may represent potential attacks, and notifies the administrator. The service examines information from the following sources:</p> <ul style="list-style-type: none"> • Built in event vulnerability data • Host information obtained from administrators or learned when process_postfire_srv probes hosts that have been attacked • Host Vulnerability information from vulnerability scanner results • Network topology paths and sessionized event data |
| process_query_srv | This process computes the results for multi-lined queries (queries that look like multi-line rules. For example, X followed by Y). |
| REPORTGEN service | The REPORTGEN service generates and sends the reports for the users. The service uses the JBOSS/Tomcat application server framework. |
| securesyslog | <p>This process supports secure syslog messages, such as those provided by Cisco ASA devices.</p> <p>This process was introduced in version 6.0.1.</p> |
| superV | The superV service acts as a software watchdog for various MARS backend processes. It monitors resource usage of the various services and various consistency conditions and restarts the appropriate services whenever necessary. The superV service also provides an event bus for the MARS processes to send messages to each other. |

Error Messages

“Error ./pnarchiver Thread 2051:PN-0102:SQL error: ORA-01005: null password given; logon denied”

Issue: Problem with archiving to NFS server. The directories for the archiving are properly created on the server but those directories remain empty.

Workaround: An interoperability issue exists between MARS and CygWin NFS server running on Windows 2003 server. To work around such interoperability issues, replace the NFS server with Microsoft Windows Services for Unix. For more information, see [Configure the NFS Server on Windows, page 6-5](#).

Page cannot be found.

Issue: Upon logging in to the web interface, user receives a “Page cannot be found.” error and the URL in the address bar is of the format: `https://<IP_address>/j_security_check`.

Workaround: If you have the MSN Search Toolbar enabled in your browser, you must disable it before logging into MARS. To disable it, right-click on the toolbar and deselect MSN Search Toolbar. Alternatively, you can simply delete the `j_security_check` at the end of the URL string and press Enter.

Hangs on "Creating Oracle database"

Issue: When using the Recovery DVD, the system hangs on "Creating Oracle database."

Workaround: This error can occur when, after reboot, the appliance is connected to a network. When the image is applied, the system hangs attempting to detect the factory default addresses on the network.

"Status: PN-0002: No message for PN-0216"

Issue: The message, "Status: PN-0002: No message for PN-0216", displays after configuring the data archive settings in the web interface.

Workaround. This error message appears when you've entered an incorrect IP address or directory path for the data archiving feature.



INDEX

A

AAA

- configure login prompts [2-17](#)

adding

- devices [3-15](#)
 - manually [3-15](#)
- routes [2-10](#)

administrative account

- default password settings [2-6](#)
- reset password [4-2](#)

archive [6-1](#)

- data [6-1](#)
- file and folder format [6-3](#)
- NFS for Windows [6-5](#)
- NFS on Linux [6-9](#)
- Windows Services for UNIX [6-5](#)

archive data

- identify time period contained [6-4](#)

archiving [6-13](#)

- starting [6-14](#)
- stopping [6-15](#)

B

backing up [6-13](#)

backup [6-1](#)

- estimating storage requirements [6-2](#)
- network connection requirements [6-2](#)
- schedule [6-1](#)
- using eth1 interface for NFS traffic [6-2](#)

browser

- configure [1-5](#)

C

Cat 5 crossover cable [A-6](#)

certificate [2-12](#)

CLI

- console connection [2-4](#)

- direct console [2-5](#)

- Ethernet console [2-5](#)

pnreset

- usage note [6-24](#)

pnrestore

- usage note [6-23, 6-24](#)

- serial console [2-5](#)

- SSH console [2-5](#)

configuration

- initial [2-1](#)

- initial procedure [2-6](#)

console connection [2-4](#)

- log in [4-1](#)

- remote shut down [4-3](#)

D

data

- archive [6-1](#)

- archiving [6-13](#)

- backup [6-1](#)

default address

- eth0 [2-5](#)

- eth1 [2-5](#)

default login [2-12](#)

default password [2-12](#)

deleting

- routes [2-10](#)
- disaster recovery
 - overview [6-16](#)
 - planning failover [6-22](#)

DNS

- configuration settings [2-15](#)
- documentation
 - related to this product [i-viii](#)

- DVD [6-16](#)

E

- e-mail settings
 - define system administrative account [2-16](#)
- error messages, list of [A-15](#)
- eth0 [2-14](#)
 - define settings [2-7](#)
- eth1 [2-14](#)
 - define settings [2-8](#)
- events per second
 - deployment planning [1-1](#)

F

- failover
 - configure standby server [6-22](#)
- file system consistency check [5-8](#)
 - during reboot [5-8](#)
- flash disk-on-module (DOM), see flash drive [6-17](#)
- flash drive
 - configuration saved on [6-17](#)
 - corruption [6-17](#)
- fsck, see file system consistency check [5-8](#)

G

- getting started
 - initial configuration [2-1](#)

Global Controller

- adding Local Controllers to [3-3](#)
- and Local Controllers [3-14, 3-15](#)
- reimaging guidelines [6-24](#)

H

- hostname
 - define for appliance [2-9](#)
- host routes
 - adding [2-10](#)
 - deleting [2-10](#)
- hot swap
 - configure standby server [6-22](#)

I

- initial configuration [2-1](#)
- interface names [2-14](#)
- Internal upgrade server, preparing for use [5-19](#)
- interoperability
 - local controllers and global controllers [3-2](#)
- IP address
 - defaults for MARS [2-5](#)

L

- license
 - 5.x software [2-11](#)
- license key [2-11](#)
 - 5.x software [2-11](#)
 - importing [2-13](#)
- Local Controller [3-14, 3-15](#)
- logging off [4-3](#)
- logging on [4-1](#)
- login
 - default [2-12](#)
- logs

viewing at console [4-7](#)

M

MARS appliance

- administering [4-1](#)
- disaster recovery [6-16](#)
- license key [2-11](#)
- log in [2-11](#)
- log off via console
 - console connection
 - log off [4-3](#)
 - log on via console [4-1](#)
- name of [2-14](#)
- reboot from console [4-4](#)
- reset password [4-2](#)
- shutdown via console [4-3](#)
- upgrade [5-3](#)

MARS software

- version [A-2](#)

N

NetFlow flows per second

- deployment planning [1-1](#)

network routes

- adding [2-10](#)
- deleting [2-10](#)

NFS Server

- Linux [6-9](#)

NTP

- configuration settings [2-10](#)

P

password

- default [2-12](#)
- recovery [4-2, 6-16](#)
- resetting [4-2](#)

- personnel qualifications warning [i-vii](#)

- personnel training warning [i-vii](#)

- pnadmin account, recovery [6-16](#)

- pnlog show command [4-7](#)

ports

- required flows [1-2](#)
- used by MARS [1-2](#)

- processes, see services. [A-12](#)

R

- rebooting [4-4](#)

recovery

- CD ROM [6-16](#)

- DVD [6-16](#)

- password [6-16](#)

- re-image Global Controller [6-20](#)

- re-image Local Controller [6-18](#)

- restore data [6-22](#)

- restore OS [6-17](#)

recovery DVD

- burn bootable [6-17](#)

- burn speed guideline [6-17](#)

- download from [6-16](#)

- format guidelines [6-17](#)

- restore Global Controller [6-20](#)

- restore Local Controller [6-18](#)

- restore OS to flash drive [6-17](#)

- recovery management [6-16](#)

- re-imaging hard drive [6-18, 6-20](#)

restore

- range of days [6-23](#)

routes

- adding [2-10](#)

- deleting [2-10](#)

S

scheduled activities

archive intervals [6-5](#)

search domains [2-16](#)

self-signed certificate [2-12](#)

services

determine status [4-4](#)

expected differences in Global Controller [4-5, 5-9, A-12](#)

expected status [4-5, 5-9, A-12](#)

list of [A-12](#)

starting system [4-6](#)

stopping system [4-6](#)

shutting down [4-3](#)

SSL

self-signed [2-12](#)

starting

archiving [6-14](#)

system services [4-6](#)

status, determining system [4-4](#)

stopping

archiving [6-15](#)

support information

collecting [A-3](#)

get_mars_summary_info.sh script [A-3](#)

pnlog mailto

contents of [A-4](#)

supporting devices

deployment planning [1-1](#)

system administrative account [2-12](#)

T

troubleshoot

cannot add device [A-3](#)

delete device [A-3](#)

error messages [A-15](#)

password recovery [A-2](#)

re-add device [A-3](#)

rename device [A-3](#)

U

updates

software updates [2-18](#)

upgrade

burn CD-ROM [5-18](#)

checklist [5-3](#)

determine upgrade path [5-7](#)

download packages [5-19](#)

from CLI [5-21](#)

from GUI [5-13](#)

Local Controller from Global Controller [5-16](#)

periodic system consistency checks [5-8](#)

prepare internal server [5-19](#)

proxy settings [5-20](#)

V

version

IPS signature version

determine [A-2](#)

MARS software [A-2](#)

W

warnings

regarding

training and qualifications of personnel working on unit [i-vii](#)

Windows Services for UNIX [6-5](#)

create share [6-7](#)

enable logging [6-8](#)

install [6-6](#)

Z

Zone [2-15](#)

