Install and Setup Guide for Cisco Security MARS

Release 5.3.x
March 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-14672-01

Install and Setup Guide for Cisco Security MARS

CONTENTS

Preface

Revised: May 9, 2007, OL-14672-01

This manual describes how to install and prepare the Cisco Security Monitoring, Analysis, and Response System Appliance (MARS Appliance) Version 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 functions 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, "Appliance Overview and Specifications," provides an overview of MARS and presents front and back panel diagrams for each supported appliance.
- Chapter 2, "Deployment Planning Guidelines," provides guidance for device placement and calculating event/second monitoring rates to determine appropriate device monitoring limits.
- Chapter 3, "Preparing for Installation," identifies safety information and site preparation information.
- Chapter 4, "Installing the Appliance," describes how to install the MARS Appliance in a rack.
- Chapter 5, "Initial MARS Appliance Configuration," provides instructions on the initial configuration of the MARS Appliance.

- Chapter 6, "Administering the MARS Appliance," describes how to maintain the appliance. It includes procedures for upgrading the appliance and for performing tasks at the command line using a Secure Shell (SSH) connection. These tasks include backing up data and performing restorations using the Recovery DVD.
- Appendix A, "Command Reference," explains how to use the CLI, and it describes the commands that you can execute from the CLI interface.
- Appendix B, "Troubleshooting," identifies backend services and describes their roles in the system. It also identifies common error messages and helps you troubleshoot known issues.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** font
Variables you enter	*`italic screen`* font
Menu items and button names	**boldface** font
Selecting a menu item	Option > Network Preferences

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning Definition

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the *translated safety warnings* that accompanied this device.

Note: SAVE THESE INSTRUCTIONS

Note: This documentation is to be used in conjunction with the specific product installation guide that shipped with the product. Please refer to the Installation Guide, Configuration Guide, or other enclosed additional documentation for further details.

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Voor een vertaling van de waarschuwingen die in deze publicatie verschijnen, dient u de vertaalde veiligheidswaarschuwingen te raadplegen die bij dit apparaat worden geleverd.

Opmerking BEWAAR DEZE INSTRUCTIES.

Opmerking Deze documentatie dient gebruikt te worden in combinatie met de installatiehandleiding voor het specifieke product die bij het product wordt geleverd. Raadpleeg de installatiehandleiding, configuratiehandleiding of andere verdere ingesloten documentatie voor meer informatie.

Varoitus **TÄRKEITÄ TURVALLISUUTEEN LIITTYVIÄ OHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. Tässä asiakirjassa esitettyjen varoitusten käännökset löydät laitteen mukana toimitetuista ohjeista.

Huomautus SÄILYTÄ NÄMÄ OHJEET

Huomautus Tämä asiakirja on tarkoitettu käytettäväksi yhdessä tuotteen mukana tulleen asennusoppaan kanssa. Katso lisätietoja asennusoppaasta, kokoonpano-oppaasta ja muista mukana toimitetuista asiakirjoista.

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions d'avertissements figurant dans cette publication, consultez les consignes de sécurité traduites qui accompagnent cet appareil.

Remarque CONSERVEZ CES INFORMATIONS

Remarque Cette documentation doit être utilisée avec le guide spécifique d'installation du produit qui accompagne ce dernier. Veuillez vous reporter au Guide d'installation, au Guide de configuration, ou à toute autre documentation jointe pour de plus amples renseignements.

Warnung **WICHTIGE SICHERHEITSANWEISUNGEN**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewusst. Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise sind im Lieferumfang des Geräts enthalten.

Hinweis BEWAHREN SIE DIESE SICHERHEITSANWEISUNGEN AUF

Hinweis Dieses Handbuch ist zum Gebrauch in Verbindung mit dem Installationshandbuch für Ihr Gerät bestimmt, das dem Gerät beiliegt. Entnehmen Sie bitte alle weiteren Informationen dem Handbuch (Installations- oder Konfigurationshandbuch o. Ä.) für Ihr spezifisches Gerät.

Figyelem **FONTOS BIZTONSÁGI ELOÍRÁSOK**

Ez a figyelmezeto jel veszélyre utal. Sérülésveszélyt rejto helyzetben van. Mielott bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplo figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján keresheto meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Per le traduzioni delle avvertenze riportate in questo documento, vedere le avvertenze di sicurezza che accompagnano questo dispositivo.

Nota CONSERVARE QUESTE ISTRUZIONI

Nota La presente documentazione va usata congiuntamente alla guida di installazione specifica spedita con il prodotto. Per maggiori informazioni, consultare la Guida all'installazione, la Guida alla configurazione o altra documentazione acclusa.

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette varselssymbolet betyr fare. Du befinner deg i en situasjon som kan forårsake personskade. Før du utfører arbeid med utstyret, bør du være oppmerksom på farene som er forbundet med elektriske kretssystemer, og du bør være kjent med vanlig praksis for å unngå ulykker. For å se oversettelser av advarslene i denne publikasjonen, se de oversatte sikkerhetsvarslene som følger med denne enheten.

Merk TA VARE PÅ DISSE INSTRUKSJONENE

Merk Denne dokumentasjonen skal brukes i forbindelse med den spesifikke installasjonsveiledningen som fulgte med produktet. Vennligst se installasjonsveiledningen, konfigureringsveiledningen eller annen vedlagt tilleggsdokumentasjon for detaljer.

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. O utilizador encontra-se numa situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha em atenção os perigos envolvidos no manuseamento de circuitos eléctricos e familiarize-se com as práticas habituais de prevenção de acidentes. Para ver traduções dos avisos incluídos nesta publicação, consulte os avisos de segurança traduzidos que acompanham este dispositivo.

Nota GUARDE ESTAS INSTRUÇÕES

Nota Esta documentação destina-se a ser utilizada em conjunto com o manual de instalação incluído com o produto específico. Consulte o manual de instalação, o manual de configuração ou outra documentação adicional inclusa, para obter mais informações.

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Vea las traducciones de las advertencias que acompañan a este dispositivo.

Nota GUARDE ESTAS INSTRUCCIONES

Nota Esta documentación está pensada para ser utilizada con la guía de instalación del producto que lo acompaña. Si necesita más detalles, consulte la Guía de instalación, la Guía de configuración o cualquier documentación adicional adjunta.

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Se översättningarna av de varningsmeddelanden som finns i denna publikation, och se de översatta säkerhetsvarningarna som medföljer denna anordning.

OBS! SPARA DESSA ANVISNINGAR

OBS! Denna dokumentation ska användas i samband med den specifika produktinstallationshandbok som medföljde produkten. Se installationshandboken, konfigurationshandboken eller annan bifogad ytterligare dokumentation för närmare detaljer.

Предупреждение ВАЖНЫЕ СВЕДЕНИЯ ПО БЕЗОПАСНОСТИ

Этот символ предупреждает о наличии опасности. При неправильных действиях возможно получение травм. Перед началом работы с любым оборудованием необходимо ознакомиться с ситуациями, в которых возможно поражение электротоком, и со стандартными действиями для предотвращения несчастных случаев. Переведенный текст предупреждений содержится в соответствующем документе, поставляемом вместе с устройством.

Примечание СОХРАНЯЙТЕ ЭТУ ИНСТРУКЦИЮ
Примечание Эта инструкция должна использоваться вместе с руководством по установке конкретного изделия, входящим в комплект поставки. Дополнительные сведения см. в руководстве по установке, руководстве по настройке и другой документации, поставляемой с изделием.

警告　有关安全的重要说明

这个警告符号指有危险。您所处的环境可能使身体受伤。操作设备前必须意识到电流的危险性，务必熟悉操作标准，以防发生事故。如果需要了解本说明中出现的警告符号的译文，请参阅本装置所附之安全警告译文。

注意　保存这些说明
注意　本文件应与本产品附带的具体安装说明一并阅读。如欲了解详情，请参阅《安装说明》、《配置说明》或所附的其他文件。

警告　安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。このマニュアルに記載されている警告の各国語版は、装置に付属の「Translated Safety Warnings」を参照してください。

注　これらの注意事項を保管しておいてください。
注　この資料は、製品に付属のインストレーション ガイドと併用してください。詳細は、インストレーション ガイド、コンフィギュレーション ガイド、または添付されているその他のマニュアルを参照してください。

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-specifc version of the *Cisco Security MARS Documentation Guide 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

Appliance Overview and Specifications

Revised: March 3, 2008, OL-14672-01

This chapter defines components of the Cisco Security Monitoring, Analysis, and Response System (MARS) and describes the front and backplanes of the various appliance models. This chapter contains the following sections:

System Description

Cisco Security MARS is a security threat mitigation (STM) system. It delivers a range of information about your networks' health as reported by devices in your networks. It processes raw events from your reporting devices, sessionizes[1] them across different devices, evaluates for matching inspection rules (system and user-defined), identifies false positives, and consolidates information using diagrams, charts, queries, reports, and rules.

MARS helps you be more productive by:

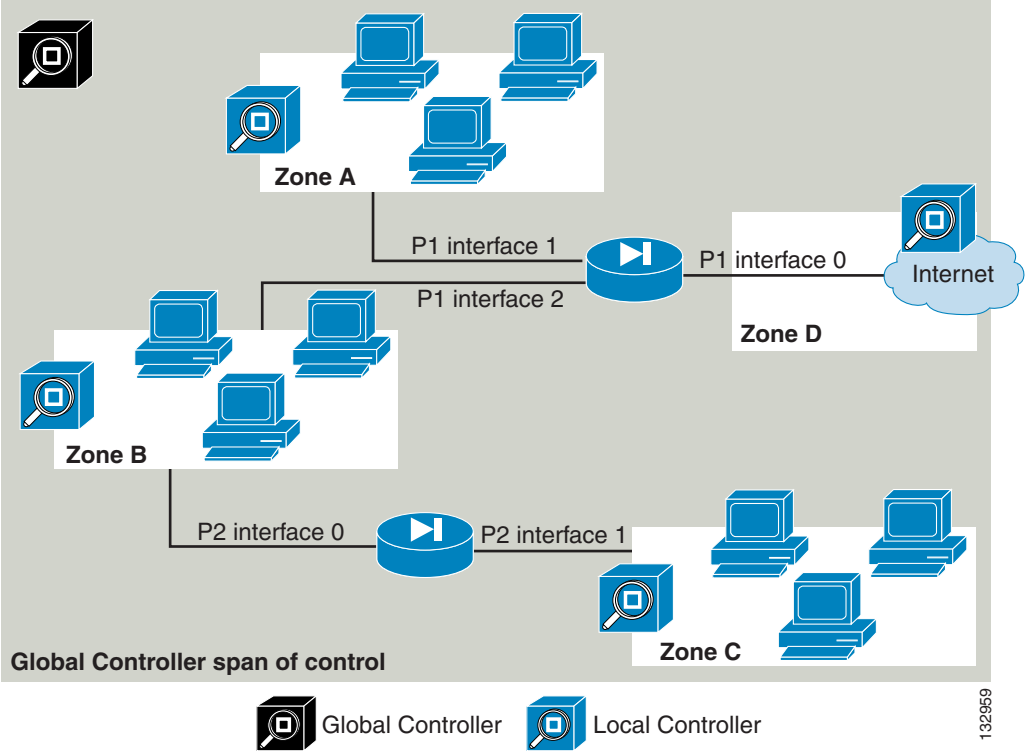
- Reducing the amount of raw data that requires manual review
- Enabling an evolving view of the network security posture
- Identifying hot spots of malicious activity
- Blocking undesirable traffic from the network

The MARS system operates at distinct and separate levels based on how much information is provided about your networks' reporting devices. At its most basic level, MARS functions as a syslog server. As you add information about reporting devices, MARS begins to sessionize the raw data, and after you configure additional reporting devices and enable the more verbose reporting features, it presents a much more comprehensive view of your network, from which you can quickly drill-down to a specific MAC address, for example.

Figure 1-1 presents an example deployment of MARS, which identifies the components of the system and their relationships.

1. Sessionize refers to correlating the reported network data. logs, and events into a higher-level interpretation to identify those packets as part of a single session, or a communication, that has a beginning, a body, and an end.

Figure 1-1 Relationship of Global Controller to Local Controller to Reporting/Mitigation Device



The Cisco Security MARS system comprises the following components:

- Local Controller, page 1-2
- Global Controller, page 1-3
- MARS Web Interface, page 1-3
- Reporting and Mitigation Devices, page 1-3

Local Controller

The Local Controller models are as follows—MARS 25R, 25, 55, 110R, 110, and 210. Each model differs in its ability to process and store events from reporting devices, enabling you to accurately address your needs based on the size of your network and the traffic volume.

Local Controllers receive and pull data from reporting devices, such as firewalls, routers, intrusion detection/prevention systems, and vulnerability assessment systems. Based on the data obtained from those devices, and the level of integration with them, MARS can present you with suggested mitigation rules for detected attacks and, in some cases, push those rules to the mitigation device, which is a network device that contains the attack by restricting network access to the infected hosts.

A Local Controller summarizes information about the health of your network based on data it receives from the reporting devices that it monitors.

The Local Controller performs the following functions:

- Collects all raw events
- Sessionizes events across different devices

- Fires inspection rules for incidents
- Determines false positives
- Delivers consolidated information in diagrams, charts, queries, reports, and notifications
- Detects inactive reporting devices
- Derives set of IOS/IPS Distributed Threat Mitigation (DTM) signatures based on attacks reported by monitored CISCO IPS 5.x appliances
- Acts as a repository for the IOS/IPS DTM signatures, from which IOS/IPS devices can download current signature sets

Global Controller

If you deploy numerous Local Controllers, you can deploy a Global Controller that summarizes the findings of two or more Local Controllers. In this way, the Global Controller enables you to scale your network monitoring without increasing the management burden. The Global Controller provides a single user interface for defining new device types, inspection rules, and queries, and it enables you to manage Local Controllers under its control. This management includes defining administrative accounts and performing remote, distributed upgrades of the Local Controllers. The Global Controller is available in the following models—MARS GC2R and GC2 .

MARS Web Interface

The MARS web interface operates on a client computer. With many features common to both the Local Controller and Global Controller, the web interface uses a tabbed, hyperlinked, browser-based user interface. You access the web interface from any computer that can access the MARS Appliance on your network. For more information on client requirements, see Web Browser Client Requirements, page 3-10.

From the web interface, you can perform most of your administrative functions, including all functions that are not supported at the command line. Although this manual includes procedures for initially configuring the appliance using the web interface, the following publications reference their corresponding web interface:

- *User Guide for Cisco Security MARS Local Controller*
- *User Guide for Cisco Security MARS Global Controller*

Reporting and Mitigation Devices

If you consider the MARS system from a top-down perspective, you see that the Global Controller monitors Local Controllers and that Local Controllers monitor one or more reporting devices. *Reporting devices* provide MARS with data about the network, from traffic flows, as in the case of a router, to the configuration of possible attack targets, such as from a vulnerability assessment system.

A reporting device that can deny a traffic flow is called a *mitigation device* (for example, a switch). MARS provides mitigation support in two forms:

- For supported Layer 3 devices (based on the OSI Network Model), MARS provides you with a suggested device and set of commands that can be used to halt an ongoing, detected attack. You can use this information to manually block the attack.

- For supported Layer 2 devices, MARS recommends a device, a set of commands to halt the ongoing, detected attack, and provides a method for making the configuration changes on your behalf.

How you configure your reporting devices and mitigation devices greatly affects the ability of MARS to detect ongoing attacks. You can learn more about how to configure these devices in the following:

- *User Guide for Cisco Security MARS Local Controller*
- *User Guide for Cisco Security MARS Global Controller*

For a complete list of the supported reporting and mitigating devices, see:

- *Supported and Interoperable Devices and Software for Cisco Security MARS Local Controller 4.3.x and 5.3.x*
- *Supported and Interoperable Devices and Software Versions for Cisco Security MARS Global Controller 4.3.x and 5.3.x*

Network Cable Requirements

Warning **To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.**

The Ethernet connectors are designed for attaching an unshielded twisted pair (UTP) Ethernet cable equipped with standard RJ-45 compatible plugs. Press one end of the UTP cable into the Ethernet connector until the plug snaps securely into place. Connect the other end of the cable to an RJ-45 port on a hub or other device, depending on your network configuration. Observe the following cabling restrictions for 10BASE-T, 100BASE-TX, and 1000BASE-TX networks:

- For 10BASE-T networks, use Category 3 or greater wiring and connectors.
- For 100BASE-TX and 1000BASE-TX networks, use Category 5 or greater wiring and connectors.
- The maximum cable run length is 328 feet or 100 meters.

Hardware Descriptions—MARS 25R, 25, 55, 110R, 110, 210, GC2R, and GC2

The Cisco Security MARS 25R, 25, 55, 110R, 110, 210, GC2R, and GC2 appliances are built with the second generation of CS-MARS hardware, and operate with only CS-MARS software versions 5.X.

This section consists of the following subsections:

- MARS 110R, 110, 210, GC2R, and GC2 Front and Back Panels, page 1-17

Technical Specifications for MARS 25R, 25, and 55

Table 1-1 summarizes chassis and component descriptions; Table 1-2 summarizes environmental and electrical descriptions.

Table 1-1 Technical Specifications—MARS 25R, 25, and 55

Chassis Feature	MARS 25R and MARS 25	MARS 55
Maximum Weight	15 kg (33 lbs)	18.14 kg (40lbs)
Dimensions	Rack (1U) Height: 4.24 cm (1.67 in) Width w/o rails: 43.00 cm (16.93 in) Depth 50.80 cm (20 in)	Rack (1U) Height: 4.24 cm (1.67 in) Width w/o rails: 43.00 cm (16.93 in) Depth 64.80 cm (25.51 in)
Power Supplies	350W ATX	350W ATX
Front Side Bus	1067 MHz	1067 MHz
Integrated Network Controller	NIC 1–Embedded Intel 82573 E/V (Tekoa) 10/100/1000 Gigabit Ethernet Controller NIC 2–Embedded Intel 82541 PI (Tabor) 10/100/1000 Gigabit Ethernet Controller	NIC 1–Embedded Intel 82573 E/V (Tekoa) 10/100/1000 Gigabit Ethernet Controller NIC 2–Embedded Intel 82541 PI (Tabor) 10/100/1000 Gigabit Ethernet Controller
Modem	US Robotics 56k V.92 Performance Pro Modem (USR802972B-OEM	US Robotics 56k V.92 Performance Pro Modem (USR802972B-OEM
Hard Drive Storage	1x 250GB SATA-IO 3.0 Gps HDD 7200RPM, 16 MB Buffer	500 GB RAID 1 2x 500 SATA-IO 3.0 Gps HDD 7200RPM, 32 MB Buffer Hot-Swappable Front Accessible
DVD-ROM	Slimline optical drive	Slimline optical drive
System battery	Lithium button cell	Lithium button cell

Table 1-2 Environmental Parameters—MARS 25, 25R, and 55

Environmental Parameter	MARS 25R and MARS 25	MARS 55
Temperature range	Operating: +10°C to +35°C derated 0.5 °C for every 1,000 ft (305 m) to a maximum of 10,000 ft. The maximum rate of change not to exceed 10°C per hour Non-operating: –40° C to +70° C	Operating: +10°C to +35°C derated 0.5 °C for every 1,000 ft (305 m) to a maximum of 10,000 ft. The maximum rate of change not to exceed 10°C per hour Non-operating: –40° C to +70° C
Humidity (non-operating)	90% relative humidity, Non-condensing at +35°C	90% relative humidity, Non-condensing at +35°C
System Cooling Requirement	1,194 BTU/hour max. (350W)	1,194 BTU/hour max. (350W)
Vibration	Unpackaged: 5 Hz to 500 Hz, 2.20 g RMS random	Unpackaged: 5 Hz to 500 Hz, 2.20 g RMS random
Shock	Operating: Half sine, 2 g peak, 11 mSec Unpackaged: Trapezoidal, 25 g, velocity change 136 inches/sec Packaged: 18 inches in non-palletized free fall (>= 40 lbs to < 80 lbs)	Operating: Half sine, 2 g peak, 11 mSec Unpackaged: Trapezoidal, 25 g, velocity change 136 inches/sec Packaged: 18 inches in non-palletized free fall (>= 40 lbs to < 80 lbs)
Acoustic Noise	Sound Pressure: 55 dBA (Rack mount) in an idle state at typical office ambient temperatures Sound Power: 7.0 bels in an idle state at typical office ambient temperatures.	Sound Pressure: 55 dBA (Rack mount) in an idle state at typical office ambient temperatures Sound Power: 7.0 bels in an idle state at typical office ambient temperatures.
Electrostatic discharge (ESD)	Tested to +/-15 kilovolts (kV) with no component damage.	Tested to +/-15 kilovolts (kV) with no component damage.

Technical Specifications for MARS 110R, 110, 210, GC2, and GC2R

Table 1-3 summarizes chassis and component descriptions; Table 1-4 summarizes environmental and electrical descriptions.

Table 1-3 Technical Specifications—MARS 110R, 110, 210, GC2, and GC2R

Chassis Feature	MARS 110R and 110	MARS 210, GC2R, and MARS GC2
Maximum Weight	29.5 kg (65 lbs)	29.5 kg (65 lbs)
Dimensions	2 Rack Units (2U) Height: 87.3 mm (3.44 in) Width w/o rails: 430 mm (16.93 in) Width with rails: 451.3 mm (17.77 in) Depth: 704.8 mm (27.75 in)	2 Rack Units (2U) Height: 87.3 mm (3.44 in) Width w/o rails: 430 mm (16.93 in) Width with rails: 451.3 mm (17.77 in) Depth: 704.8 mm (27.75 in)
Power Supplies	2 X 750W Redundant (1 + 1) ATX Hot-swappable 100-240 VAC 50-60Hz	2 X 750W Redundant (1 + 1) ATX Hot-swappable 100-240 VAC 50-60Hz
Power Consumption	11A maximum @110 VAC 5.5A maximum @ 220 VAC	11A maximum @110 VAC 5.5A maximum @ 220 VAC
Integrated Network Controller	Dual Intel 82563 EB 10/100/1000 PHYs supporting Intel I/O Acceleration Technology	Dual Intel 82563 EB 10/100/1000 PHYs supporting Intel I/O Acceleration Technology
PCI NIC	Dual Port Intel Pro/1000 PT Network Controller	Dual Port Intel Pro/1000 PT Network Controller
Modem	US Robotics 56k V.92 Performance Pro Modem (USR5610B) or US Robotics 56k V.92 Performance Pro Modem (USR802972A-OEM)	US Robotics 56k V.92 Performance Pro Modem (USR5610B) or US Robotics 56k V.92 Performance Pro Modem (USR802972A-OEM)
Hard Drive Storage	1.5TB RAID 10 6 X 500GB SATA-IO 3.0 Gps HDD 7200 RPM, 16MB Buffer Hot-swappable Front accessible	2.0 TB[1] RAID 10 6 X 750GB SATA-IO 3.0 Gps HDD 7200 RPM, 16 MB Buffer Hot-swappable Front accessible
DVD-ROM	Slimline IDE DVD-ROM	Slimline IDE DVD-ROM
System battery	Lithium button cell	Lithium button cell

1. Although there is a total of 4.5 TB storage, RAID 10 has a maximum size configuration of 2 TB Redundant, or 4 TB total

Table 1-4 Environmental Parameters—MARS 110R, 110, 210, GC2R, and GC2

Environmental Parameter	MARS 110R and MARS 110	MARS 210, GC2R, and GC2
Temperature range	Operating: +10°C to +35°C derated 0.5 °C for every 1,000 ft (305 m) to a maximum of 10,000 ft. The maximum rate of change not to exceed 10°C per hour Non-operating: –40° C to +70° C	Operating: +10°C to +35°C derated 0.5 °C for every 1,000 ft (305 m) to a maximum of 10,000 ft. The maximum rate of change not to exceed 10°C per hour Non-operating: –40° C to +70° C
Humidity (non-operating)	90% relative humidity, Non-condensing at +30°C	90% relative humidity, Non-condensing at +30°C
System Cooling Requirement	1,826 BTU/hour (535W)	1,826 BTU/hour (535W)
Vibration	Unpackaged: 5 Hz to 500 Hz, 2.20 g RMS random	Unpackaged: 5 Hz to 500 Hz, 2.20 g RMS random
Shock	Operating: Half sine, 2 g peak, 11 mSec Unpackaged: Trapezoidal, 25 g, velocity change 136 inches/sec Packaged: 18 inches in non-palletized free fall (>= 40 lbs to < 80 lbs)	Operating: Half sine, 2 g peak, 11 mSec Unpackaged: Trapezoidal, 25 g, velocity change 136 inches/sec Packaged: 18 inches in non-palletized free fall (>= 40 lbs to < 80 lbs)
Acoustic Noise	Sound Pressure: 55 dBA (Rack mount) in an idle state at typical office ambient temperatures Sound Power: 7.0 bels in an idle state at typical office ambient temperatures.	Sound Pressure: 55 dBA (Rack mount) in an idle state at typical office ambient temperatures Sound Power: 7.0 bels in an idle state at typical office ambient temperatures.
Electrostatic discharge (ESD)	Tested to 15 kilovolts (kV) with no component damage.	Tested to 15 kilovolts (kV) with no component damage.

Part Numbers, License Key, and Serial Numbers

The part numbers of Cisco Security MARS Appliances and the Field Replaceable Units (FRUs) that operate with software releases 5.X are as follows:

Local Controller Appliances

- CS-MARS-25R-K9
- CS-MARS-25-K9
- CS-MARS-55-K9
- CS-MARS-110R-K9
- CS-MARS-110-K9
- CS-MARS-210-K9

Global Controller Appliances

- CS-MARS-GC2R-K9
- CS-MARS-GC2-K9

FRU Description	FRU Part Number
SR2500 (Driskill 2) 750 Watt Power Supply Module (MARS 110R, 110, 210, GC2R, GC)	CS-MARS-D750-PS =
500 GB SATA-IO HDD (MARS 55)	CS-MARS-H500-HD =
500 GB SATA-IO HDD (MARS 110R, 110)	CS-MARS-S500-HD =
750 GB SATA-IO HDD (MARS 210, GC2R, GC)	CS-MARS-S750-HD =
RAID Controller Back-Up Battery Unit (MARS 110R, 110, 210, GC2R, GC)	CS-MARS-X10-BB =
Rack-mount Kit (MARS 110R, 110, 210, GC2R, GC)	CS-MARS-X10-RAIL=

Serial Numbers

If you have difficulty identifying or physically locating the serial number sticker on your appliance chassis, use the Cisco Product Identification Tool at the following URL:

http://tools.cisco.com/Support/CPI/index.do

You must be registered with Cisco Systems Customer Connection Online to access this tool. If you are not registered, you can register at the following URL:

http://tools.cisco.com/RPF/register/register.do

The chassis, hard drive, and power supply serial numbers are also reported in the **show inventory** CLI command.

License Key

The license key sticker is on the chassis, and on the Recovery DVD case shipped with your product.

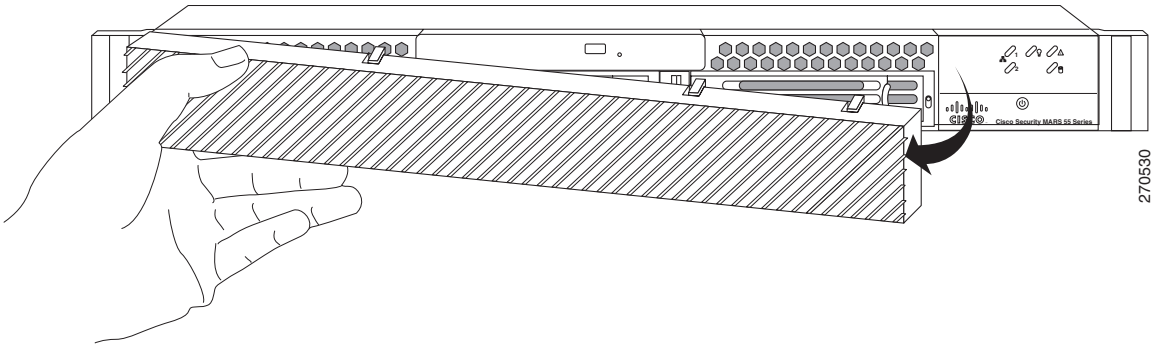
Removing and Replacing the Front Bezel

For the MARS 55, 110R, 110, 210, GC2R, and GC2, you must remove the front bezel to access the DVD ROM, hard drives, and control panel buttons. The bezels do not lock. The MARS 25R and 25 front panel features are accessible without removing the bezel.

MARS 55

To remove the MARS 55 bezel, support the left-side hinge with your hand, as shown in Figure 1-2. Pull the bezel from the right-hand side, swing open, then gently detach left-hand side from hinge.

Figure 1-2 Removing the Front Bezel from a MARS 55

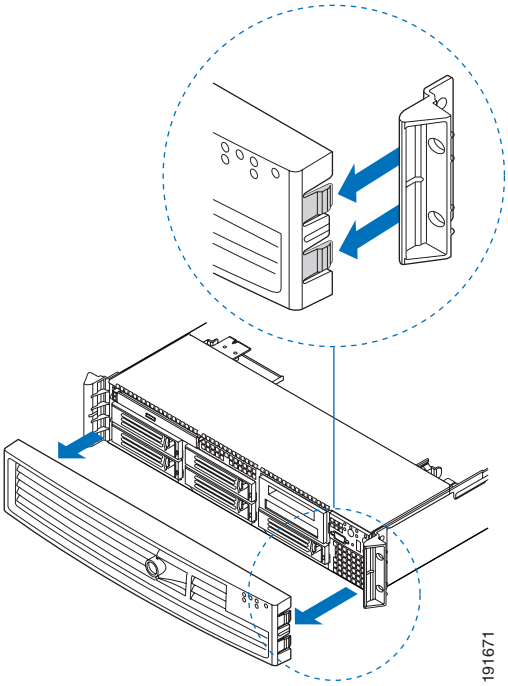


MARS 110, 110R, 210, GC2R, and GC2

To remove the bezel form the, pull the bezel from the appliance, as shown in Figure 1-3.

To replace the bezel, line up the center notch on the bezel with the center guide on the rack handles, then push the bezel onto the front of the MARS Appliance until it clicks into place.

Figure 1-3 Removing the Front Bezel from a MARS 110R, 110, 210, GC2, and GC2R



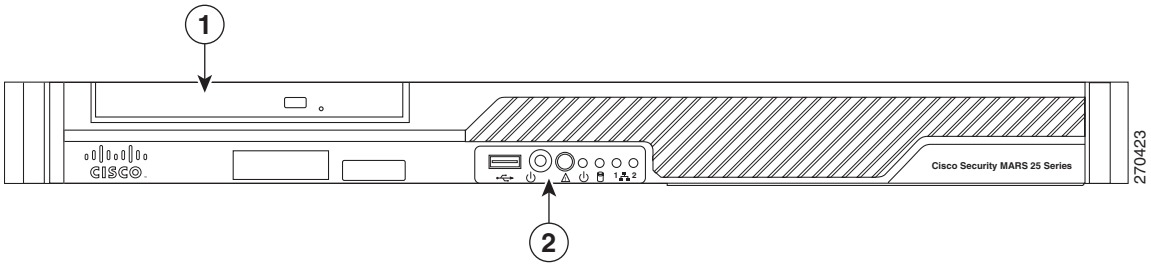
MARS 25R and 25 Front and Back Panels

Front Panel Features—MARS 25 and 25R

The front panel elements are shown in Figure 1-4 and described in the following subsections:

- Control Panel Description—MARS 25R and 25, page 1-11
- Control Panel LED Descriptions—MARS 25R and 25, page 1-12

Figure 1-4 Front Panel—MARS 25R and 25

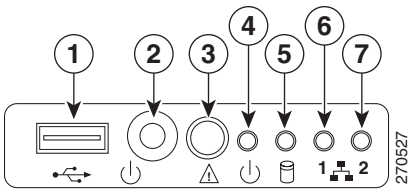


1	Slimline Optical DVD drive	**2**	Control Panel

Control Panel Description—MARS 25R and 25

The control panel power button and status LEDs are supported. Figure 1-5 shows the layout and functions of the control panel.

Figure 1-5 Control Panel Elements—MARS 25R and 25



1	USB Port 2 (not supported)	**2**	Power On/Off Button
3	Not used	**4**	System Power LED
5	Hard Drive Activity LED	**6**	NIC 1 LED
7	NIC 2 LED		

Control Panel LED Descriptions—MARS 25R and 25

Table 1-5 describes the function of control panel LEDs.

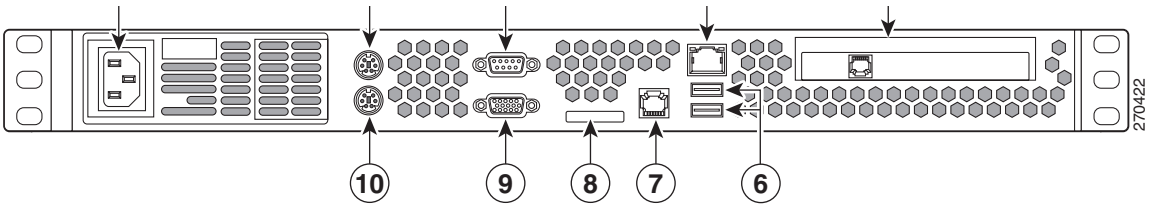
Table 1-5 Control Panel LEDs—MARS 25R and 25

Figure 1-5 Reference Number	Control Panel LED	State Description
3	Not used	
4	**Power On/Off LED**	**Steady Green**—Legacy power on **Blinking Green**—Sleep state (not supported) **Off**—Power is off.
5	**Hard Drive LED**	**Random blinking**—Indicates disk activity **Off**—No disk activity
6	**NIC 1 LED**	**Steady Green**—NIC has link
7	**NIC 2 LED**	**Blinking Green**—NIC Activity

Back Panel Features—MARS 25R and 25

Figure 1-6 depicts the back panel of the MARS 25R, 25, and 55 appliances.

Figure 1-6 Back Panel—MARS 25R, 25, and 55



1	AC Power Connector	2	PS2 Mouse Port
3	DB9 Serial Port	4	NIC 1 or eth0 (10/100/1000 Mps)
5	Modem	6	USB Ports 0 and 1 (not supported)
7	NIC 2 or eth1 (10/100/1000 Mps)	8	Diagnostic LEDs (4)[1]
9	VGA Video Connector	10	PS2 Keyboard Port

1. Used by Technical Assistance Center for troubleshooting.

MARS 55 Front and Back Panels

Front Panel Features—MARS 55

The front panel elements are shown in Figure 1-8 and described in the following subsections:

- Control Panel Description—MARS 55, page 1-14
- Control Panel LED Descriptions—MARS 55, page 1-14

Figure 1-7 Front Panel—MARS 55 with Bezel

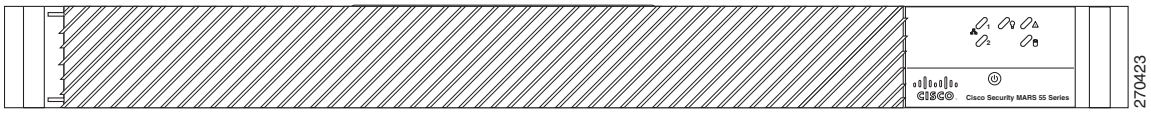
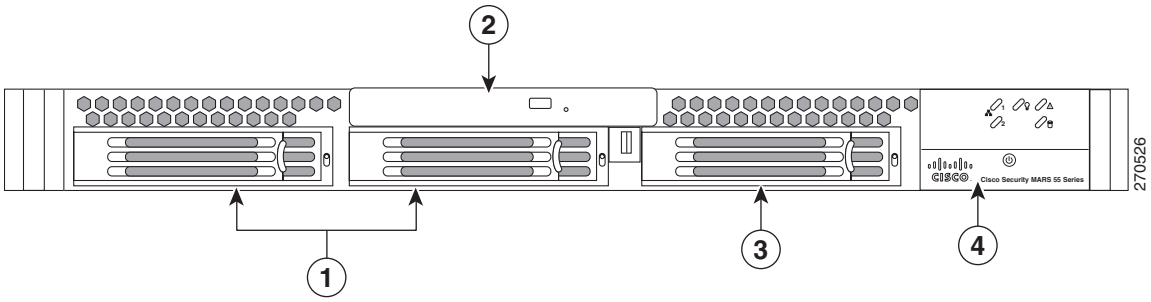


Figure 1-8 Front Panel—MARS 55 with Bezel Removed



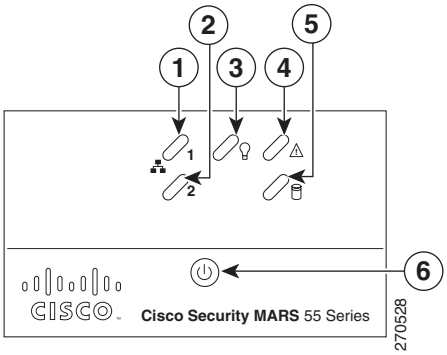
1	Hard drives	**2**	Slimline Optical DVD drive
3	Empty Hard Drive Bay with Spare Carrier	**4**	Control Panel

Note To maintain the proper air pressure within the system, all hard drive bays must be populated with either a hard drive, or a drive blank.

Control Panel Description—MARS 55

The MARS 55 control panel has a power button and status LEDs. Figure 1-9 shows the layout and functions of the control panel.

Figure 1-9 Control Panel Elements—MARS 55



1	NIC 1 LED	**2**	NIC 2 LED
3	System Power LED	**4**	Not used
5	Hard Drive Activity LED	**6**	Power On/Off Button

Control Panel LED Descriptions—MARS 55

Table 1-6 describes the function of control panel LEDs.

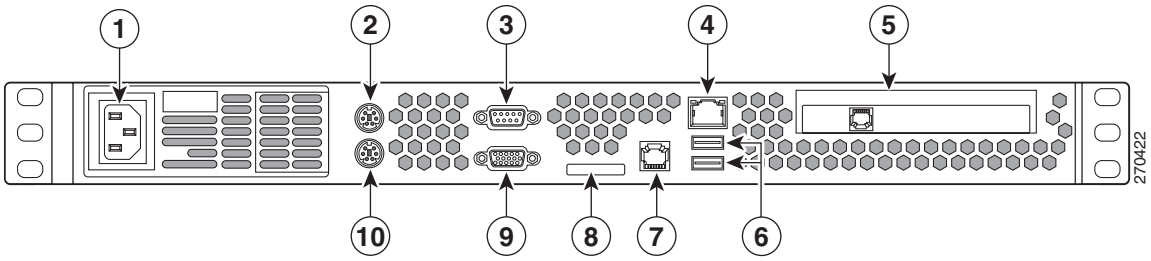
Table 1-6 Control Panel LEDs—MARS 55

Figure 1-9 Reference Number	Control Panel LED	State Description
1	**NIC 1 LED**	**Steady Green**—NIC has link
2	**NIC 2 LED**	**Blinking Green**—NIC Activity
3	**Power On/Off LED**	**Steady Green**—Legacy power on **Blinking Green**—Sleep state (not supported) **Off**—Power is off.
4	Not used	
5	**Hard Drive LED**	**Random blinking**—indicates disk activity **Off**—No disk activity

Back Panel Features—MARS 55

Figure 1-10 depicts the back panel of the MARS 55 appliance.

Figure 1-10 Back Panel—MARS 25R, 25, and 55

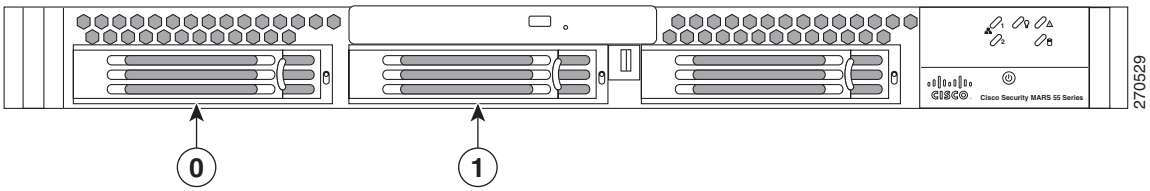


1	AC Power Connector	**2**	PS2 Mouse Port
3	DB9 Serial Port	**4**	NIC 1 or eth0 (10/100/1000 Mps)
5	Modem	**6**	USB Ports 0 and 1 (not supported)
7	NIC 2 or eth1(10/100/1000 Mps)	**8**	Diagnostic LEDs (4)[1]
9	VGA Video Connector	**10**	PS2 Keyboard Port

1. Used by Technical Assistance Center for troubleshooting.

Hard Drive Slot Number Layout—MARS 55

Figure 1-11 Hard Drive Slot Numbers



MARS Appliance	Storage Capacity[1]	Hard Drive Slot to PD Numbers	RAID 1 Pairs
MARS 55	500GB RAID 1 2 X 500GB SATA-IO 3.0 Gps HDD 7200 RPM, 32 MB Buffer Hot-Swappable Front Accessible	Slot **0** is **Port 0** Slot **1** is **Port 1**	Slot **0** and Slot **1**

1. The stated storage capacity is the sum of the rated capacity of all the hard drives and does reflect bytes reserved for the RAID overhead on each drive.

Power Supply Description—MARS 25R, 25, and 55

The MARS 25R, 25, and 55 have a 350 watt ATX power supply (PS) with the following features:

- Over-temperature protection (OTP)
- Over-current protection (OCP)
- Over-voltage protection (OVP)

Over-Temperature Protection (OTP)

The power supply is protected against over-temperature conditions caused by loss of fan cooling or excessive ambient temperature. In an OTP condition the power supply will shutdown. When the power supply temperature drops to the rated safety limit, the power supply restores power automatically, while a 5 V standby remains constantly on. The power supply alerts the system of the OTP condition with the power supply FAIL signal and the Power LED on the control panel.

Over-Current Protection (OCP)

The power supply and power distribution board shutdown and latch off after an over-current condition occurs. This latch is cleared by an AC power interruption.

Over-Voltage Protection (OVP)

The power supply and power distribution board shutdown and latch off after an over-voltage condition occurs. This latch is cleared by an AC power interruption.

AC Power Source Requirements

The power supply operates within the parameters listed in Table 1-7.

Table 1-7 MARS 25R, 25, and 55 Power Maximums and Minimums

Parameter	110 Line Voltage	220 Line Voltage
Minimum	90 V^{rms}	180 V^{rms}
Rated	100–127 V^{rms}	200–240 V^{rms}
Maximum	140 V^{rms}	264 V^{rms}
Start-up VAC	85 VAC +/– 4 VAC	
Power Off VAC	75 VAC +/– 5 VAC	
Maximum Input AC Current[1]	6.0 A^{rms}	3.0 A^{rms}
Frequency	Minimum: 47 Hz; Rated: 50/60 Hz; Maximum: 63 Hz	

1. Maximum input current value is measured at maximum load and minimum voltage (90VAC for 110 line voltage, 180VAC for 220 line voltage.

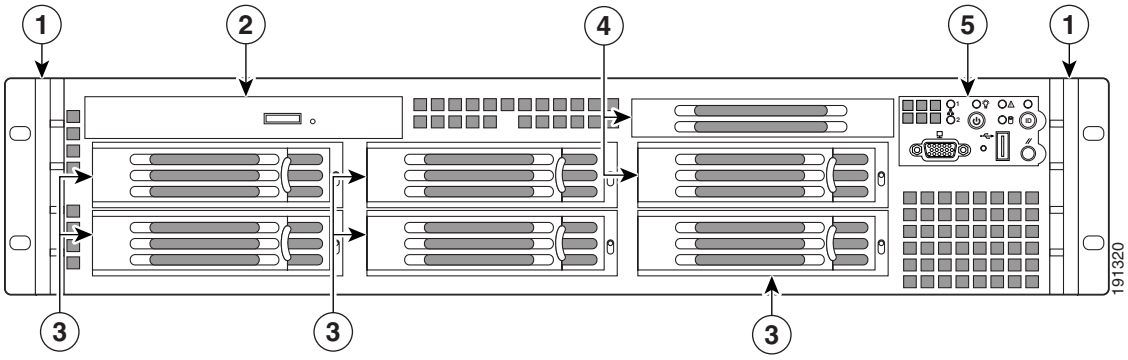
MARS 110R, 110, 210, GC2R, and GC2 Front and Back Panels

Front Panel Features—MARS 110R, 110, 210, GC2R, and GC2

The front panel elements are shown in Figure 1-12 and described in the following subsections:

- Control Panel Description—MARS 110R, 110, 210, GC2R, and GC2, page 1-18
- Control Panel LED Descriptions—MARS 110R, 110, 210, GC2R, and GC2, page 1-20

Figure 1-12 Front Panel of MARS 110R, 110, 210, GC2R, and GC2—with Bezel Removed



1	Rack Handles	**2**	Slim-Line DVD-ROM
3	Hard Drive Bays (5 total)	**4**	Flex Bay—MARS uses the Flex Bay as the 6th hard drive.
5	Standard Control Panel		

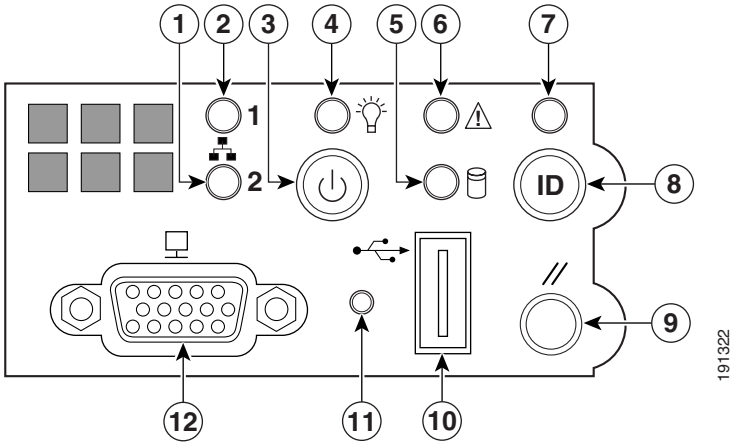
Note The USB ports on the front and back panels are not supported.

Note To maintain the proper air pressure within the system, all hard drive bays must be populated with either a hard drive, or a drive blank.

Control Panel Description—MARS 110R, 110, 210, GC2R, and GC2

The standard control panel supports several push buttons and status LEDs. Figure 1-13 shows the layout and functions of the control panel. The Universal Serial Bus (USB) port is not supported.

Figure 1-13 Control Panel Elements—MARS 110R, 110, 210, GC2R, and GC2



1	NIC 2 activity LED	**2**	NIC 1 activity LED
3	Power on/off button—Toggles the system power on and off. Use for hard power-downs when a software shut down cannot be performed.	**4**	Power LED
5	Hard drive activity LED	**6**	System status LED

7	System Identification LED—Toggles the front and rear panel System ID LEDs on/off enabling you to more easily locate the appliance from behind a rack.	**8**	System identification button
9	System Reset button—Reboots and initializes the system. Use for system restarts and initialization when a software reboot cannot be performed. Data in memory is lost, but RAID cache data is preserved.	**10**	USB 2.0 Connector (Not supported)
11	Recessed Non-maskable Interrupt (NMI) Button (Tool Required)—Diagnostic function used by Cisco TAC	**12**	VGA video-out connector—Standard VGA video-out connector. Attach an external monitor and a keyboard to the appliance to access the command line interface. It cannot be used at the same time as the back panel VGA connector.

Control Panel LED Descriptions—MARS 110R, 110, 210, GC2R, and GC2

Table 1-8 describes the function of control panel LEDs.

Table 1-8 Control Panel LEDs—MARS 110R, 110, 210, GC2R, and GC2

Control Panel LED	Figure 1-13 Reference Number	State Description
NIC 1 or NIC 2 LED	2, 1	**Steady Green**—NIC has link **Blinking Green**—NIC Activity
Power On/Off LED	4	**Steady Green**—Legacy power on **Blinking Green**—Sleep state (not supported) **Off**—Power is off.
System Identification LED	7	**Note** **This LED is also on the back panel** **Solid Blue**—Blue identification LEDs are on **Off**—Blue identification LEDs are off

Table 1-8 Control Panel LEDs—MARS 110R, 110, 210, GC2R, and GC2

Control Panel LED	Figure 1-13 Reference Number	State Description
System Status LED	6	**Note** **This LED is also on the back panel** **Alternating Green and Amber Blink**—Pre-DC 5V standby power is on. There are 15–20 seconds of system initialization when AC is applied to the appliance. The control panel buttons are disabled until initialization is complete. **Solid Green**—System booted and ready **Blinking Green**—Degraded system, may be due to the following: • Cannot use some of the installed memory • Redundancy loss such as a power-supply or a fan • CPU failed or disabled • Fan alarm or fan failure. The number of operational fans should be more than the minimum number required to cool the system • Non-critical threshold crossed such as temperature or voltage. **Solid Amber**—Fatal alarm, the system has failed or shutdown possibly due to one of the following conditions: • DIMM failure • Run-time memory uncorrectable error in non-redundant mode • IERR signal asserted • Processor 1 missing • Temperature threshold crossed • Power fault • Processor configuration error **Blinking Amber**—Non-fatal alarm but system is likely to fail possibly due to one of the following conditions: • Critical voltage threshold crossed • Minimum number of fans to cool the system failed or not present **Off**—POST is running or system is off

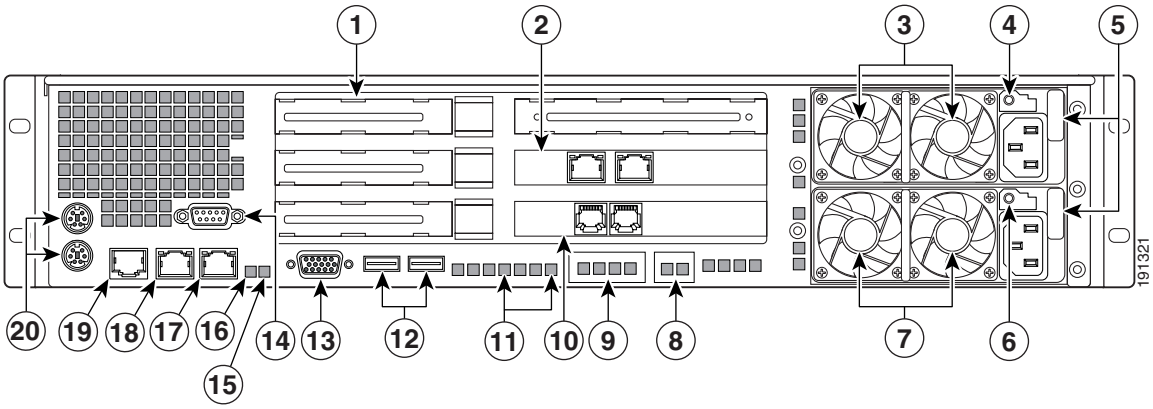
Table 1-8 Control Panel LEDs—MARS 110R, 110, 210, GC2R, and GC2

Control Panel LED	Figure 1-13 Reference Number	State Description
Hard Drive LED	**5**	**Random blinking**—indicates disk activity **Off**—No disk activity

Back Panel Features—MARS 110R, 110, 210, GC2R, and GC2

Figure 1-14 depicts the back panel of the MARS 110R, 110, 210, GC2R, and GC2 appliances.

Figure 1-14 Back Panel—MARS 110R, 110, 210, GC2R, and GC2



1	(Not supported). Low Profile Add-in Slots for PCIe Cards	**2**	(Not supported). Add-in 10/100/1000 Network Interface Card
3	Fans—Upper Power Supply Module	**4**	LED and power receptacle for the upper power supply module
5	Power supply locking levers	**6**	LED and power receptacle for the lower power supply module
7	Fans—Lower Power Supply Module	**8**	(Not supported). Intel® I/O Expansion Module bay
9	(Not supported). Intel® Remote Management Module NIC bay	**10**	56K modem (Line In and Telephone connectors)
11	POST Progress LEDs (4)	**12**	(Not supported). USB port 5 and USB port 6
13	VGA Video-out connector	**14**	DB-9 Serial A connector
15	Blue System Identification LED	**16**	System Status LED
17	Integrated NIC 2 (eth1-10/100/1000 Mbps)	**18**	Integrated NIC 1 (eth0-10/100/1000 Mbps)
19	RJ45 Serial B connector	**20**	PS/2 keyboard and mouse connectors

Connector Descriptions

Table 1-9 describes the type and function of the back panel communication ports of the MARS 110R, 110, 210, GC2R, and GC2.

Table 1-9 Communication Port Descriptions—MARS 110R, 110, 210, GC2R, and GC2

Connector	Description
DB-9 Serial	Table 1-10 lists the pin number assignments for the 9-pin D-subminiature serial port connector.
RJ-45 Serial	Table 1-11 lists the pin numbers assignments for the RJ-45 serial port connector.
Modem Line-in	The MARS Appliance has a V.90 modem for sending SMS and pager alerts. Connect the line-in port to the wall jack using the provided standard telephone cable (RJ-11 connectors).
Modem External Telephone	You can connect a POTS telephone to the telephone port with a standard telephone cable (RJ-11 connectors).
VGA Port	Connect a monitor to this standard VGA port, and a keyboard to the keyboard port to view the console logs and to access the command line interface. It cannot be used at the same time as the Front Panel VGA connector.
Keyboard	PS/2 keyboard connector. To access the console logs, or the command line interface connect a keyboard to the keyboard connector and a monitor to the VGA port.
Mouse	PS/2 mouse port. Not supported.
USB Ports (0 and 1)	Not supported.

Table 1-9 Communication Port Descriptions—MARS 110R, 110, 210, GC2R, and GC2

Connector	Description
Ethernet Add-in NIC connectors	Not supported.
Integrated Ethernet NIC connectors (eth0 and eth1)	10/100/1000–megabit-per-second (Mbps) autosensing Ethernet ports (autosensing detects line speed and duplex mode). MARS supports the operation of both Ethernet connectors. Table 1-8 lists LED descriptions. NIC 1 is eth0 and NIC 2 is eth1. Each Ethernet connector provides all the functions of a network expansion card and supports the 10BASE-T, 100BASE-TX, and 1000BASE-TX Ethernet standards. The MARS Appliance monitors network traffic destined to the IP address assigned to eth0. The eth0 connector is the port to which the **gateway** command applies. Therefore, eth0 must be attached to the network from which the reporting devices are accessible. The eth1 connector is typically used as an out-of-band management network, which provides faster graphical user interface (GUI) response to the administrator. To use eth1, you must define static routes to the destination networks for that interface.

Figure 1-15 Pin Numbers for the Serial Port Connector

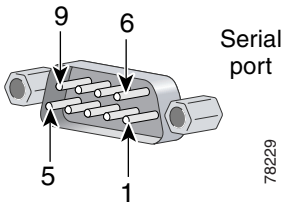


Table 1-10 DB-9 Serial Port Pin-outs

Pin	Signal Name	Description
1	SPA_DCD	DCD (Carrier Detect)
2	SPA_DSR	DSR (Data Set Ready)
3	SPA_SIN_L	RXD (Receive Data)
4	SPA_RTS	RTS (Request to Send)
5	SPA_OUT_N	TXD (Transmit Data)
6	SPA_CTS	CTS (Clear to Send)
7	SPA_DTR	DTR (Data Terminal Ready)
8	SPA_RI	RI (Ring Indicate)
9	GND	Ground

Table 1-11 RJ-45 Serial Port Pin-outs

Pin	Signal Name	Description
1	SPB_RTS	RTS (Request to Send)
2	SPB_DTR	DTR (Data Terminal Ready)
3	SPB_OUT_N	TXD (Transmit Data)
4	GND	Ground
5	SPA_RI	RI (Ring Indicate)
6	SPA_SIN_N	RXD (Receive Data)
7	SPB_DSR	DSR (Data Set Ready)
8	SPB_CTS	CTS (Clear to Send)

Table 1-12 Back Panel LED Descriptions

Back Panel LED	Figure 1-14 Reference Number	Activity Description
Power supply LEDs	**4**	See Power Supply LED Descriptions, page 1-28
POST Progress LEDs	**10**	Available in field service documentation
System Identification LED	**14**	See Table 1-8
System Status LED	**15**	See Table 1-8.
Integrated NIC LEDs	**17, 18**	**Left LED** • **Off**—No network connection • **Solid Amber**—Network connection in place • **Blinking Amber**—Transmit/receive activity **Right LED** • **Off**—10 Mbps connection (if left LED is active) • **Solid Amber**—100 Mbps connection • **Solid Green**—1000 Mbps connection

Hard Drive Layout

Figure 1-16 Hard Drive Slot Numbers—MARS 110R, 110, 210, GC2R, and GC2

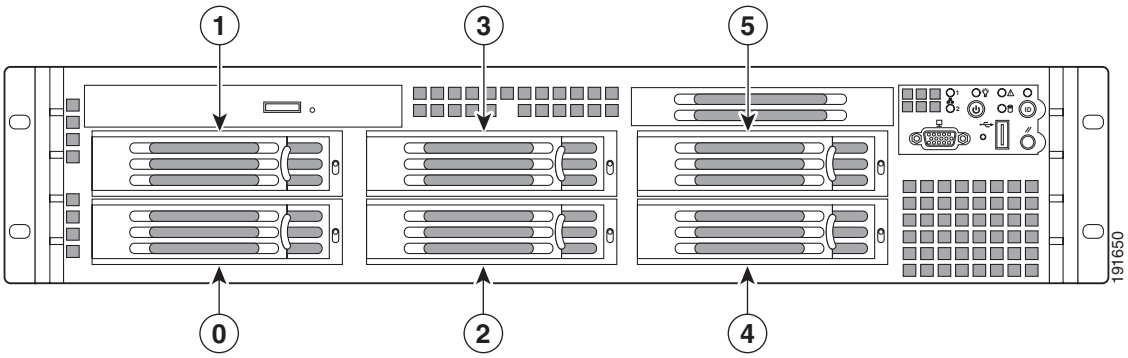


Table 1-13 Hard Drive Slot Number to CLI PD number—MARS 110R, 110, 210, GC2R, and GC2

MARS Appliance	Storage Capacity[1]	Hard Drive Slot to PD Numbers	RAID 1 Pairs
MARS 110R, 110	1.5TB RAID 10 Hot-swappable Front accessible 6 X 500GB SATA-IO HDD, Seagate Barracuda ES 3 TB 3.0Gps, 7200 RPM, 16MB Buffer	Slot **0** is **p0** Slot **1** is **p1** Slot **2** is **p2** Slot **3** is **p3** Slot **4** is **p4** Slot **5** is **p5**	Slot **0** and Slot **1** Slot ***2*** and Slot **3** Slot **4** and Slot **5**
MARS 210, GC2R, GC2	2.0TB[2] RAID 10 Hot-swappable Front accessible 6 X 750GB SATA-IO HDD, Seagate Barracuda ES 3 TB 3.0Gps, 7200 RPM, 16MB Buffer		

1. The stated storage capacity is the sum of the rated capacity of all the hard drives and does reflect bytes reserved for the RAID overhead on each drive.
2. Although there is a total of 4.5 TB storage, RAID 10 has a maximum size configuration of 2 TB Redundant, or 4 TB

Redundant Power Supply Descriptions

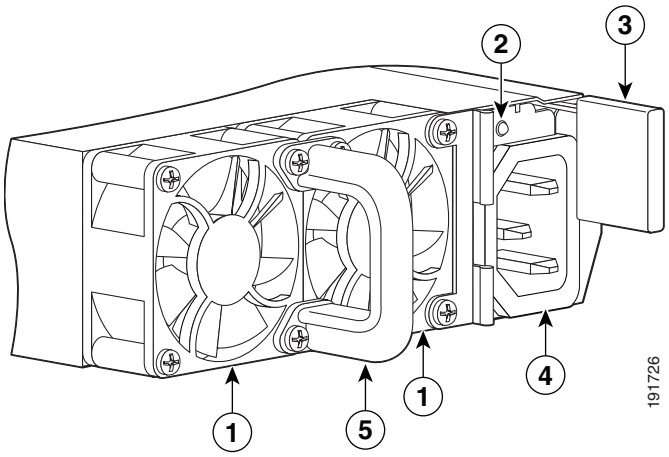
The MARS 110R, 110, 210, GC2R, and GC2 ship with two hot-swappable 750 watt redundant (1 + 1) ATX power supplies (PS) which have the following integrated management features:

- Status LED on each power module
- Over-temperature protection (OTP)
- Over-voltage protection (OVP)

For procedures on hotswapping a power supply, see Chapter 26, “Hot-swapping a Power Supply Unit.”

Caution On a 20 amperes AC outlet, no more than a total of four (4) systems should be connected to a single outlet at any time.

Figure 1-17 Power Supply Module—MARS 110R, 110, 210, GC2R, and GC2



1	Integrated fan	**2**	Status LED
3	Retaining clip	**4**	AC power socket
5	Pull handle		

Over-Temperature Protection (OTP)

The power supply is protected against over-temperature conditions caused by loss of fan cooling or excessive ambient temperature. In an OTP condition the power supply will shutdown. When the power supply temperature drops to the rated safety limit, the power supply restores power automatically, while the 5 V standby remains constantly on. The power supply alerts the system of the OTP condition with the power supply FAIL signal and the Power LED on the control panel.

Over-Current Protection (OCP)

The power supply and power distribution board shutdown and latch off after an over-current condition occurs. This latch is cleared by an AC power interruption.

Over-Voltage Protection (OVP)

The power supply and power distribution board shutdown and latch off after an over-voltage condition occurs. This latch is cleared by an AC power interruption.

AC Power Source Requirements

Each power supply has a socket to accommodate an AC power cord. Each power supply operates within the parameters listed in Table 1-14.

Table 1-14 Power Supply Maximums and Minimums—MARS 110R, 110, 210, GC2R, and GC2

Parameter	110 Line Voltage	220 Line Voltage
Minimum	90 V^{rms}	180 V^{rms}
Rated	100–127 V^{rms}	200–240 V^{rms}
Maximum	140 V^{rms}	264 V^{rms}
Start-up VAC	85 VAC +/– 4 VAC	
Power Off VAC	75 VAC	
Maximum Input AC Current[1]	12.0 A^{rms}	6.0 A^{rms}
Maximum Rated Input AC Current[2]	11.0 A^{rms}	5.5 A^{rms}
Frequency	Minimum: 47 Hz; Rated: 50/60 Hz; Maximum: 63 Hz	

1. Maximum input current at low input voltage range is measured at maximum load—minimums are 90VAC for a 110 Line, and 180VAC for a 220 Line.
2. Maximum rated input current is measured at 100VAC and 200VAC.

Power Supply LED Descriptions

Each power supply module has a two-color Amber/Green LED to indicate power supply status.

- **Solid amber**—Indicates no AC power for this power supply unit only, or there is a power supply critical event causing a shutdown. For instance, a general failure, a blown fuse, an over-current protection event, an over-voltage protection event, or a fan failure.
- **1Hz blinking amber**— Power supply warning event is occurring and the power supply is operating. Warning events are high temperature, high power, high current, or slow fan.
- **Solid green**—Power supplies are operating normally
- **1Hz blinking green**—AC power is present but only 5V standby is on (Power Button is off)

Checking Power Supply Operational Status

Example 1-1 displays the power supply status information in an excerpt of a **show healthinfo** CLI command output. The power supply unit should evaluated for hotswapping if the status is down. An email alert is sent to the administrator when a power supply changes status from "ok." PS1 is the lower power supply, PS2 is the upper power supply. In normal operation, PS1 supplies most of the power requirements, and PS2 is the redundant power supply.

Example 1-1 Power Supply Status in the show healthinfo CLI Command.

```
[pnadmin]$ show healthinfo
<SNIP>
Power Supply            Value   Status
---------------------------------------
PS1 AC Current  2.36 Amps       ok
PS2 AC Current  0.12 Amps       ok
PS1 +12V Current        21 Amps ok
PS2 +12V Current        0 Amps  ok
PS1 +12V Power  248 Watts       ok
PS2 +12V Power  0 Watts         ok
PS1 Status      0x01            ok
PS2 Status      0x09            ok
```

<SNIP>

CHAPTER 2

Deployment Planning Guidelines

Revised: May 9, 2007, OL-14672-01

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

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 2-1 to help you plan your deployment.

Table 2-1 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 Sever	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 Upgrading the Appliance Software, page 6-6.
GUI Client	Yes	This host is one from which you run the GUI to managed the appliance.

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 2-2 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 2-2 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 Man ager	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 2-2 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.

CHAPTER 3

Preparing for Installation

Revised: January 1, 2008, OL-14672-01

This chapter describes safety instructions and site requirements for installing the MARS Appliance and guides you through installation preparation. It contains the following sections:

Safety

This section provides safety information for installing this product.

Warnings and Cautions

Read the installation instructions in this document before you connect the system to its power source. Failure to read and follow these guidelines could lead to an unsuccessful installation and possibly damage the system and components.

You should observe the following safety guidelines when working with any equipment that connects to electrical power or telephone wiring. They can help you avoid injuring yourself or damaging the MARS Appliance.

Note The English warnings in this document are followed by a statement number. To see the translations of a warning into other languages, look up its statement number in the *Regulatory Compliance and Safety Information for the MARS 5.3.x*

The following warnings and cautions are provided to help you prevent injury to yourself or damage to the devices:

Warning **Before working on a system that has an On/Off switch, turn OFF the power and unplug the power cord.** Statement 1

Warning **Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.** Statement 12

Warning **This unit is intended for installation in restricted access areas. A restricted access area is where access can only be gained by service personnel through the use of a special tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.** Statement 37

Warning **This unit might have more than one power cord. To reduce the risk of electrical shock, disconnect all power supply cords before servicing the unit.** Statement 106

Warning **The safety cover is an integral part of the product. Do not operate the unit without the safety cover installed. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards.** Statement 117

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001**.**

Warning **Read the installation instructions before you connect the system to its power source.** Statement 1004

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:** Statement 1006

Warning **There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.** Statement 1015

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.** Statement 1029

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

Warning **Before opening the chassis, disconnect the telephone-network cables to avoid contact with telephone-network voltages.** Statement 1041

Warning **This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.** Statement 1045

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

General Precautions

Observe the following general precautions when using and working with your system:

- Keep your system components away from radiators and heat sources, and do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the computer gets wet, see the appropriate chapter in your troubleshooting guide or contact the Cisco Technical Assistance Center. For instructions on contacting the Technical Assistance Center, see Obtaining Documentation, Obtaining Support, and Security Guidelines, page xvii, in the Preface.
- Do not push any objects into the openings of your system components. Doing so can cause fire or electric shock by shorting out interior components.
- Position system cables and power cables carefully; route system cables and the power cable and plug so that they cannot be stepped on or tripped over. Be sure that nothing rests on your system components' cables or power cable.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.

- To avoid possible damage to the system board, wait 5 seconds after turning off the system before removing a component from the system board or disconnecting a peripheral device from the computer.

Maintaining Safety with Electricity

Follow these guidelines when working on equipment powered by electricity:

- If any of the following conditions occur contact the Cisco Technical Assistance Center:
  - The power cable or plug is damaged.
  - An object has fallen into the product.
  - The product has been exposed to water.
  - The product has been dropped or damaged.
  - The product does not operate correctly when you follow the operating instructions.
- Use the correct external power source. Operate the product only from the type of power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult the Cisco Technical Assistance Center or a local power company.
- Use only approved power cable(s). You have been provided with a power cable for your MARS Appliance that is intended for your system (approved for use in your country, based on the shipping location). Should you have to purchase a power cable, ensure that it is rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.
- To help prevent electric shock, plug the MARS Appliance, components, and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable.
- Observe power strip ratings. Make sure that the total ampere rating of all products plugged into the power strip does not exceed 80% of the rating.
- To help protect your system and components from sudden, transient increases and decreases in electrical power, Cisco recommends the use an uninterruptable power supply (UPS) for your MARS Appliances.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local and national wiring rules.

Protecting Against Electrostatic Discharge

Static electricity can harm delicate components inside your computer. To prevent static damage, discharge static electricity from your body before you touch any of your computer's electronic components, such as the microprocessor. You can do so by touching an unpainted metal surface on the computer chassis.

As you continue to work inside the computer, periodically touch an unpainted metal surface to remove any static charge your body may have accumulated.

You can also take the following steps to prevent damage from electrostatic discharge (ESD):

- When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your computer. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
- When transporting a sensitive component, first place it in an antistatic container or packaging.
- Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads and workbench pads.

Preventing EMI

When you run wires for any significant distance in an electromagnetic field, electromagnetic interference (EMI) can occur between the field and the signals on the wires.

Note Bad plant wiring can result in radio frequency interference (RFI).

Note Strong EMI, especially when it is caused by lightning or radio transmitters, can destroy the signal drivers and receivers in the system, and can even create an electrical hazard by conducting power surges through lines and into the system.

To predict and remedy strong EMI, consult RFI experts.

Preparing Your Site for Installation

This section describes the requirements your site must meet for safe installation and operation of your MARS Appliance. Ensure that your site is properly prepared before beginning installation.

Environmental

When planning your site layout and equipment locations, remember the precautions described in this section to help avoid equipment failures and reduce the possibility of environmentally caused shutdowns. If you are experiencing shutdowns or unusually high errors with your existing equipment, these precautions will help you isolate the cause of failures and prevent future problems.

Use the following precautions when planning the operating environment for your MARS Appliance:

- Always follow the ESD-prevention procedures described in Preventing EMI, page 3-5, to avoid damage to equipment. Damage from static discharge can cause immediate or intermittent equipment failure.
- Make sure that the chassis cover is secure. The chassis allows cooling air to flow effectively within it. An open chassis allows air leaks, which could interrupt and redirect the flow of cooling air from internal components.
- Electrical equipment generates heat. Ambient air temperature might not be adequate to cool equipment to acceptable operating temperatures without adequate circulation. Make sure that the room in which you operate has adequate air circulation.

Also, verify that make sure your environment is suitable for the MARS Appliance:

Environmental Parameter	MARS 110 and MARS 110R	MARS 210, and GC2
Temperature range	Operating: +10°C to +35°C with the maximum rate of change not to exceed 10°C per hour Non-operating: –40° C to +70° C	Operating: +10°C to +35°C with the maximum rate of change not to exceed 10°C per hour Non-operating: –40° C to +70° C
Relative humidity	Non-operating: 90% Non-condensing at +28°C	Non-operating: 90% Non-condensing at +28°C
System Cooling Requirement	1,826 BTU/hour	1,826 BTU/hour
Vibration	Unpackaged: 5 Hz to 500 Hz, 2.20 g RMS random	Unpackaged: 5 Hz to 500 Hz, 2.20 g RMS random
Shock **OL-14672-01**	Operating: Half sine, 2 g peak, 11 mSec Unpackaged: Trapezoidal, 25 g, velocity change 136 inches/sec Packaged: Non-palletized free fall in height 24 inches (>= 40 lbs to < 80 lbs)	Operating: Half sine, 2 g peak, 11 mSec Unpackaged: Trapezoidal, 25 g, velocity change 136 inches/sec Packaged: Non-palletized free fall in height 24 inches (>= 40 lbs to < 80 lbs)
Altitude		
Acoustic Noise	Sound Pressure: 55 dBA (Rack mount) in an idle state at typical office ambient temperatures Sound Power: 7.0 BA in an idle state at typical office ambient temperatures.	Sound Pressure: 55 dBA (Rack mount) in an idle state at typical office ambient temperatures Sound Power: 7.0 BA in an idle state at typical office ambient temperatures.

Choosing a Site for Installation

Warning **This unit is intended for installation in restricted access areas. A restricted access area is where access can only be gained by service personnel through the use of a special tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.** Statement 37

- Choose a site with a dry, clean, well-ventilated and air-conditioned area.
- Choose a site that maintains an ambient temperature of 10° to 35°C (50° to 95°F).
- Choose a site with sufficient room in the front to open the hot-swappable hard drives (about ten inches).
- Choose a site with sufficient room in the rear to attach the power cords and Ethernet cables (about four inches).
- Avoid areas that receive direct sunlight.

Grounding the System

Warning **Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 213

Creating a Safe Environment

Follow these guidelines to create a safe operating environment:

- Keep tools and chassis components off the floor and away from foot traffic.
- Clear the area of possible hazards, such as moist floors, ungrounded power extension cables, and missing safety grounds.
- Keep the area around the chassis free from dust and foreign conductive material (such as metal flakes from nearby construction activity).

AC Power

Ensure that the plug-socket combination is accessible at all times, because it serves as the main disconnecting device.

Warning **This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.** Statement 1045

Cabling

Use the cables in the accessory kit to connect the MARS Appliance console port to a console or computer that is running a console program. In addition to using the console cable, use the provided standard Ethernet cable to connect the MARS Appliance to your network. For information detailing cable requirements, see Network Cable Requirements, page 1-4.

Inline Filter for the Modem

An inline filter for line impedance matching is shipped in the Accessory Kit. Insert the male RJ-11 connector of the filter into the Line-in socket of the MARS modem. Insert the local telephone cable into the RJ-11 socket of the filter.

The following countries require the filter to be used with the MARS modem:

Australia, Austria, Belgium, China, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Korea, Luxembourg, Netherlands, Poland, Portugal, Spain, Sweden, and the UK.

Precautions for Rack-Mounting

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:** Statement 1006

Observe the following precautions for rack stability and safety. Also refer to the rack installation documentation accompanying the rack for specific warning and caution statements and procedures.

Note "Component" refers to any server, storage system, or appliance, and to various peripherals or supporting hardware.

- Do not move large racks by yourself. Due to the height and weight of the rack, a minimum of two people are needed to accomplish this task.
- Ensure that the rack is level and stable before extending a component from the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80% of the branch circuit rating.
- Ensure that proper airflow is provided to components in the rack.
- Do not step or stand on any system or component when servicing other systems and components in a rack.
- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Precautions for Products with Modems, Telecommunications, or Local Area Network Options

Observe the following guidelines when working with options:

- Do not connect or use a modem or telephone during a lighting storm. There may be a risk of electrical shock from lightning.
- Never connect or use a modem or telephone in a wet environment.
- Do not plug a modem or telephone cable into the Ethernet connector.
- Disconnect the modem cable before opening a product enclosure, touching or installing internal components, or touching an uninsulated modem cable or jack.
- Do not use a telephone line to report a gas leak while you are in the vicinity of the leak.
- Install the line-impedance filter to the modem.

Required Tools and Equipment

You need the following tools and equipment to install the MARS Appliance:

- Number 2 Phillips screwdriver
- Needle-nosed pliers
- Tape measure and level
- Antistatic mat or antistatic foam
- ESD grounding strap

Packaging Contents Checklist

Before unpacking the MARS Appliance, check the outside of the box for signs of damage from the shipment. If you suspect that the box was damaged during shipment, tell the carrier, and fill out the appropriate damage claims.

While unpacking the MARS Appliance, place the box so that the direction arrows on the box are facing up. Open the top of the box, and lift the appliance clear. Place the MARS Appliance on a clean flat surface. Re-inspect the appliance for damage.

Each appliance ships with the following items:

- One copy of *Software License Claim Certificate*
- One copy of *Cisco Secure MARS Documentation Guide and Warranty*
- One copy of *Regulatory Compliance and Safety Information for the Cisco Security MARS Appliances.*
- One appliance
- One Appliance Recovery DVD
- Two rail kit boxes, each containing two rack rails assemblies with screws (each rail kit supports a specific set of racks, see Selecting the Appropriate Rail Kit, page 3-10 for more information)
- Two to four sets of keys (depending on the appliance model)
- One or two standard computer power cords (depending on the appliance model)
- One telephone cable
- One Category 5 (Cat 5) crossover cable
- One serial cable
- One xDSL In-line filter

Review this checklist to ensure that each item is present. Write down the appliance's serial number and license key and store them in a safe place. The serial number and license keys both appear as labels on the actual appliance. For information on locating these items, refer to the diagrams in Hardware Descriptions—MARS 25R, 25, 55, 110R, 110, 210, GC2R, and GC2, page 1-4.

Selecting the Appropriate Rail Kit

The two rail kits provided with your MARS Appliance provide support for different types of appliance racks. You should select the rail kit that is compatible with your rack and ignore the other kit. Use the following guidance to select the correct rail kit:

- **AXXBASICRAIL**. This basic rail kit supports both threaded hole racks and square hole, enclosed racks, but it does not support non-threaded circular hole racks. Most racks use this kit.
- **AXXHERAIL**, This tool-less rail kit uses a hanging adapter that allows you to support non-threaded circular hole racks.

Web Browser Client Requirements

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

- Configuring Internet Explorer Settings, page 3-10
- Configuring Pop-Up Blockers, page 3-14
- Correcting Issues Caused by the 832894 (MS04-004) Security Update or the 821814 Hotfix, page 3-15
- Obtaining the Required Browser Plug-ins, page 3-15

Configuring Internet Explorer Settings

You must 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).

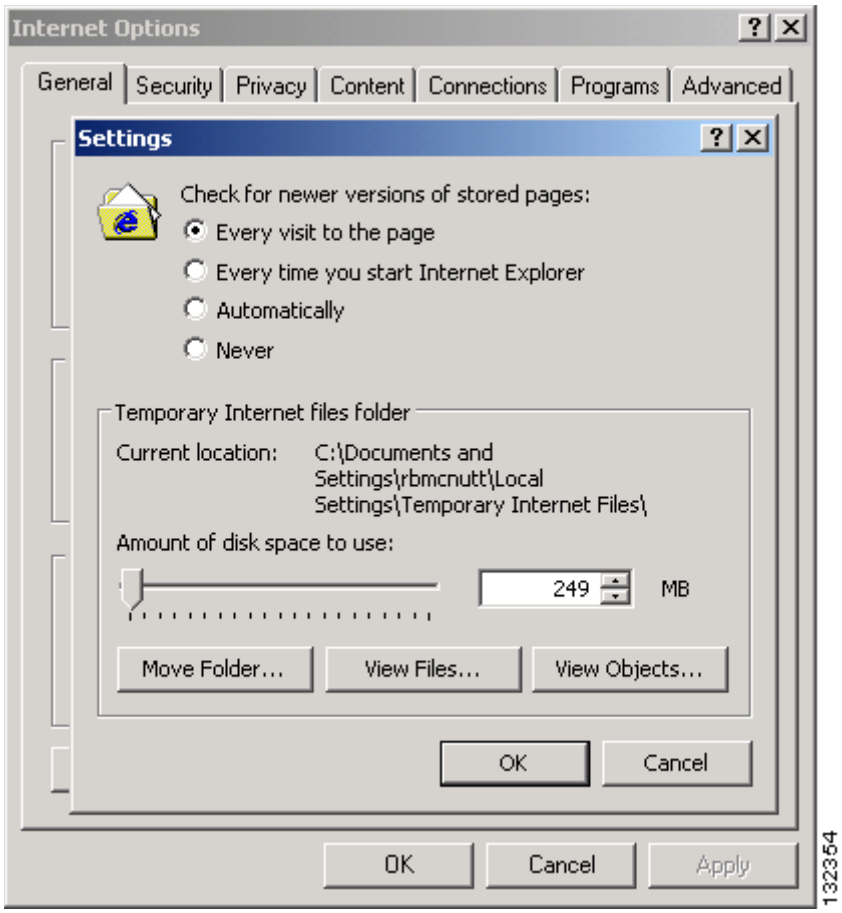
To configure Internet Explorer to meet these requirements, follow these steps:

Step 1 Start Internet Explorer.

Step 2 Click **Tools > Internet Options**.

Step 3 On the General tab under Temporary Internet Settings, click **Settings**.

Figure 3-1 Internet Explorer Page Cache Settings

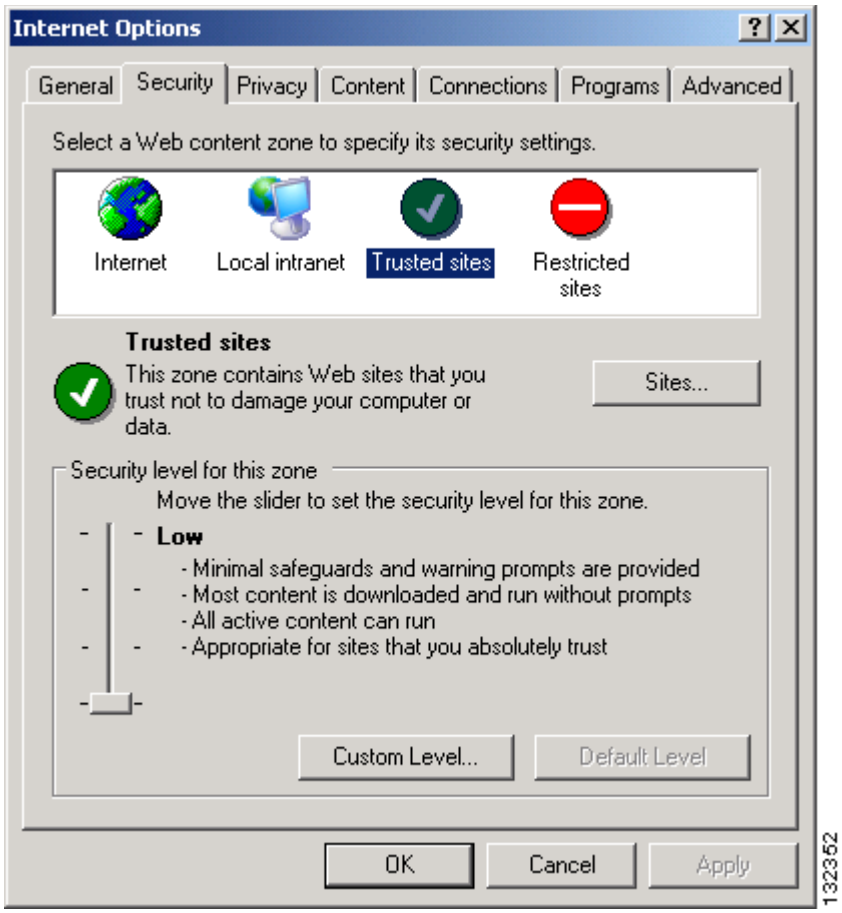


Step 4 Click the **Every Visit to the Page** radio button.

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**.

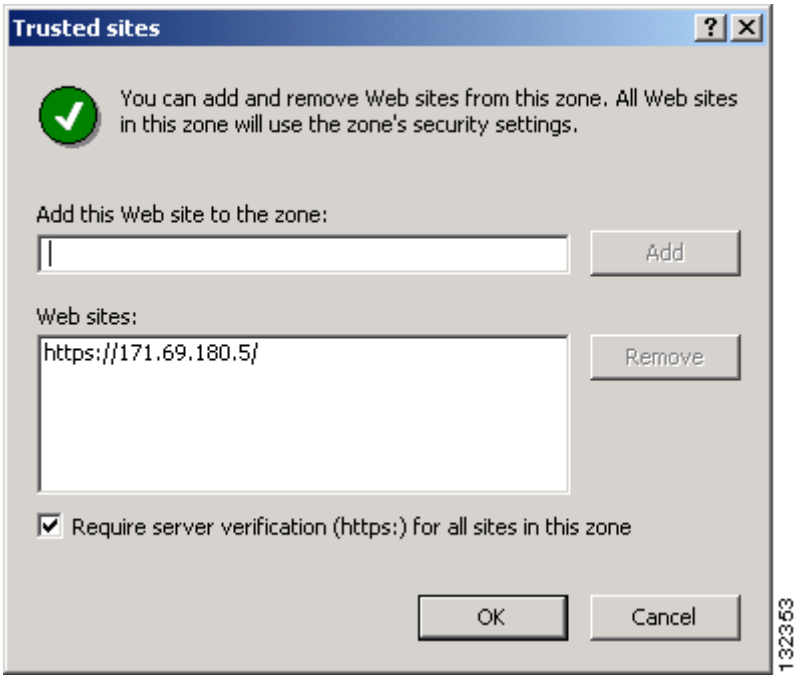
Figure 3-2 Internet Explorer Security Settings



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 3-3 Internet Explorer Trusted Sites



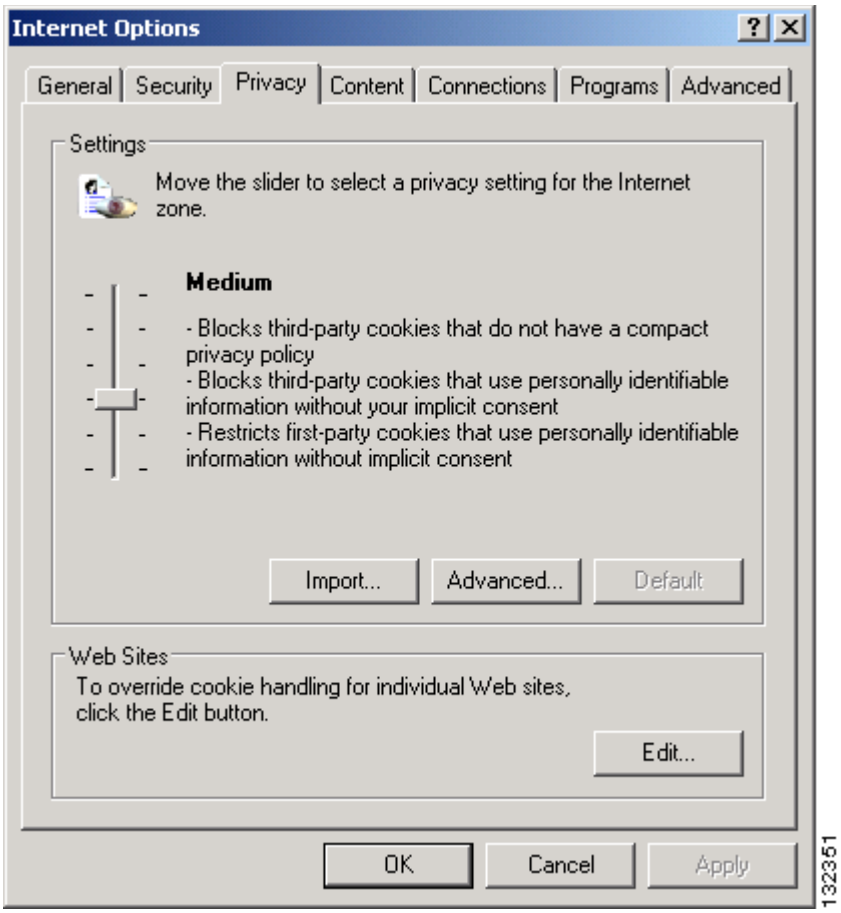
Step 8 Enter the URL used to connect to the MARS Appliance in the Add this Web site to the zone box and click **Add**.

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 3-4 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

An issue introduced in a recent 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/readermain.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 4

Installing the Appliance

Revised: May 9, 2007, OL-14672-01

This chapter describes how to unpack and install any Cisco Security Monitoring, Analysis, and Response System Appliance (MARS Appliance). It describes requisite safety information, environmental requirements, how to install in a rack, and how to cable the appliance. It contains the following sections:

Installation Quick Reference

Table 4-1 provides an overview of the installation and initial configuration process. Following installation and initial configuration, see the following publications for information on how to use a browser and the HTML interface to fully configure your MARS Appliance to provide the security threat mitigation (STM) services you want from this installation:

- *User Guide for Cisco Security MARS Local Controller*
- *User Guide for Cisco Security MARS Global Controller*

Table 4-1 Quick Reference

Task	References
Use the rack mount kit to install the MARS Appliance in a rack.	Installing the MARS Appliance in a Rack, page 4-2
Connect the MARS Appliance to an AC power source.	Connecting to the AC Power Source, page 4-7
Connect network and console cables.	Connecting Cables, page 4-8
Power on the appliance and Verify Operation	Powering on the Appliance and Verifying Hardware Operation, page 4-8

Table 4-1 Quick Reference (continued)

Task	References
Perform initial configuration of the MARS Appliance.	Initial MARS Appliance Configuration, page 5-1
Configure the MARS Appliance to monitor reporting devices.	Next Steps, page 5-18

Installing the MARS Appliance in a Rack

This section provides instructions for installing the MARS Appliance on a rack in the following subsection:

- Rack-Mounting MARS Appliances 110R, 110, 210, GC2R, and GC2, page 4-4

The rack must be properly secured to the floor, ceiling, or upper wall, and where applicable, to adjacent racks. The rack should be secured using floor and wall fasteners and bracing specified by industry standards.

Before installing the MARS Appliance in a rack, read Preparing Your Site for Installation, page 3-5, to familiarize yourself with the proper site and environmental conditions. Failure to read and follow these guidelines could lead to an unsuccessful installation and possibly damage the system and components. Perform the steps below when installing and servicing the MARS Appliance.

The following rack installation procedures are for the rack rails included with the appliance on a typical rack unit. Because a variety of rack units exist, this is a general guide to connecting the appliance to the rack

When installing and servicing the MARS Appliance:

- Disconnect all power and external cables before installing the system.
- Install the system in compliance with your local and national electrical codes:
  - United States: National Fire Protection Association (NFPA) 70; United States National Electrical Code.
  - Canada: Canadian Electrical Code, Part, I, CSA C22.1.
  - Other countries: If local and national electrical codes are not available, see IEC 364, Part 1 through Part 7.
- Do not work alone under potentially hazardous conditions.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Do not install the MARS Appliance in a rack that has not been securely anchored in place. Damage to the system and personal injury may result.
- Due to the size and weight of the computer system, never install the computer system by yourself.

See Precautions for Rack-Mounting, page 3-8, for additional safety information on rack installation.

Warning

To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- **This unit should be mounted at the bottom of the rack if it is the only unit in the rack.**
- **When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.**
- **If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.** Statement 1006

A rack is measured in rack units (RUs). An RU is equal to 44 mm or 1.75 inches. MARS Appliances require the following rack space:

Table 4-2 Appliance Dimensions in Rack Units

Model	Dimensions[1]
MARS 110R, 110, 210, GC2R, and GC2	2RU x 27.75 in (704.8 mm)

1. A rack unit (RU) is a standardized measure for the height of rack-mountable equipment. One RU is 44.45 mm (1.75 in) high, 482.6 mm (19 in.) wide.

Rack-Mounting MARS Appliances 110R, 110, 210, GC2R, and GC2

Your Cisco Security MARS 110R, 110, 210, GC2R or GC2 appliances can be mounted on a 19-inch rack. There are three methods for mounting the appliance on a rack. Instructions for installing your chassis on a rack are included in the rail kit, part number CS-MARS-X10-RAIL=.

The following procedures are provided for your reference:

- Installing the Chassis Handles, page 4-4
- Fixed Bracket Rack-Mount Installation, page 4-5
- Fixed Bracket Rack Mount Removal, page 4-7
- Step 3Remove and service the system., page 4-7
- Basic Rail Rack-Mount Removal, page 4-5
- Tool-less Rail Rack-Mount Servicing, page 4-7

Caution When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.

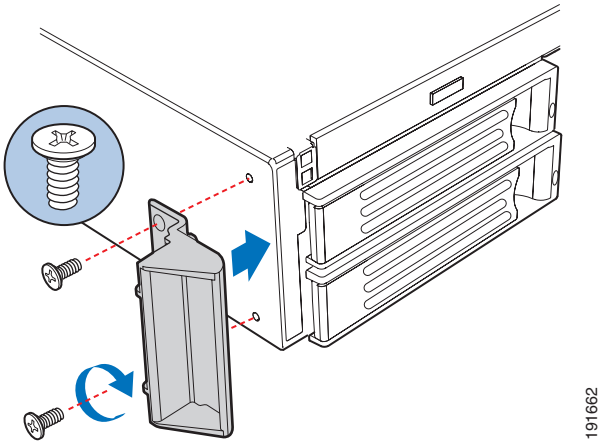
Installing the Chassis Handles

The chassis handles enable you to easily push and pull the chassis on the rack rails. To install the chassis handles do the following:

Step 1 Remove the front bezel.

Step 2 Align the chassis handle with the two holes on the side of the MARS Appliance, as shown in Figure 4-1.

Figure 4-1 Installing a Chassis Handle on a MARS 110R, 110, 210, GC2R or GC2



Step 3 Attach the chassis handle to the MARS Appliance with two screws as shown in Figure 4-1.

Step 4 Install the chassis handle on the other side of the MARS Appliance.

Step 5 Replace the front bezel.

End of Procedure

Basic Rail Rack-Mount Installation

Step 1 Extend the inner rail until it locks.

Step 2 Depress the spring safety lock to release the inner rail.

Step 3 Remove the inner rail from the rail assembly.

Step 4 Attach the outer rail slides to the rack posts using two #10-32 x 1/2 screws at the front posts, and two #10-32 x 1/2 screws at the rear posts.

Note The rail flanges mount to the inside of each post.

Step 5 Insert the inner rails over the server chassis sidewall studs.

Step 6 Slide the inner rails toward the front of the server chassis.

Step 7 Secure the inner rails with one #6-32 x 1/4 screw for each rail.

Step 8 Align the inner rails (attached to the server chassis) with the outer rail assemblies (attached to the rack).

Step 9 Engage the matching rails and slide the server chassis into the rack until the two safety stops lock into position.

Step 10 Depress the two safety locks (one on each side).

Step 11 Slide the server chassis all the way into the rack.

Step 12 Use the rack screws (#10-32 x 3/4) to secure the chassis and rack handles into the rack.

End of Procedure

Basic Rail Rack-Mount Removal

Step 1 Disconnect all cables from the back of the system.

Tip You can use the system LED to properly identify the system you are servicing.

Step 2 Pull the appliance from rack until brackets are fully extended.

Step 3 Push in both clips on the brackets and slide the system forward until the inner rail separates from the outer rail.

End of Procedure

Fixed Bracket Rack-Mount Installation

Step 1 Fully extend a rail assembly; the finger tab for the extension lock is revealed.

Step 2 Press the finger tab and slide the inside rail from the middle rail until it completely separates.

Note The middle rail and outer rail cannot be separated.

Step 3 Position an inside rail along one side of the chassis with the finger tab facing outward and located closer to the rear of the chassis.

Step 4 Align the holes in the rail with the tabs on the chassis and place the rail against the chassis.

Step 5 Slide the rail as far as it will go toward the front of the chassis to engage the tabs.

Step 6 Fasten the rail to the chassis using one screw at the front of the chassis.

Step 7 In the same manner, attach the other inside rail to the other side of the chassis

Step 8 Using two screws, attach one nut bar to the inside of the rack post. Do not completely tighten the screws; leave them loose enough to allow insertion of the brackets in the next step.

Step 9 Insert the slotted foot of a rail bracket between each nut bar and post.

Step 10 Align the face of the bracket foot with the inside edge of the rack post and firmly tighten the screws.

Step 11 Repeat steps 8 to 10 above to install the other 3 brackets (2 front & 2 back). Ensure all brackets are at the same height on the rack.

Step 12 Position a rail assembly (middle and outer rails) with its black plastic end caps toward the rear of the rack and its outer rail closest to the brackets.

Step 13 Align the front screw hole in the outer rail with the threaded hole nearest the front of the front bracket and fit the rail assembly into the front and rear brackets.

Step 14 Slide the middle rail toward the front until the access hole in the middle rail is aligned with the front screw hole in the outer rail.

Step 15 Insert screw through the access hole and loosely attach the outer rail to the front bracket.

Step 16 In a similar manner to steps 13 through 15, install a screw through a slot in the outer rail and into the rear-most threaded hole in the front bracket. Firmly tighten this screw.

Step 17 Firmly tighten the front screw installed loosely in step 15.

Step 18 In the same manner, attach the other rail assembly to the other side.

Step 19 Slide the middle rail toward the front until the rear bracket area is accessible.

Step 20 Attach the rear end of the outer rail to the rear bracket with at least one screw. If possible, attach at two places.

Step 21 Similarly, attach the other rail assembly to the other side.

Step 22 Fully extend the left and right rails until the extension locks have engaged and the rails will not push back in. The rail system is now ready to receive the chassis.

Caution Lifting and placing the chassis in the rails is a two-person task. If required, use a lifting device.

Step 23 With the chassis front facing you, lift the chassis and carefully insert the rails attached to the chassis in the extended rails.

Step 24 Slide the chassis toward the rear of the cabinet until the rails lock together.

Step 25 Depress and hold down the finger tabs on both extension locks while sliding the chassis toward the rear.

Step 26 Slide the chassis all the way into the rack until the chassis handles are against the front posts.

End of Procedure

Fixed Bracket Rack Mount Removal

Step 1 Disconnect all cables from the back of the system.

Tip You can use the system LED to properly identify the system you are servicing.

Step 2 Remove screws from the brackets and remove the system from the rack.

Step 3 Remove and service the system.

End of Procedure

Tool-less Rail Rack-Mount Servicing

Step 1 To service the system, pull the system out from the rack.

Step 2 Disconnect the power cable(s) and proceed with servicing the system.

Step 3 When the servicing is completed, reconnect the power cable(s).

Step 4 Pull up on the green tabs on each rail and slide the system back into the rack.

Caution Be careful not to dislodge any cables when moving the appliance.

End of Procedure

Connecting to the AC Power Source

Warning **This equipment must be grounded. Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.** Statement 1024

Connect the AC power receptacle to the AC power source with the provided power cable. Some units have two power cables, one for each AC power receptacle in the appliance.

Connecting Cables

Use unshielded twisted pair (UTP) copper wire Ethernet cable, with standard RJ-45 compatible plugs, to connect the MARS Appliance to the network. Your MARS Appliance comes with one or two standard computer power cords, a Cat 5 crossover cable, Inline Filter for the Modem, page 3-8, and a telephone cable. The telephone jack is required to enable pager- and SMS-based alerts from MARS Appliance.

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001

To connect the cables:

Step 1 Plug the network connection into the Ethernet 0 port. See the appropriate back panel diagram in Hardware Descriptions—MARS 25R, 25, 55, 110R, 110, 210, GC2R, and GC2, page 1-4, for the location of the Ethernet 0 port.

Step 2 Insert the male RJ-11 connector of the inline impedance matching filter into the line-in socket of the MARS modem. Insert the local telephone cable into the RJ-11 socket of the filter.

See the appropriate back panel diagram in Hardware Descriptions—MARS 25R, 25, 55, 110R, 110, 210, GC2R, and GC2, page 1-4, for the location of the modem sockets. The line-in socket is labeled with a socket icon, the external telephone socket is labeled with a telephone icon. See the "Inline Filter for the Modem" section on page 3-7 for a list of countries that require the filter.

Step 3 Connect a console to the console/serial port using the one of the options described in Establishing a Console Connection, page 5-4. You can also establish more than one console connection.

Powering on the Appliance and Verifying Hardware Operation

Before powering on the appliance, verify that all the cables and cords are firmly seated in their jacks and sockets. Make sure that the vents for the appliance's fans have sufficient clearance and that the appliance's air intakes are not blocked.

Caution If you hear a loud beeping sound after turning on the appliance, check the rear panel and make sure that all appliance power supply switches are fully clicked into the ON position. If all switches are locked into the ON position, and you continue to hear the beeping, a power supply might not be functioning. Turn off the appliance's power and contact Cisco Support.

MARS Appliances 110R, 110, 210, GC2R, and GC2

Step 1 Verify that the power cables are connected to the power supplies and to a live AC power source.

Step 2 Press the Power button on the control panel.

The System Status LED flashes alternately amber and green for approximately 15 to 20 seconds, then glows steady green when the system is operational. See the section, "Control Panel LED Descriptions—MARS 110R, 110, 210, GC2R, and GC2" for further information on determining the operational status.

When the appliance is operational, start the software configuration. See Chapter 5, "Initial MARS Appliance Configuration," for more information on its default configuration settings.

CHAPTER 5

Initial MARS Appliance Configuration

Revised: September 27, 2007, OL-14672-01

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 Controller* and the *User Guide for Cisco Security MARS Global Controller*.

This chapter contains the following sections:

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
❑	**1. Establish a console connection to the appliance.** 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: • 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 After you configure your console connection, you must power up the appliance. *Result*: The appliance is powered up and you can see the command line prompt through your console connection. For more information, see: • Establishing a Console Connection, page 5-4
❑	**2. Command Line Configuration: Setting the system administrative account's default password and configuring the interfaces.** 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: • 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. 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. **Note** The MARS Appliance does not allow you to configure both of its interfaces on the same network. *Result*: 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. For more information, see: • Configuring Basic Network Settings at the Command Line, page 5-6 • Change the Default Password of the System Administrative Account, page 5-6 • Specify the IP address and Default Gateway for the Eth0 Interface, page 5-7. • (Optional) Specify the IP Address and Default Gateway for the Eth1 Interface, page 5-8

✓	Task
❑	**3. Command Line Configuration.** 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: • Log in to the appliance using the system administrative account and the new password. • Set the hostname of the appliance. *Result*: The hostname is configured for the appliance. The appliance reboots. For more information, see: • Specify the Appliance Hostname, page 5-9.
❑	**4. Command Line Configuration.** 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: • 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.) *Result*: 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. For more information, see: • Specify the Time Settings, page 5-10 • Set Up Additional Routes, page 5-9 • Completing the Cable Connections, page 5-11

✓	Task
❑	**5. Complete initial configuration using the web interface.** 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 3-10). During this phase, you configure the following: • 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 *Result*: You have configured your appliance to communicate on the network, properly correlate events, and issue system e-mails to a monitored e-mail address. For more information, see: • Completing the Configuration using MARS web interface, page 5-11 • Licensing the Appliance, page 5-11 • Verifying and Updating Network Settings, page 5-14 • Specifying the DNS Settings, page 5-15 • Configure E-mail Settings for the System Administrative Account, page 5-16 • Configure TACACS/AAA Login Prompts, page 5-17
❑	**6. Upgrade the appliance to the most recent software version.** 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. *Result*: The appliance is running the most recent version of software. For more information, see: • Checklist for Upgrading the Appliance Software, page 6-6

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 Hardware Descriptions—MARS 25R, 25, 55, 110R, 110, 210, GC2R, and GC2, page 1-4. 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 Hardware Descriptions—MARS 25R, 25, 55, 110R, 110, 210, GC2R, and GC2, page 1-4. 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 5-1, 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 = pnadmin
  - 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 5-6.

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 5-6
- Specify the IP address and Default Gateway for the Eth0 Interface, page 5-7
- (Optional) Specify the IP Address and Default Gateway for the Eth1 Interface, page 5-8
- Specify the Appliance Hostname, page 5-9
- Specify the Time Settings, page 5-10
- Set Up Additional Routes, page 5-9

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 5-4.

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 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 5-4.

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 5-6.

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 and Default Gateway 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. To ensure that traffic is routed correctly from eth1, you may also have to define static routes for it. For information on defining static routes on a per-interface basis, see Set Up Additional Routes, page 5-9.

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 5-4.

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 5-6.

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 5-4.

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 5-6.

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 Command Reference, page A-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 5-4. 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 A-26.

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 5-11.

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

How you license your appliance depends on the model number and the software support you are running. For the newer models running 5.x software, your appliance comes with a *Software License Claim Certificate*, which you use to generate your license key using a web browser.

To license your appliance, select the correct software version and following the provided instructions:

License the 5.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*>/**

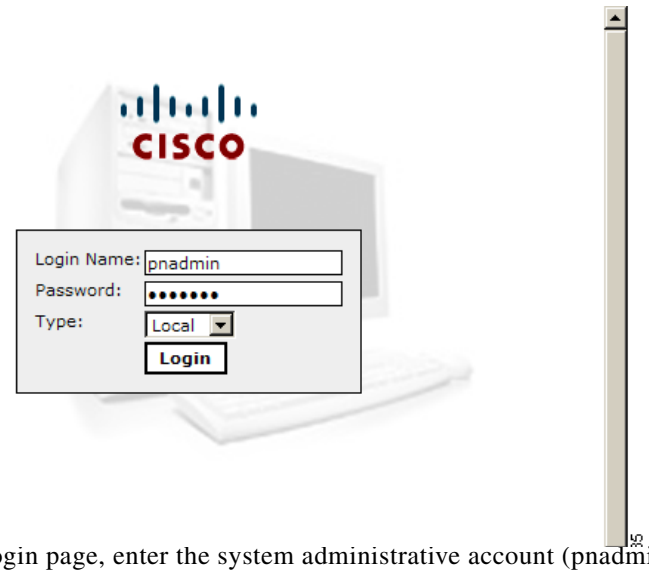
where *machine_name* is the name of the appliance as defined in Specify the Appliance Hostname, page 5-9, and *ip_address* is the address assigned to the interface to which you are attempting to connect (either eth0 or eth1), as configured in Specify the IP address and Default Gateway for the Eth0 Interface, page 5-7, or Specify the IP Address and Default Gateway for the Eth1 Interface, page 5-8.

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 5-1 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 5-4, or Change the Default Password of the System Administrative Account, page 5-6.

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 5-2 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 5-3 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

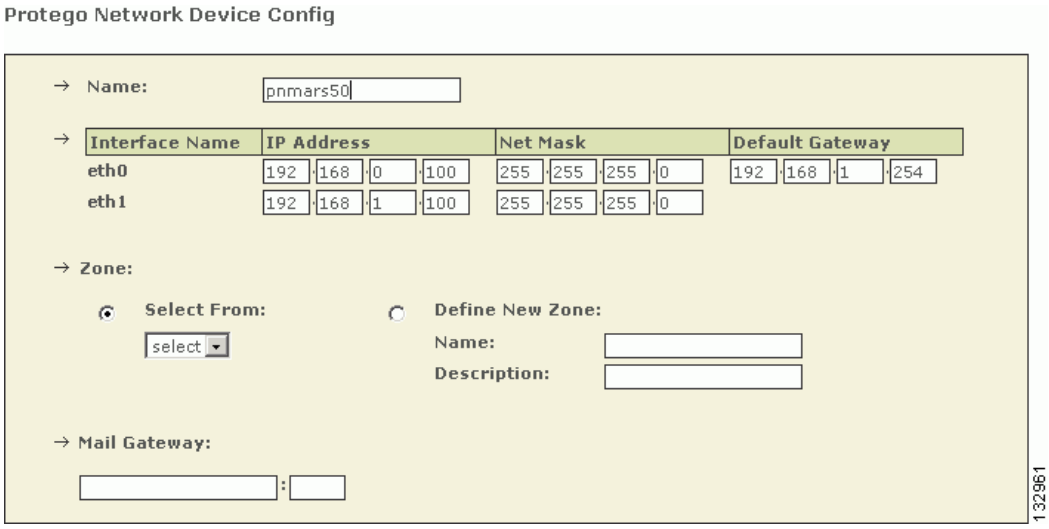
To complete the configuration of the appliance, you must enter basic configuration information that can only be set using the web interface. Specifically, you must designate its network zone (if it is a Global Controller) and enter e-mail gateway information, which is used by the appliance to deliver 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 5-4 Entering Configuration Information (Global Controller example)



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 Hardware Descriptions—MARS 25R, 25, 55, 110R, 110, 210, GC2R, and GC2, page 1-4 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

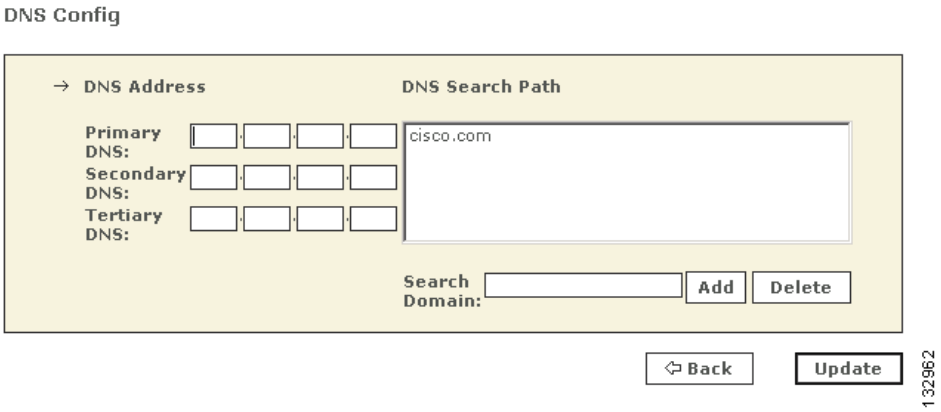
The local TCP/IP stack that resides on the appliance uses DNS services just as any host on the network does. In addition, MARS uses DNS to resolve the IP addresses into hostnames for events that it studies. This mapping enables you to study events by hostname or by IP address.

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 5-5 Domain Name Server Information



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 pnstop and then a pnstart 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 6-5 and Start Appliance Services via the Console, page 6-5.

Configure E-mail Settings for the System Administrative Account

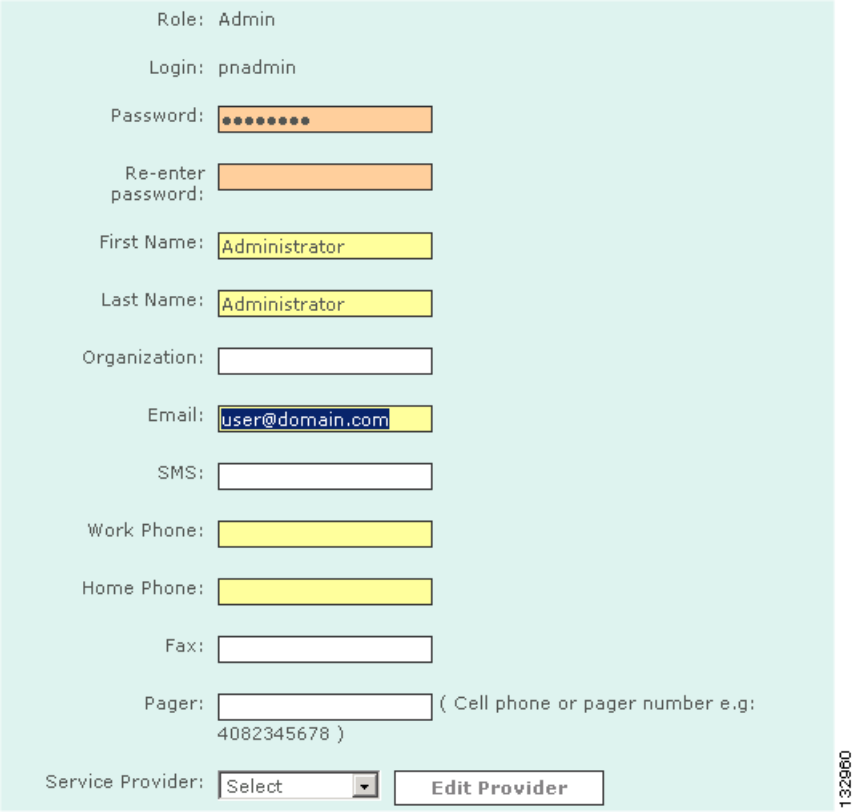
One of the required settings for MARS is the e-mail address for the system administrative account, pnadmin. The MARS Appliance uses this e-mail address to deliver import notifications and reports about system status.

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**.

Configure 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 Upgrading the Appliance Software, page 6-6.

When the software update is complete, you can identify the reporting devices to monitor, as discussed in Next Steps, page 5-18.

Next Steps

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 following guides, as applicable to your appliance:

- *User Guide for Cisco Security MARS Local Controller*
- *User Guide for Cisco Security MARS Global Controller*

CHAPTER 6

Administering the MARS Appliance

Revised: January 1, 2008, OL-14672-01

This chapter describes a core set of maintenance tasks for Cisco Security Monitoring, Analysis, and Response System (MARS). Because these tasks affect the overall health and accuracy of the MARS system, you should develop an operational strategy and process for performing them. This chapter contains the following sections:

For all other MARS Appliance configuration and administration tasks, see either the *User Guide for Cisco Security MARS Global Controller* or the *User Guide for Cisco Security MARS Local Controller*, depending on which product you own.

Performing Command Line Administration Tasks

This section details basic administrative tasks that you perform using a console connection to the MARS Appliance. This section contains the following procedures:

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 5-4.

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 6-32.

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 6-2.

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. For more information on powering up the appliance, see Powering on the Appliance and Verifying Hardware Operation, page 4-8.

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.

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 6-2.

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

Step 3 At the `Are you sure you want to shut down? (Y/N)` prompt, type **Y** for yes and then press **Enter**.

Result: The MARS Appliance powers off.

Log Off the Appliance via the Console

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

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.

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 6-2.

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

Result: The MARS Appliance displays the following message:

```
Are you sure you want to reboot? (Y/N)
```

Step 3 Type **Y** for yes and then press **Enter**.

Result: 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.

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 6-2.

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

The system displays the following status information:

```
Module  State   Uptime
DbIncidentLoaderSrvRUNNING01:12:18
KeywordQuerySrvRUNNING01:12:18
csdam   RUNNING 01:12:18
csiosipsRUNNING01:12:18
csips   RUNNING 01:12:18
cswin   RUNNING 01:12:18
device_monitorRUNNING01:12:18
discoverRUNNING01:12:18
graphgenRUNNING01:12:18
pnarchiverRUNNING01:12:18
pndbpurgerRUNNING01:12:18
pnesloaderRUNNING01:12:18
pnmac   RUNNING 01:12:18
pnparserRUNNING01:12:19
process_event_srvRUNNING01:12:19
process_inlinerep_srvRUNNING01:12:19
process_postfire_srvRUNNING01:12:19
process_query_srvRUNNING01:12:19
superV  RUNNING 01:12:20
```

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 three services running: graphgen, pnarchiver, and superV—all other services are stopped.

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 6-4.

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 6-2.

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 6-4.

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 6-2.

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, page A-38, of Appendix A, "Command Reference." 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 6-2.

Step 2 Type **pnlog show** and the appropriate argument.

Step 3 Press **Enter**.

Result: The console begins scrolling the output of the executed command.

Step 4 To stop the output at any time, press **Ctrl+C**.

Result: The system returns to the system prompt.

Checklist for Upgrading the 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
	1. Determine whether you should upgrade or reimage the MARS Appliance. 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. • *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. • *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 6-32. *Result*: You determine whether you will upgrade or reimage your MARS Appliance.
❑	**2. Determine the version that you are running.** Before you upgrade your appliance, you must determine what version you are running. You can determine this in one of two ways: • **web interface.** To the 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)`, for example, `3.4.1 (1922)`. **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. *Result*: You have identified the version running on your appliance and know whether you must contact Cisco support or continue with this checklist.

✓	Task
❑	**3. Determine the medium for upgrading.** Before upgrading your appliance, you must determine what medium to use. Your choice of medium determines whether you must upgrade from the CLI. • **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 HTML interface unless otherwise noted. **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. *Result*: 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. For more information, see: • Burn an Upgrade CD-ROM, page 6-10 • Prepare the Internal Upgrade Server, page 6-10.
❑	**4. Understand the required upgrade path and limitations.** 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. 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. You have identified the complete list of upgrade packages that you must download. For more information, see: • Important Upgrade Notes, page 6-11 • Determine the Required Upgrade Path, page 6-12.

✓	Task
❑	**5. Download all required upgrade packages from the Cisco.com website.** After you have identified the upgrade packages to download, log in to Cisco.com using your Cisco.com account and download the various packages. To download upgrade packages, you must have a valid SMARTnet support contract for the MARS Appliance. Depending on your selection in *Step 3., you will either store these files on the* Internal Upgrade Server *or burn a CD-ROM image.* *Result*: 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 Internal Upgrade Server or a CD-ROM. For more information, see: • Download the Upgrade Package from Cisco.com, page 6-12.
❑	**6. Understand the upgrade approach you want to use.** *Select from the following upgrade options:* **Note** If you are running a version earlier than 3.4.1, you must select an option that supports upgrading from the CLI. • 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 (web interface only). • Upgrade from a CD-ROM at the command line (CLI only). *Result*: You have determined the appropriate upgrade approach to use based on your selected medium and currently running version.

✓	Task
❑	**7. Identify any required proxy server settings.** 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. **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. *Result*: You have either specified the proxy server settings in the web interface, or you have noted the settings for later use. For more information, see: • Specify the Proxy Settings for the Global Controller or Local Controller, page 6-13.
❑	**8. Upgrade the appliance to the next appropriate version, as determined by the upgrade path.** From the appliance, use the method you chose in Step 6. to upgrade incrementally, as determined in Step 5., to the desired version. *Result*: You have applied each required upgrade package. For more information, see: • Upgrade Global Controller or Local Controller from its User Interface, page 6-14 • Upgrade from the CLI, page 6-15 • Upgrading a Local Controller from the Global Controller, page 6-17

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.

Important Upgrade Notes

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

General Notes

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

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

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

Upgrade to 5.3.2

The upgrade is from 5.3.1 to 5.3.2. No important notes exist for this release.

Upgrade to 5.3.1

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

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

Upgrade to 5.2.8

The upgrade is from 5.2.7 to 5.2.8. No important notes exist for this release.

Upgrade to 5.2.7

The upgrade is from 5.2.4 to 5.2.7; no 5.2.5 or 5.2.6 releases exist.

Determine the Required Upgrade Path

When upgrading from one software version to another, a prerequisite version is always required. This prerequisite version is the minimum level required to be running on the appliance before you can upgrade to the most recent version.

Table 6-1 Upgrade Path Matrix for 5.x Releases

From Version	Upgrade To	Upgrade Package
5.2.4	5.2.7	csmars-5.2.7.pkg
5.2.7	5.2.8	csmars-5.2.8.pkg
5.2.8	5.3.1	csmars-5.3.1.pkg
5.3.1	5.3.2	csmars-5.3.2.pkg

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/cdcrgstr/applications_overview.html

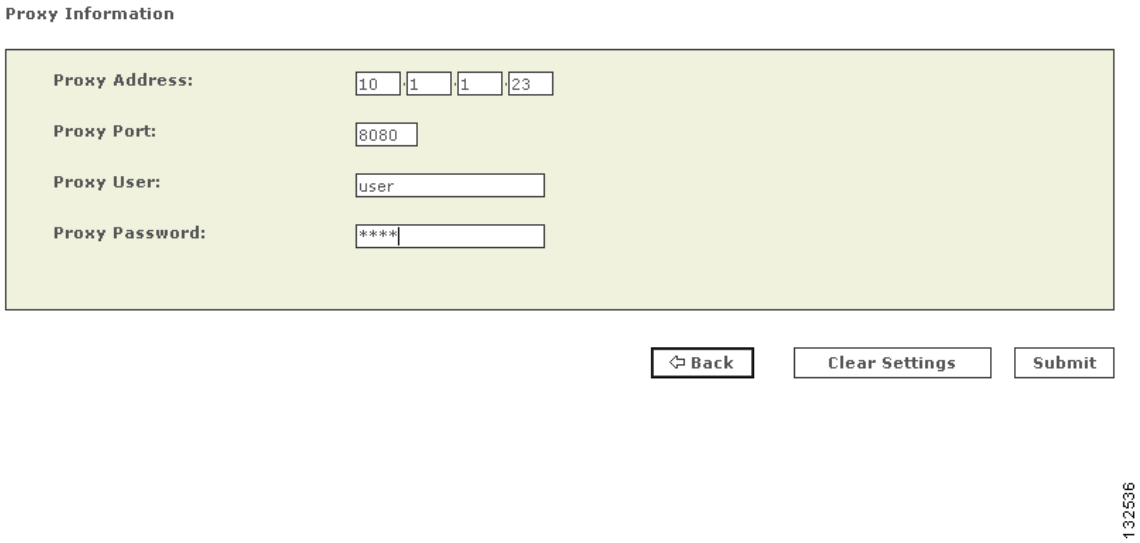
Specify the Proxy Settings for the Global Controller or Local Controller

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 6-17.

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**.



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.

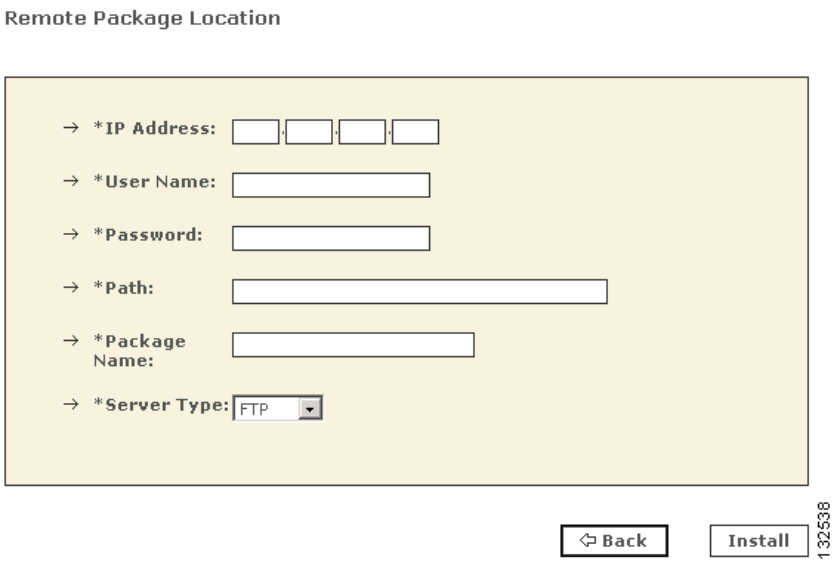
Upgrade Global Controller or Local Controller from its User Interface

Note This procedure is valid for versions 3.4.1 and later.

To upgrade the appliance from the user interface, follow these steps:

Step 1 Open the MARS user interface in your browser.

Step 2 Select **Admin > System Maintenance > Upgrade**.



Step 3 In the IP Address field, enter the address of the server where the upgrade package files are stored.

Step 4 In the User Name and Password fields, enter your Internal Upgrade Server login information.

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.

Step 5 In the Path field, specify the path where the package file is stored, relative to the type of server access used.

Step 6 Select the appropriate protocol in the Server Type box.

You can download the install package using either HTTPS or FTP.

Step 7 In the Package Name field, specify the full name of the package file that you have downloaded.

Step 8 Click **Download**.

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 9 Click **Install**.

Result: After you click Install, the system needs some time to process the upgrade. After the upgrade is complete, the system reboots. During the upgrade, the user interface is also restarted.

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 A-50.

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.myttpserver*.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.myttpserver.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.

Upgrading a Local Controller from the Global Controller

When upgrading a Local Controller from within the Global Controller user interface, you need to determine whether the Local Controller resides behind a proxy server. If so, you must configure the proxy settings for the Local Controller within the Global Controller user interface. After you have specified the settings, you can upgrade the Local Controller as you normally would.

Note If Local Controller proxy information is not provided and you attempt to download an upgrade for that appliance, the Local Controller attempts to connect to Internal Upgrade Server and fails after a period of time.

When you upgrade a Global Controller and its monitored Local Controllers, you first upgrade Global Controller, which requires that you identify the Internal Upgrade Server information. The Global Controller then pushes this server information to all its selected Local Controllers, which allows the Local Controller to locate the Internal Upgrade Server and start the download and upgrade process. The Local Controller does not retrieve the upgrade package from the Global Controller.

Before You Begin

- This procedure is valid for versions 3.4.1 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.

Specify the Proxy Settings in the Global Controller

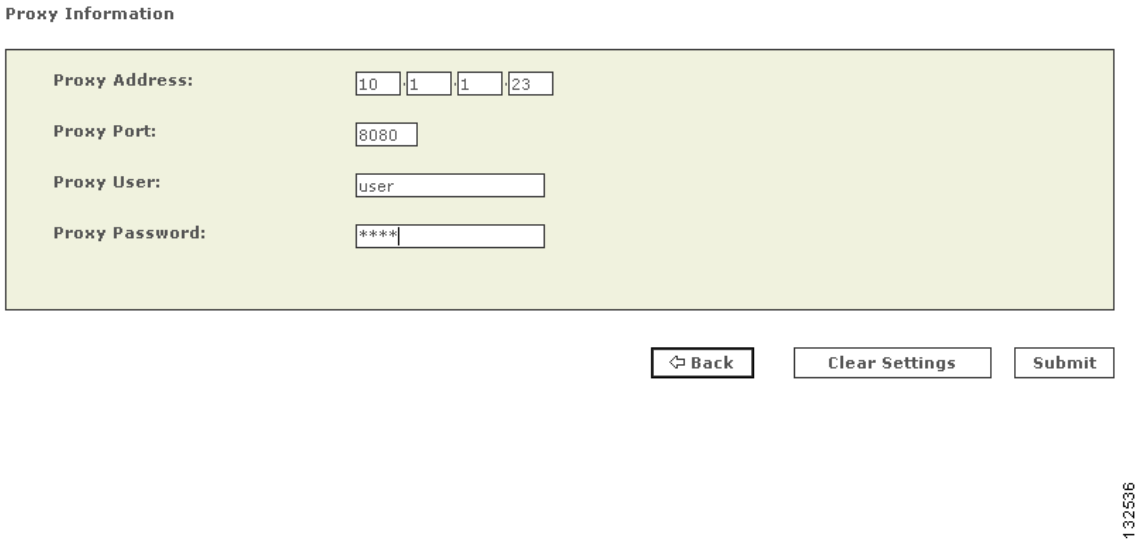
To specify the proxy settings for a Local Controller in the Global Controller user interface, follow these steps:

Step 1 Open the MARS user interface in your browser.

Step 2 Select **Admin > System Maintenance > Upgrade**.

Step 3 Click **Proxy Settings**. next to the Local Controller that you want to upgrade.

Result: The Global Controller user interface loads the Proxy Information page (**Admin > System Parameters > Proxy Settings)** on the selected Local Controller.



Step 4 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 5 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 not 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 6 In the Proxy Password field, specify the password associated with the username you just provided.

Step 7 Click **Submit** to save your changes.

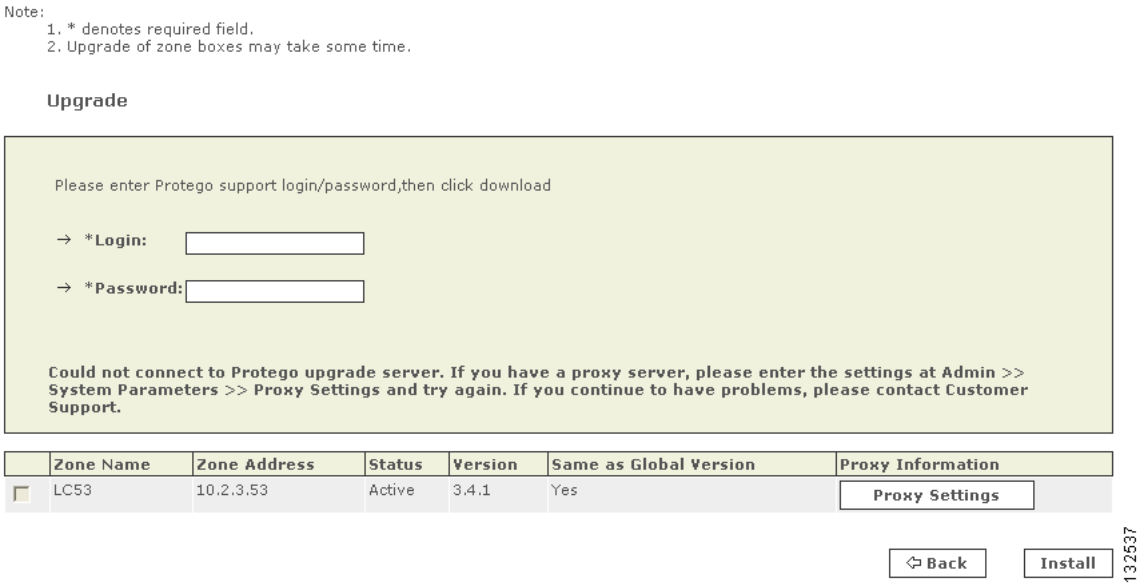
Upgrade Local Controller from the Global Controller User Interface

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.

Step 1 Open the MARS user interface in your browser.

Step 2 Select **Admin > System Maintenance > Upgrade**.

Result: The list of Local Controllers that can be selected to upgrade appears.



Step 3 In the Login and Password fields, enter the Internal Upgrade Server login and password that you have assigned to your Internal Upgrade Server.

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.

Step 4 Select the check box next to the Local Controller to upgrade, and click **Download**.

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 in the Global Controller, page 6-18.

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 5 Click **Install**.

Result: After you click Install, the remote system needs some time to process the upgrade. After the upgrade is complete, the remote system reboots. During the upgrade, the user interface is also restarted.

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) protocol. 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 NFS archive. 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 NFS server to archive the data for more than one MARS Appliance; however, you must specify a unique directory in the NFS 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 servers, see:

- http://www.cisco.com/en/US/products/ps6241/products_device_support_table09186a0080467232.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 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 NFS server to ensure a reliable network connection that can transmit 10 MB/second exists between the NFS 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 NFS server on the MARS Appliance and that you verify any intermediate routers and firewalls allow for multi-hour NFS 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 6-21
- Format of the Archive Share Files, page 6-21
- Archive Intervals By Data Type, page 6-23
- Guidelines for Restoring, page 6-40
- pnrestore, page A-43

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

1. Configure the NFS server:
   - Configure the NFS Server on Windows, page 6-24

  - Configure the NFS Server on Linux, page 6-27
  - Configure the NetApp NFS Server, page 6-28
2. Configure Lookup Information for the NFS Server, page 6-29
3. Configure the Data Archive Setting for the MARS Appliance, page 6-30

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 11-3.
- 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 6-21 and Access the Data Within an Archived File, page 6-32.
- 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 6-40, and Guidelines for Restoring, page 6-40.

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:\MARSBackups\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:\MARSBackups\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 NFS 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 statical 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 NFS archive 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 NFS 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 NFS archive. As a result, MARS performs simple data maintenance on the NFS 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 NFS server.

Refer to Table 6-2 for the archive interval for each type of data.

Table 6-2 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

Table 6-2 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
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.mspx

System Requirements for WSU 3.5

http://www.microsoft.com/windowsserversystem/sfu/productinfo/sysreqs/default.mspx

Microsoft Windows Services for UNIX 3.5 Reviewer's Guide

http://www.microsoft.com/windowsserversystem/sfu/techinfo/revguide.mspx

Performance Tuning Guidelines for Microsoft Services for Network File System

http://www.microsoft.com/technet/interopmigration/unix/sfu/perfnfs.mspx

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 6-24
- Configure a Share using Windows Services for UNIX 3.5, page 6-26

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 6-26.

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 6-27. Otherwise, continue with Configure the Data Archive Setting for the MARS Appliance, page 6-30.

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 6-30.

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 functionaliy of the shell environment running on the server. As such, you must use an external UNIX/Linux admininstrative 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 admininstrative host. For information on configuring such a host, refer to the documentation for you Network Appliance server.

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

Step 1 If you have not exported an 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 **FilerView**, 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 disable 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 and 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 6-30.

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 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.

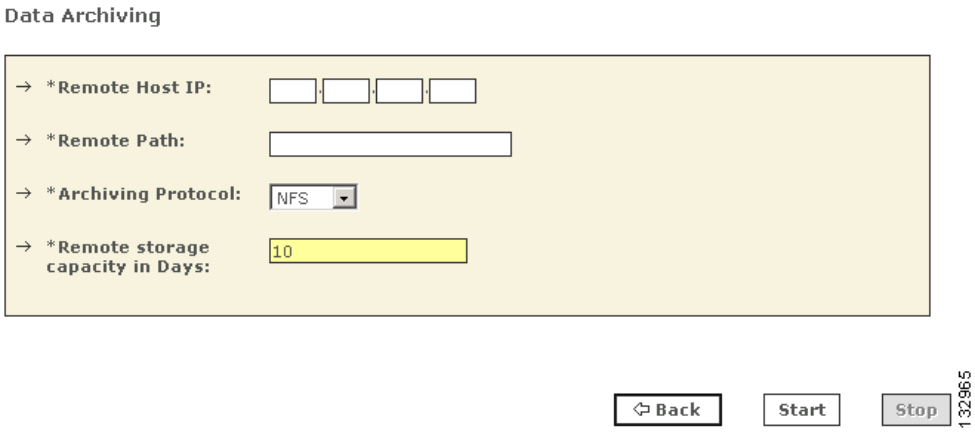
Before You Begin

You must set up the NFS server correctly to archive the appliance's data. See Configure the NFS Server on Windows, page 6-24 or Configure the NFS Server on Linux, page 6-27.

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 In the Remote Host IP field, enter the IP address of the remote NFS server or a NAS system that supports the NFS protocol.

Step 3 In the Remote Path field, enter the export path on the remote NFS server or a NAS system where you want to store the archive files.

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

Step 4 In the Archiving Protocol field, select **NFS**.

No other options are available.

Step 5 In the Remote storage capacity in Days field, 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.

Step 6 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 NFS server is not correctly configured. If you receive these messages, consult Configure the NFS Server on Windows, page 6-24 or Configure the NFS Server on Linux, page 6-27.

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

Step 7 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 6-21

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 <*achive_path*>

where *archive_path* is the remote path value specified in Configure the Data Archive Setting for the MARS Appliance, page 6-30.

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 6-33
- Downloading and Burning a Recovery DVD, page 6-33
- Recovery the MARS Operating System, page 6-34
- Re-Imaging a Local Controller, page 6-35
- Re-Imaging a Global Controller, page 6-36
- Restoring Archived Data after Re-Imaging a MARS Appliance, page 6-38

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 6-35, and Re-Imaging a Global Controller, page 6-36. If you have configured the MARS Appliance to archive data, as described in Configuring and Performing Appliance Data Backups, page 6-19, you can also recover the configuration and event data using the procedure in Restoring Archived Data after Re-Imaging a MARS Appliance, page 6-38.

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-4.1.1.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 or DVD+RW (DVD-R is not supported) 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 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 6-33. 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 A-22, hostname, page A-18, and the dns, page A-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 appropriate model in Hardware Descriptions—MARS 25R, 25, 55, 110R, 110, 210, GC2R, and GC2, page 1-4.)

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 date, 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

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 to the appropriate model in Hardware Descriptions—MARS 25R, 25, 55, 110R, 110, 210, GC2R, and GC2, page 1-4.)

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**.

a. If you are re-imaging a MARS 110R or 110, the following message appears on the console. Otherwise, continue with Step 6.

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

b. 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 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 (between an hour and an hour and a half), 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 5, "Initial MARS Appliance Configuration."

Step 9 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 Controller*.
- Recover the previously archived data using the procedure in Restoring Archived Data after Re-Imaging a MARS Appliance, page 6-38

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 date, 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 6-37.)

- 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

- 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 6-37, 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 appropriate model in Hardware Descriptions—MARS 25R, 25, 55, 110R, 110, 210, GC2R, and GC2, page 1-4.)

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
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 5, "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 Global Controller*.
- (**Recommended**) Recover the previously archived data using the procedure described in Restoring Archived Data after Re-Imaging a MARS Appliance, page 6-38.

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 6-40.

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 A-43, 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 6-35, or Re-Imaging a Global Controller, page 6-36, 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 <NFSServerIP>:/<archive_path>
```

Where *NFSSeverIP* 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 NFS server by IP address, separated by a :/ and then the pathname *NFSSeverIP*:/*archive_path*. For more information on these settings, see Configure the Data Archive Setting for the MARS Appliance, page 6-30.

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.

Upsizing a MARS Appliance

You can migrate, or upsize, to a different appliance model by following the same process and restrictions as configuring a standby or secondary appliance. The technique involves restoring a backup from the original, source appliance on the replacement appliance.

To restore to a different replacement 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 replacement appliance differs from restoring to the actual appliance that performed the archive.

Note This operation cannot be used to migrate from 4.3.x to 5.3.x, as the software version on the replacement appliance must match that of the software version used to create the backup image.

The following issues must be addressed when restoring to a replacement appliance:

- You must purchase a new license key for the replacement 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 replacement appliance.
- When restoring the image to the replacement appliance, you need to take the source appliance off the network or perform the operation behind a gateway that can perform NAT. When the replacement appliance comes up and you are on the same network, you receive an IP address conflict error, because the IP address assigned to the replacement appliance exactly matches that of the source appliance.

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 6-40.

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 6-40.

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 A-43.
- 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 6-40.
- 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 6-21.
- 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 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 A-43, 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 completed on each Local Controller before attempting to restore the Global Controller.

APPENDIX A

Command Reference

Revised: February 22, 2008, OL-14672-01

This appendix summarizes the command line interface (CLI) commands of MARS Appliance 5.3.x. You can access the CLI using one of four possible console connections, as described in Establishing a Console Connection, page 5-4.

This appendix contains the following sections:

Command Privileges and Modes

To access the CLI on the MARS Appliance, you must have a console connection to the appliance and use the system administrative account, pnadmin. No other administrative account defined in the web interface has privileges to access the console connection. For more information about establishing a console connection, see Establishing a Console Connection, page 5-4.

Note There is only one command mode for the MARS Appliances.

CLI Conventions

The CLI uses the following conventions:

- The key combination **^C**, or **Ctrl-C**, means hold down the **Ctrl** key while you press the **C** key.
- A string is defined as a nonquoted set of characters.

Checking Command Syntax

The serial console interface provides several types of responses to incorrect command entries:

Command Line Entry	System Display
Command line that does not contain any valid commands.	`Unknown command`
Valid command that does not contain required options.	`Incomplete command`
Valid command that does not provide valid options or parameters.	`Invalid input`

In addition, some commands have command-specific error messages that notify you that a command is valid, but that it cannot run correctly.

System Help

You can obtain help using the following methods:

- For a list of all commands and a brief description, enter **help** or **?**, and then press **Enter**.
- For syntax help on a specific command, type the command name, a space, a dash, and a lowercase **h**, and then press **Enter**, for example, **arp -h**. The help contains command usage information and syntax.

Command Summary

Table A-1 summarizes all commands available on the MARS Appliance. Refer to the full description of commands that you are not familiar with before using them.

Table A-1 Command Summary

Command	Location of GUI Equivalent	Summary Description	Location of Full Description
?	—	Print list of available commands.	?, page A-6
arp	—	Display/manipulate/store the arp table.	arp, page A-7
date	—	Set/show date.	date, page A-9
diskusage	—	Display percentage of disk used.	diskusage, page A-10
dns	Admin > System Setup > Configuration Information	Add/remove/show domain name resolving servers.	dns, page A-11
dnssuffix	Admin > System Setup > Configuration Information	Add/remove/show domain name suffixes search path.	dnssuffix, page A-12
domainname	—	Set/show name of the domain to which the MARS Appliance belongs.	domainname, page A-13
exit	—	Switch to standard mode/log out.	exit, page A-14

Table A-1 Command Summary (continued)

Command	Location of GUI Equivalent	Summary Description	Location of Full Description
expert	—	Switch to expert debugging mode (for using Cisco TAC personnel only).	expert, page A-15
gateway	Admin > System Setup > Configuration Information	Show/set default gateway of the MARS Appliance.	gateway, page A-16
help	—	Print list of available commands.	help, page A-17
hostname	The *Name* field on the Admin > System Setup > Configuration Information page.	Set/show the hostname of the MARS Appliance.	hostname, page A-18
hotswap[1]	—	Hot add or remove hard disk drive.	hotswap, page A-19
ifconfig	Admin > System Setup > Configuration Information	Configure/store network interface.	ifconfig, page A-22
model	—	Displays the model number and mode of the MARS Appliance.	model, page A-23
netstat	—	Show network statistics.	netstat, page A-24
nslookup	—	Look up the IP address or domain name.	nslookup, page A-25
ntp	—	Synchronize system clock with Network Time Protocol (NTP) servers.	ntp, page A-26
passwd	Admin > User Management (pnadmin)	Change administrative password used to access the appliance from the Secure Shell (SSH) or GUI client.	passwd, page A-27
passwd expert	—	Change the customer portion of the expert debugging mode password used to access the appliance from the Secure Shell (SSH).	passwd expert, page A-28
ping	—	Sends Internet Control Message Protocol (ICMP) echo_request packets for diagnosing basic network connectivity.	ping, page A-29
pndbusage	—	Shows the current database usage and explains how future space will be claimed, either through unused partitions or purging of oldest data.	pndbusage, page A-31
pnexp	—	Export configuration and event data from a 4.3.x appliance for import into a MARS Appliance running 5.3.1 or later.	pnexp, page A-32
pnimp	—	Import configuration and event data previously exported from a MARS Appliance running 4.3.x into a one running 5.3.1 or later.	pnimp, page A-35

Table A-1 Command Summary (continued)

Command	Location of GUI Equivalent	Summary Description	Location of Full Description
pnlog	Admin > System Maintenance > View Log Files Admin > System Maintenance > Set Runtime Logging Levels Help > Feedback	Show system log/set log level.	pnlog, page A-38
pnreset	—	Reset the MARS Appliance to factory defaults.	pnreset, page A-40
pnrestore	—	Restore MARS system configuration and data from a backup.	pnrestore, page A-43
pnstart	—	Start MARS applications.	pnstart, page A-47
pnstatus	—	Show running status of MARS applications.	pnstatus, page A-48
pnstop	—	Stop MARS applications.	pnstop, page A-49
pnupgrade	Admin > System Maintenance > Upgrade Admin > System Parameters > Proxy Settings	Upgrade the software running on the MARS Appliance.	pnupgrade, page A-50
raidstatus[1]	—	Display the status of hard disk drives.	raidstatus (5.x), page A-52
reboot	—	Reboot the MARS Appliance.	reboot, page A-57
route	—	Configure/store routing tables.	route, page A-58
script	—	Command line interface to provided script files. usage: script [-b] program	script, page A-60
show healthinfo	—	Displays operational status of components in the MARS Appliance.	show healthinfo, page A-61
show inventory	—	Displays identifying details of essential components in the MARS Appliance.	show inventory, page A-63
shutdown	—	Shut down the MARS Appliance.	shutdown, page A-65
snmpwalk	—	Communicates with a network entity using SNMP GETNEXT requests.	snmpwalk, page A-66
ssh	—	User interface to the SSH client.	ssh, page A-67
sslcert	—	Generate a new self-signed SSL certificate.	sslcert, page A-69
ssllist	—	List existing ssl certificates	ssllist, page A-70
syslogrelay setcollector	—	Displays the IP address of the device to which syslogs are forwarded.	syslogrelay setcollector, page A-71

Table A-1 Command Summary (continued)

Command	Location of GUI Equivalent	Summary Description	Location of Full Description
syslogrelay src	—	Displays list of source addresses for which syslogs are forwarded.	syslogrelay src, page A-72
syslogrelay list	—	Displays list of syslog collector and sources.	syslogrelay list, page A-74
sysstatus	—	User interface to the Unix top command.	sysstatus, page A-76
tcpdump	—	Dump traffic on a network.	tcpdump, page A-78
telnet	—	User interface to the TELNET client.	telnet, page A-79
time	—	Set/show time for the MARS Appliance.	time, page A-80
timezone	—	Set/show timezone for the MARS Appliance.	timezone, page A-81
traceroute	—	Displays the network route that packets take to reach a specified host.	traceroute, page A-82
unlock	Admin > Management > User Management	Unlocks access to the GUI for all or specified accounts after login failure.	unlock, page A-83
version	Help > About	Displays the version of software running on the MARS Appliance.	version, page A-84

1. This command applies only to the MARS 100/100e, MARS 200, and the Global Controller appliance models.

Command Syntax Conventions

Command descriptions in this document and in the CLI help system use the following conventions:

- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate optional elements.
- Braces ({ }) indicate a required choice. Braces within square brackets ([{ }]) indicate a required choice within an optional element.
- Angle brackets (< >) indicate the following elements:
  - Arguments
  - Character string that you enter but that does not appear on the screen, such as a password
- Bold indicates commands and keywords that are entered literally as shown.
- Italics indicate arguments for which you supply values.

Commands

This section describes the Cisco Security Monitoring, Analysis, and Response System commands. Command names are case sensitive.

?

The **?** command lists available commands and provides a brief description of each command.

Syntax Description

This command has no arguments or keywords.

Examples

To see the full list of commands that are available, enter:

```
?
```

arp

The **arp** command relates to the ARP cache on the MARS Appliance. You can view the list of mappings, clear an entry, or add a new mapping.

To display the current entries in the ARP cache, enter:

arp

To display the cached entries for a specific host, enter:

arp [**-evn**] [**-H** *type*] [**-i** *if_local*] **-a** [*hostname*]

To add a host to the cache, enter one of the following commands:

arp [**-v**] [**-H** *type*] [**-i** *if_local*] **-s** *hostname hw_addr* [*netmask*] **pub**

arp [**-v**] [**-H** *type*] [**-i** *if_local*] **-s** *hostname hw_addr* [**temp**]

arp [**-v**] [**-H** *type*] [**-i** *if_loca*] **-Ds** *hostname if_dest* [*netmask*] **pub**

To delete a host from the cache, enter:

arp [**-v**] [**-i** *if_local*] **-d** *hostname* [**pub** | **nopub**]

In all places where a hostname is expected, you can alternatively enter an IP address in dotted-decimal notation.

As a special case for compatibility the order of the hostname and the hardware address can be exchanged.

Each complete entry in the ARP cache is marked with the C flag. Permanent entries are marked with M and published entries have the P flag.

Note You cannot add arp entries from a file, as you do not have access to the file system on the MARS Appliance.

Syntax Description

noneThe default behavior *of this command* displays the IP address, hardware type, interface name, and MAC address associated with the network interface in the MARS Appliance.

-vTell the user what is going on by being verbose.

-nDisplay numerical addresses instead of symbolic host, port, or usernames.

-H *type*When setting or reading the ARP cache, this optional parameter identifies which class of entries (hardware type) ARP should check for. The default value of this parameter is *ether*. The list of valid type values is as follows:

- strip (Metricom Starmode IP)
- ash (Ash)
- ether (Ethernet)
- tr (16/4 Mbps Token Ring)
- tr (16/4 Mbps Token Ring [New])
- ax25 (AMPR AX.25)

- netrom (AMPR NET/ROM)
- rose (AMPR ROSE)
- arcnet (ARCnet)
- dlci (Frame Relay DLCI)
- fddi (Fiber Distributed Data Interface)
- hippi (HIPPI)
- irda (IrLAP)
- x25 (generic X.25) .

-a [*hostname*],Displays the entries of the specified hosts. If the hostname parameter is not used, all entries are displayed.

-d *hostname*Delete any entry for the specified host.

-DUse the interface *if_dest*'s hardware address.

-eShows the entries in default (Linux) style.

-i *If_local*Select an interface in the appliance. When dumping the ARP cache only entries matching the specified interface are printed. When setting a permanent or temp ARP entry, the entry is associated with this interface; if this option is not used, the routing table is used to determine the most likely interface through which the address is reachable. For *pub* entries the specified interface is the interface on which ARP requests are answered. This value must be different from the interface to which the IP datagrams will be routed (*if_dest*).

-s *hostname hw_addr*

Manually create an ARP address mapping entry for host hostname with hardware address set to *hw_addr* class. For the Ethernet class, use the 6-bytes in hexadecimal notation, separated by colons. You can determine this value using the **ipconfig /all** command on the host for which you are defining this entry. When adding proxy arp entries (that is, those with the publish flag set), a netmask may be specified to proxy arp for entire subnets. If the temp flag is not supplied entries are permanently stored in the ARP cache. You cannot define an ARP entry for an entire subnet.

Examples

To permanently add an arp cache entry for a management host (marsgui) reachable from eth1, enter:

```
arp -v -H ether -i eth1 -s marsgui 00:05:9A:3C:78:00 pub
```

To remove the entry defined above, enter:

arp -v i eth1 -d marsgui nopub

date

To display or set the system date, use the **date** command.

Note Time changes on the appliance are immediate, which can affect active incident correlation. If you change the time by greater than 30 minutes, you should restart your appliance to ensure that all processes synchronize using the new time.

date [*newdate*]

Syntax Description

none The default behavior of this command displays the date in the mm/dd/yy format (for example, 04/28/05)

newdate Identifies the date to which you want to change the appliance clock. You can use either of the following formats: mm/dd/yyyy or mm/dd/yy.

Examples

To display the current date, enter:

```
date
```

To change the date to March 12, 2004, enter either of the following commands:

```
date 03/12/2004

date 03/12/04
```

diskusage

To display the amount of disk space available on all partitions, enter

diskusage

For all MARS Appliance models, the Oracle database has three partitions:

- /u01: Stores the Oracle binary files.
- /u02: Stores the data files.
- /u03: Stores the replay log files, which are cached, in-memory working files not yet committed to the data store.

If any of these partitions reaches 99% capacity, the Oracle database will experience operational issues.

The size of the data partition (/u02) varies based on the model:

- MARS 20: 74 GB
- MARS 50: 148 GB
- MARS 100: 565 GB
- MARS 200: 795 GB

Syntax Description

noneThe default behavior *of this command* displays amount of disk space available on all partitions in the MARS Appliance

Examples

To display the disk usage for all partitions in the MARS Appliance, enter the following command:

```
diskusage
```

The following is sample output for a MARS 100, as noted by the size of the /u02 partition:

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda3              20G  5.7G   13G  31% /
/dev/sda1             129M   14M  108M  12% /boot
/dev/sda5              20G  4.8G   13G  26% /opt
/dev/sda6              20G  130M   18G   1% /log
/dev/sda7              29G  134M   27G   1% /pnarchive
/dev/sda8              20G  2.7G   16G  14% /u01
/dev/sda9             9.8G  2.2G  7.2G  23% /u03
/dev/sda10            565G   15G  522G   3% /u02
none                 1005M     0 1005M   0% /dev/shm
```

dns

To display or specify the IP addresses of the Domain Name Services (DNS) servers that the MARS Appliance should use to resolve IP addresses into hostnames, use the **dns** command.

dns [*primary*] [*secondary*] [*tertiary*]

Note If the DNS configuration is changed from the web interface, you must perform a pnstop and then a pnstart 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 6-5 and Start Appliance Services via the Console, page 6-5.

Syntax Description

noneThe default behavior *of this command* displays the current set of IP addresses assigned to the primary, secondary, and tertiary DNS servers.

*primary*Identifies the IP address of the DNS server that should be used first to resolve hostnames and/or IP addresses. Only the primary is required.

*secondary*Identifies the IP address of the DNS server that should be used second to resolve hostnames and/or IP addresses. This address is optional. If this value is left blank, any previously defined secondary entries are deleted.)

*tertiary*Identifies the IP address of the DNS server that should be used last to resolve hostnames and/or IP addresses. This address is optional. If this value is left blank, any previously defined tertiary entries are deleted.

Examples

To display the current DNS server entries, enter:

```
dns
```

To set the primary DNS server to 192.168.101.3 and the secondary DNS server to 192.168.102.5, enter:

```
dns 192.168.101.3 192.168.102.5
```

dnssuffix

To display, add, or remove the DNS search paths associated with the adapters in the MARS Appliance, use the **dnssuffix** command.

dnssuffix [**add** | **del**] *searchpath*

Syntax Description

noneThe default behavior *of this command* displays the current domain search paths defined for the appliance.

addSpecifies that the text that follows "add" should be added as a new dns search path.

delSpecifies that the text that follows "del" should be removed from the dns search path, if found.

*searchpath*Identifies the domain name to be used for local DNS searches.

Examples

To display the current DNS search path, enter:

```
dnssuffix
```

To add example.com to the search path, enter:

```
dnssuffix add example.com
```

To remove example.com from the search path, enter:

```
dnssuffix del example.com
```

domainname

To set or show the DNS domain of the MARS Appliance, use the **domainname** command.

domainname [*domain*]

Syntax Description

none The default behavior *of this command* displays the current domain value, if defined. Otherwise, it displays no value.

domain Name of DNS domain.

Examples

This command sets the domain name to example.com:

```
domainname example.com
```

To display the current domain name, enter:

```
domainname
```

exit

To log out of the system, use the **exit** command.

exit

Syntax Description

This command has no arguments or keywords.

Examples

The following command logs you out of the system:

```
exit
```

expert

To enable expert debugging mode on the MARS Appliance, use the **expert** command.

expert

The **expert** command, undocumented before the 4.1.3, is for exclusive use by Cisco to aid in debugging customer issues that require direct access to the internal data store of the MARS Appliance. You may further restrict access to the **expert** command by setting the customer portion of the expert mode password via the **passwd expert** command. This command removes the default expert mode password set on the appliance from the factory.

While you can use the **passwd expert** command to restrict access to the **expert** command, only authorized Cisco support personnel are able to access the expert debugging mode of an appliance.

See also passwd expert, page A-28.

Syntax Description

noneThe default behavior of this command prompts the user to provide authentication credentials to enable the expert debugging mode. Only authorized Cisco support personnel can properly authenticate.

Examples

None.

gateway

To show or set the default gateway to be used by the MARS Appliance, use the **gateway** command.

gateway [*address*]

Syntax Description

none The default behavior of this command displays the current gateway setting, if defined. Otherwise, it displays no value.

address Changes the default gateway address to the value specified. Use decimal notation.

Examples

To display the current default gateway address used by the appliance, enter:

```
gateway
```

To set the default gateway address to 192.168.101.1, enter:

```
gateway 192.168.101.1
```

help

The **help** command displays a complete list of commands that are available at the serial console.

help [*name*]

Syntax Description

none The default behavior of this command displays the full list of commands that are available and their corresponding brief description.

name Identifies the command for which you want to see the brief description.

Examples

To display the complete list of available commands, enter:

```
help
```

To display a brief description about the **netstat** command, enter:

```
help netstat
```

hostname

To set or show the hostname of the MARS Appliance, use the set **hostname** command.

hostname [*hostname*]

Note Changing the hostname requires that the appliance reboot. This reboot will occur automatically after your change the hostname. However, you are prompted to verify the hostname change. To cancel the hostname change without rebooting, enter **no** at the `Hostname change will cause the system to reboot. Do you want to proceed?` prompt.

Syntax Description

none The default behavior of this command displays the current hostname value, if defined. Otherwise, it displays no value.

hostname Identifies the value to which the hostname for the MARS Appliance should be set.

Examples

This command sets the MARS Appliance name to csmars1:

```
hostname csmars1
```

To see the current hostname, enter:

```
hostname
```

hotswap

Use the **hotswap** command to remove and add hard drives to MARS Appliances with RAID arrays. This command *must* be executed before a hard drive is physically removed from or added to the RAID array.

hotswap {**add** | **remove** | **list all**} *disk*

Command History

Release	Modification
3.X	This command was introduced.
5.2.4	The **list all** keyword was added. The *disk* argument range of values include 0.
5.3.2	The **list all** keyword was modified to display the chassis hard drive slot to Port and PD number map; support for MARS 55 was added.

Syntax Description

add	Indicates that the hard drive with the designated *disk* number is to be added to the RAID array.
remove	Indicates that the hard drive with the designated *disk* number is to be removed from the RAID array.
list all	Displays a map of chassis hard drive slots and their related Port or PD number.
disk	Thechassis hard drive slot number of the hard drive to be hotswapped.

Usage Guidelines

To hotswap a hard drive is to replace the hard drive without powering down or rebooting the appliance.

For MARS Appliances 110, 110R, 210, GC2R, and GC2, the valid *disk* arguments range from 0 to 5.

For the MARS Appliance 55 the valid *disk* arguments are 0 and 1.

To hotswap a hard drive, execute **hotswap remove** *disk*, replace the hard drive in the slot designated by *disk*, then execute **hotswap add** *disk*. Check the operational status of the hard drive and the RAID array with the **raidstatus** command.

Whenever a **hotswap remove** *disk* command is executed, the hard drive in that slot is removed from the array and another must be added to restore full redundancy to the RAID array.

If the wrong *disk* value is entered, that hard drive is dropped from the RAID array, but can be rebuilt into the array without physically removing and inserting the hard drive by executing a **hotswap add** *disk* command. It can take up to 300 minutes for a single hard drive to be rebuilt into the RAID array.

For more information on RAID hotswapping procedures, see the chapter, “System Maintenance” in the *User Guide for Cisco Security MARS Local Controller* at the following URL:

MARS Appliances 55, 110R, 110, 210, GC2R, and GC2

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/5.3/user/guide/local_controller/maintain.html

Examples

In the following example, a hard drive is hotswapped in slot 5 of a MARS 210. The hard drive status is verified with the **raidstatus** command:

```
[pnadmin]$ version
5.3.2 (2702)
[pnadmin]$ hotswap list all
Hardware RAID is found with 6 disks!
Disks available to be hotswapped:
        |==============|==============|==============|
        |     PD 1     |     PD 3     |     PD 5     |
        |--------------|--------------|--------------|
        |     PD 0     |     PD 2     |     PD 4     |
        |==============|==============|==============|

[pnadmin]$ hotswap remove 5

Adapter: 0: EnclId-14 SlotId-5 state changed to OffLine.
Disk 5 can now be safely removed from the system.


[pnadmin]$ raidstatus
Adapter Information:
-------------------------------------------------------
Product Name     : Intel(R) RAID Controller SROMBSAS18E
Firmware Version : 1.03.00-0211
BIOS Version     : MT30

Adapter RaidType        Status  Stripe  Size            Cache
---------------------------------------------------------------
a0      Raid-10         Degraded        64kB    2097151MB       Enabled

PD      Status  Size & Block                            Model
        Serial#
-------------------------------------------------------------------------------
p0      Online  715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD09EEZ
p1      Online  715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD09CQT
p2      Online  715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD094KY
p3      Online  715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD08NZX
p4      Online  715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD09EWP
p5      Offline 715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD06AQ2


[pnadmin]$ hotswap add 5

Started rebuild progress on device(Encl-14 Slot-5)
Disk 5 has been successfully added to RAID



[pnadmin]$ raidstatus
Adapter Information:
-------------------------------------------------------
Product Name     : Intel(R) RAID Controller SROMBSAS18E
Firmware Version :  1.03.00-0211
BIOS Version     : MT30

Adapter RaidType        Status  Stripe  Size            Cache
```

```
-------------------------------------------------------------
a0      Raid-10         Degraded        64kB    2097151MB       Enabled

PD      Status  Size & Block                           Model
        Serial#
-------------------------------------------------------------------------------
p0      Online  715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD09EEZ
p1      Online  715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD09CQT
p2      Online  715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD094KY
p3      Online  715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD08NZX
p4      Online  715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD09EWP
p5      Rebuild 715404MB [0x575466f0 Sectors]   ATA     ST3750640NS     E
        3QD06AQ2

Rebuild Progress on Device at Enclosure 14, Slot 5 Completed 17% in 32 Minutes.
```

Related Commands

Command	Description
raidstatus (5.x)	Displays the status of the RAID array and of the individual HDDs.

ifconfig

To display or modify the current IP address and network mask pairs associated with the network interfaces installed in the MARS Appliance, use the **ifconfig** command.

ifconfig {**eth0** | **eth1**} *ip_addr netmask*

Syntax Description

noneThe default behavior of this command displays the current settings for both the eth0 and eth1 interfaces.

eth0 Identifies that you want to set the IP address/netmask value for the eth0 interface. This option cannot be used in conjunction with eth1. If you do not specify the *ip_addr* and `netmask` values, this option displays the current settings for the eth0 interface.

eth1 Identifies that you want to set the IP address/netmask value for the eth0 interface. This option cannot be used in conjunction with eth0. If you do not specify the *ip_addr* and `netmask` values, this option displays the current settings for the eth1 interface.

*ip_addr*Identifies the IP address to assign to the specified interface (eth0 or eth1). You must specify a netmask value following this value.

*netmask*Identifies the network mask value to use with the address specified. You must specify the IP address before specifying this value.

Usage Guidelines

For more information on the physical placement of eth0 versus eth1, see the corresponding appliance model under Hardware Descriptions—MARS 25R, 25, 55, 110R, 110, 210, GC2R, and GC2, page 1-4.

For MARS Appliances 110, 110R, 210, GC2R, and GC2, eth0 is integrated NIC 1, eth1 is integrated NIC 2; eth2 and eth4 are unsupported.

Examples

To display the current interface address settings, enter:

```
ifconfig
```

To set the IP address of eth1 to 192.168.101.2/32, enter:

```
ifconfig eth1 192.168.101.2 255.255.255.255
```

Related Commands

Command	Description
show healthinfo	Displays operational status of appliance components.

displays the detailed usage guidelines on this command.

model

Use the **model** command to display the model and mode of the MARS Appliance.

model

Syntax Description

noneThe default behavior of this command lists model and mode of the MARS Appliance.

-hDisplays the detailed usage guidelines on this command.

Examples

The following displays the model information about the MARS Appliance:

```
[pnadmin]$ model
mars50
local
standard
[pnadmin]$
```

netstat

Use the **netstat** commands to display the status of network connections on either TCP, UDP, RAW or UNIX sockets.

netstat

By default, the **netstat** command only displays status on active sockets that are not in the LISTEN state (that is, connections to active processes).

Syntax Description

noneThe default behavior of this command lists current Internet connections and UNIX domain sockets.

-hDisplays the detailed usage guidelines on this command.

-rDisplays information about the routing table on the MARS Appliance.

-vDisplays verbose information. Useful for obtaining information about unconfigured address families.

-VDisplays version of command.

nslookup

Look up the IP address or domain name using its counterpart. This command launches an interactive console that displays information that you can use to diagnose Domain Name System (DNS) infrastructure. Before using this tool, you should be familiar with how DNS works.

Syntax Description

nslookup puts you into interactive command mode. To quit the command mode and return to the command prompt, enter **exit**.

ntp

The Network Time Protocol (NTP) synchronizes the clocks of computers across a network. By specifying an NTP server, you are instructing the appliance to contact that server to retrieve appropriate time settings. Synchronized times is especially important to MARS, because timestamp information provided by the reporting devices (and the appliance itself) is critical to accurate reconstruction of what transpires on the network.

Note Time changes on the appliance are immediate, which can affect active incident correlation. If you change the time by greater than 30 minutes, you should restart your appliance to ensure that all processes synchronize using the new time.

Warning **When operating in a Global Controller/Local Controller hierarchy configuration, 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.**

Use **ntp server** to identify the primary and secondary NTP server with which the appliance should synchronize. To force a synchronization with the NTP server, use **ntp sync**. To disable the use of ntp by this appliance, use **ntp disable**.

ntp server [*ntp_server1*] [*ntp_server2*]

Syntax Description

noneThe default behavior of this command displays the current settings for the NTP servers. If no servers have been identified, it displays the message: ntp is not setup.

ntp_server1 Identifies the server, by IP address, that runs the NTP server from which you want this MARS Appliance to retrieve system time information. This time value sets the clock used to date and correlate events that are received by the appliance.

ntp sync Forces the MARS Appliance to synchronize with the NTP server. If the first server is unreachable, the appliance attempts to synchronize with the secondary server.

ntp disable Disables the use of NTP on the MARS Appliance.

Examples

To specify that 192.168.101.5 and 192.168.103.21 are your primary and secondary NTP servers, respectively, enter:

```
ntp server 192.168.101.5 192.168.103.21
```

To force a synchronization between the MARS Appliance and the NTP servers you have identified, enter:

```
ntp sync
```

To disable NTP synchronization, enter:

```
ntp disable
```

passwd

To change the password of the system administrative account (pnadmin) associated with the appliance, use the **passwd** command.

passwd [*new_pword*]

Syntax Description

noneThe default behavior *of this command* displays the command's usage guidelines.

*new_pword*Identifies the password to which you want to set the system administrative account's password.

Examples

To change the system administrative account password to *Ou812o*, enter:

```
[pnadmin]$ passwd
New password: <Ou812o>
Retype new password: <Ou812o>
[pnadmin]$
```

passwd expert

To change the customer portion of the password associated with expert debugging mode of the appliance, use the **passwd expert** command.

passwd expert [*new_pword*]

While you can use the **passwd expert** command to restrict access to the **expert** command, only authorized Cisco support personnel are able to access the expert debugging mode of an appliance.

See also expert, page A-15.

Syntax Description

noneThe default behavior *of this command* displays the command's usage guidelines.

*new_pword*Identifies the password to which you want to set the expert mode password.

Examples

To change the customer portion of the password associated with expert mode of the appliance to *Ou812o*, enter:

```
[pnadmin]$ passwd expert
New password: <Ou812o>
Retype new password: <Ou812o>
[pnadmin]$
```

ping

To send ICMP echo_request packets for diagnosing basic network connectivity between the appliance and a network host, use the **ping** command.

ping [**-LRUbdnqrvV**] [**-c** *count*] [**-i** *interval*] [**-w** *wait*] [**-p** *pattern*] [**-s** *packetsize*] [**-t ttl**] [**-I** *if_addr*] [**-T** *option*] [**-Q** *tos*] *host*

Use Ctrl+C or ^C to stop the output of this command and return to the command prompt.

Note The options used in this command are case sensitive.

Syntax Description

noneThe default behavior *of this command* displays the command's usage guidelines.

-bAllow pinging a broadcast address.

-c *count*Stop after sending count ECHO_REQUEST packets. With deadline option, ping waits for count ECHO_REPLY packets, until the timeout expires.

-dSet the SO_DEBUG option on the socket being used.

-i *wait*Identifies the wait interval in seconds between each sent packet. The default is one second.

-I *if_addr*Set source address to the specified interface address.

-l *preload*If preload is specified, ping sends that many packets as fast as possible before falling into its normal mode of behavior. Only the super-user can use this option.

-LSuppress loopback of multicast packets. This flag only applies if the ping destination is a multicast address.

-nNumeric output only. No attempt will be made to look up symbolic names for host addresses.

-p *pattern*You can specify up to 16 "pad" bytes to fill out the packet you send. This is useful for diagnosing data-dependent problems in a network. For example, "-p ff" will cause the sent packet to be filled with all 1s.

-Q *tos*Set Quality of Service-related bits in ICMP datagrams. The tos value can be either decimal or hex number. Traditionally (RFC1349), these have been interpreted as 0 for reserved (currently being redefined as congestion control), 1-4 for Type of Service, and 5-7 for Precendence. Possible settings for Type of Service are minimal cost, 0x02; reliability, 0x04; throughput, 0x08; and low delay, 0x10. Multiple TOS bits should not be set simultaneously. Possible settings for special Precedence range from priority (0x20) to net control (0xe0). You must be root (CAP_NET_ADMIN capability) to use Critical or higher Precedence value. You cannot set bit 0x01 (reserved) unless ECN has been enabled in the kernel. In RFC2474, these fields have been redefined as 8-bit Differentiated Services (DS), consisting of bits 0-1 of separate data (ECN will be used, here), and bits 2-7 of Differentiated Services Codepoint (DSCP).

-qQuiet output. Nothing is displayed except the summary lines at startup time and when finished.

-RRecord route. Includes the RECORD_ROUTE option in the ECHO_REQUEST packet and displays the route buffer on returned packets. Note that the IP header is only large enough for nine such routes. Many hosts ignore or discard this option.

-rBypass the normal routing tables and send directly to a host on an attached network. If the host is not on a directly attached network, an error is returned. This option can be used to ping a local host through an interface that has no route through it.

-s *packetsize*Specifies the number of data bytes to be sent. The default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.

-t ttlSet the IP Time to Live for multicasted packets. This flag only applies if the ping destination is a multicast address.

-T *option*Set special IP timestamp options. Timestamp option may be either tsonly (only timestamps), tsandaddr (timestamps and addresses), or tsprespec host1 [host2 [host3 [host 4]]] (timestamp prespecified hops).

-M *hint*Select Path MTU Discovery strategy. **hint** may be either do (prohibit fragmentation, even local one), want (do PMTU discovery, fragment locally when packet size is large), or don't (do not set DF flag).

-UPrint true user-to-user latency (the old behavior).

-vDisplays verbose output.

-VDisplays the version of this command.

-w *deadline*Specify a timeout, in seconds, before ping exits regardless of how many packets have been sent or received.

pndbusage

To determine how much of the total database space is used, use the **pndbusage** command:

pndbusage

This command displays the percentage used within the current partition, as well as specifies whether additional partitions are available. If no unused partitions exist, the command identifies which partition will be purged, provides an approximate schedule for when that purge will occur, and specifies the date range and total number of events scheduled to be purged.

Syntax Description

noneThe default behavior *of this command* displays the percentage of total space used by the database.

Examples

Two possible outputs exist for this command:

- If empty partitions are available, the output appears as follows:

```
Current partition started on <start date> and uses
<number>% of its available capacity.
Switching to next partition is estimated for <estimated switching date>
<number> empty partitions are available for storage.
```

- If no empty partitions exists, the output appears as follows:

```
Current partition started on <start date> and uses
<number>% of its available capacity.
Switching to next partition is estimated for <estimated switching date>
<number> events, received between <purge start date> and <purge end date> will be
purged.
```

In this case, the third line indicates the data that will be purged on the <estimated switching date>.

Indents are displayed as shown above.

pnexp

From the **pnexp** command prompt, you can access time and disk space required for a data export, review the size of the database and the data therein, start and stop the export of configuration data, event data, or both, and check the status of an ongoing export. To access the **pnexp** command prompt, use the **pnexp** command at the pnadmin prompt:

pnexp

Command History

Release	Modification
4.3.1	This command was introduced in the Local Controller and Global Controller version 4.x train.

Syntax Description

help	Displays a list of valid subcommands.
quit | exit	Quit and exit the **pnexp** command. Return to the pnadmin command prompt.
status	Display the status of the current data export operation.
log {all | recent}	Show all or recent data exporting log entries.
data	Displays the number of events, report results, statistics, and incidents in the database.
config	Displays the number of devices, reports, and rules in the database. This command should be used as a point of comparison once the configuration is imported into the target appliance. Compare with the output of the **pnimp config** command.
stop	Stop the data export operation.
esti_time [MM/DD/YY:HH]	Estimates how much time and storage is required to export the event data that was received by MARS after a specified start time—only the events received after that time are migrated. If the last argument is not specified, then the estimate is based on all event data in the database. **Note** The data export tool ignores data that was previously archived for the MARS Appliance. Each time the command is run, it writes data to a new NFS directory regardless whether data has already been archived.
export {config | data | all} {*nfs_path*} **[MM/DD/YY:HH]**	Export MARS configuration data ({**config**}), or events/reports/statistics/incidents data ({**data**}), or both ({**all**}) to the specified NFS path ({*nfs_path*}). If the last optional argument is given, only data received after that time will be exported. Example: export all 10.1.1.1:/mars/archive 02/28/07:00. The *nfs_path* value identifies the top-level archive folder on the NFS server; it does not identify a specific archive date. If you export event data to an NFS server, the specified NFS path value must *not* match the archive path used by the source appliance. The **pnexp** command creates the proper archive folder under this path. **Note** Only the start date is specified, the end date is always the current time (when event receiving is stopped.

Usage Guidelines

Use the **pnexp** command to prepare and export configuration and event data from MARS Appliance running 4.x as separate data so you can import either or both on a MARS Appliance running 5.x software. When the export operation begins, that MARS Appliance stops receiving events until the exporting process completes.

Caution Once the export operation begins, event data published to this appliance is lost, as is any event data that is not already written to the database. Follow the instructions provided in Data Migration Work Flow, page -2 to avoid losing event data.

The configuration export runs in the foreground displaying its status and errors immediately, where as event data export runs in the background. Use the **log {all | recent}** command to view the running status log for event data export.

The event export part of this operation can take a long time, as the export speed ranges between 6,000 and 30,000 events per second depending on the appliance model. Event data is exported in the following order: report result, statistics, incident and firing events, and event session. If the remote NFS server becomes unavailable during a lengthy export operation, the **pnexp** program attempts to remount the server. For event data export, logs are written to the `/log/export.log` file.

Examples

The following example specifies that the MARS Appliance should export the configuration data to the NFS archive found at 192.168.3.138:/storage/mars_migration:

```
pnexp> export config 192.168.3.138:/storage/mars_migration
WARNING: this will stop CS-MARS, do you wish to continue (yes/no): yes

!!! The exported config data is saved under sub-directory of
192.168.3.138:/storage/mars_migration/LC-220_2007-09-04-11-25-10
!!! Stopping CS-MARS processes ...
!!! Exporting config data now

Dumping configuration data, may take a while ...
Configuration dump finished.
Configdump to 192.168.3.138:/storage/mars_migration/LC-220_2007-09-04-11-25-10 finished
successfully.
```

The following example specifies that the MARS Appliance should export the event data corresponding to the configuration data in the previous example:

```
pnexp> export data 192.168.3.138:/storage/mars_migration 05/01/07:0
WARNING: this will stop CS-MARS, do you wish to continue (yes/no): yes

Estimated total number of events to export: 1401080357
Estimated time to export events: 12 hours 58 minutes
Estimated space for exported events: 66809 MB

Do you wish to continue (yes/no): yes
!!! The exported event data is saved at
192.168.3.138:/storage/mars_migration/LC-220_2007-09-04-11-25-10
!!! Stopping CS-MARS processes ...
!!! Restarting oracle ...
!!! Exporting data in background now, enter 'status' or 'log' to view data exporting
status and/or logs.
```

Tip Use the **log all** command to determine where the archives are saved. This path information is required by the **pnimp** command.

```
Sep  4 11:25:21.293 2007@LM_INFO@Thread 1024:START DATA EXPORTING...
Sep  4 11:25:21.293 2007@LM_INFO@Thread 1024:Parameter: nfs_path =
192.168.3.138:/storage/mars_migration/LC-220_2007-09-04-11-25-10
Sep  4 11:25:21.293 2007@LM_INFO@Thread 1024:Parameter: event_start_time = 05/01/07:0
Sep  4 11:25:21.395 2007@LM_INFO@Thread 1024:Trying to mount /mnt/pnarchive
Sep  4 11:25:22.677 2007@LM_INFO@Thread 1024:EXPORTING REPORT RESULTS ...
```

Related Commands

Command	Description
pnimp	Import configuration and event data into a MARS Appliance running version 5.3.1 or later.

pnimp

From the **pnimp** command prompt, you can access time required for a data import, review the size of the event data set on the NFS server, start and stop the import of configuration data or event data, and check the status of an ongoing import. To access the **pnimp** command prompt, use the **pnimp** command at the pnadmin prompt:

pnimp

Command History

Release	Modification
5.3.1	This command was introduced in the Local Controller and Global Controller 5.x train

Syntax Description

help	Displays a list of valid subcommands.
quit | exit	Quit and exit the **pnimp** command. Return to the pnadmin command prompt.
status	Display the status of the current data import operation.
log {all | recent}	Show all or recent data import log entries.
data {*nfs-path*}	Show how much data exists in the specified NFS path.
config	Displays the number of devices, reports, and rules in the migration data set. This command should be used as a point of comparison after the configuration is imported into the target appliance. Compare with the output of the **pnexp config** command.
stop	Stop the data import operations.
esti_time {nfs_path} {MM/DD/YY}	Estimates how much time is required to import the event, report, statistics, and incident data found at the specified NFS path. The *MM/DD/YY* parameter restricts the estimate to data generated on or after that date. **Note** This command does not estimate the time required to import configuration data.
import {config | data} {*nfs_path*} [MM/DD/YY	Import MARS configuration data ({config}), or events/reports/statistics/incident data ({data}) from the specified NFS path ({nfs_path}). The last argument ([MM/DD/YY]) is required for importing events/reports/statistics/incident data, meaning only importing data received or computed on or after that date. For importing config data, the latest MARS configuration data found under *nfs_path* is used. The *nfs_path* value identifies the exported archive folder on the NFS server; this path was dispayed when you ran the **pnexp export** command. **Note** You must first import the corresponding configuration data before attempting to import the event, report, statistics, incident data for reporting devices.

Usage Guidelines

Use the **pnimp** command to import configuration and event data generated from a MARS Appliance running 4.x into a MARS Appliance running 5.x software. The import operation does not affect event processing; in other words, the received events are processed upon arrival. However, it does affect the web interface and the query and report features may experience long delays and missing event or session data.

Tip To avoid IP address conflicts, reconfigure the MARS Appliance running 4.x before you import its configuration data into a new appliance.

Note When you import configuration data, it overwrites the configuration running on the MARS Appliance and reboots the appliance. After rebooting, the MARS Appliance assumes the IP address, hostname, and username/password of the appliance from which the configuration archive was exported.

The configuration import runs in the foreground displaying its status and errors immediately, where as event data export runs in the background. Use the **log {all | recent}** command to view the running status log for event data import.

Recent data is imported first. If an NFS-related problem results in a file not being imported properly, the **pnimp import** program halts and logs an error to the `/log/migrationrestore.log` file.

The next time the import operation is started, you are prompted whether to retry the last failed file. If no, the import operation continues with the next file. If another problem occurs, for example, a file corruption, that prevents a file from being imported, **pnimp import** generates a log similar to "file es_334_...gz is imported with error!" and continue with the next file.

When the import operation completes, the Local Controller begins to rebuild the RAW message indices. You can use the web interface although keyword query will remain slow until the indices are rebuilt.

Examples

The following example specifies that the MARS Appliance should import the configuration data from the NFS archive found at 192.168.3.138/storage/mars_migration/:

```
[pnadmin]$ pnimp
pnimp> import config 192.168.3.138:/storage/mars_migration/LC-220_2007-09-04-11-25-10
09/04/07
The most recent configuration archive from 4.3.1 release or later found on the NFS server
was created at 2007-09-04-11-25-10. Because events received after the config archive was
created may not be imported correctly later on when you try to import event data, so if
possible, you should always use 'pnexp' to export a fresh copy of configuration from the
Gen-1 MARS box before trying this command.

Do you wish to continue (yes/no) : yes

WARNING: this operation will overwrite current MARS box's configurations (both system and
DB) and reboot the machine. After reboot, current MARS box will take over the IP address,
hostname and MARS username/password of the MARS box from which the config archive was
exported, please make sure there will be no IP address conflict.

Do you wish to continue (yes/no): yes
!!! Stopping CS-MARS processes …
Invoking binary config importing procedure …
Recreating the database schema.
Importing data into database …
Configuration data binary import done.
Configrestore succeeded!
!!! Updating system settings …
Broadcast message from root (pts/5) (Wed Jun 13 15:23:46 2007):

The system is going down for reboot NOW!
[pnadmin]$
```

The following example specifies that the MARS Appliance should import the event data corresponding to the configuration data in the previous example:

```
pnadmin]$ pnimp

Enter 'help' for a list of valid commands, 'exit' or 'quit' to exit.
pnimp> import data 192.168.3.138:/storage/mars_migration/LC-220_2007-09-04-11-25-10
01/01/07
Last imported configuration archive is from
192.168.3.138:/storage/mars_migration/LC-220_2007-09-04-11-25-10/2007-09-04/CF/cf-4318-431
_2007-09-04-11-25-10.pna created at 2007-09-04-11-25-10. Because events received after the
config archive was created may not be imported correctly, you should import a latest copy
of configuration from the Gen-1 MARS box before trying this command if possible.

Do you wish to continue (yes/no): yes
Total number of days with data : 5
Total number of event archives to import: 89
Total number of report result archives to import: 1
Total number of statistics archives to import: 4
Total number of incident archives to import: 3
Estimated time to import all events: 2 hours 1 minutes

Do you wish to continue (yes/no): yes
!!! Importing data in background now, enter 'status' or 'log' to view data importing
status and/or logs.

pnimp>
```

Related Commands

Command	Description
pnexp	Export configuration and event data from a MARS Appliance running version 4.x (4.3.1 or later).

pnlog

To set the logging level or to view log information at the console, use the **pnlog** command. This command specifies the logging level of the MARS services, as well as the CheckPoint CPMI and LEA logs received by the MARS Appliance.

Syntax Description

none The default behavior *of this command* displays the command's usage guidelines.

pnlog show {**gui** | **backend** | **cpdebug**}

The **pnlog show** command provides running output of a particular logfile at the console. You can view one of three logfiles: the GUI logs, the backend logs (shows logs for the processes that the **pnstatus** command reports on), and CheckPoint debug logs. Press Ctrl+C to stop the output of this command.

When using **cpdebug**, you must set the **pnlog setlevel cpdebug** value to 3 or 9, as the default value of 0 turns off all CPE debug messages.

pnlog mailto {[*smtp_server*] [*sender*] [*recipient*]}

The **pnlog mailto** command is an alternative to sending a Feedback e-mail with the log files attached. It sends an e-mail from *sender* to *recipient* using *smtp_server*. The e-mail contains debugging information. These logs contain the logs specified above.

pnlog setlevel {**trace** | **debug** | **info** | **warning** | **error** | **critical**}

The **pnlog setlevel** command specifies how verbose the logs generated by the MARS Appliance services are, with *trace* being the most verbose and *critical* being the least. The default level is *info*. Unless you are actively debugging an issue, Cisco recommends that you use the default value. The *trace* and *debug* options should be used only on the advice of Cisco TAC. Setting a level of *critical* shows only the critical events, while setting a level of *warning* shows all warning or higher events (in other words, it shows warning, error, and critical events). The CLI sets a global output level while the web interface allows you to change this setting for each service (use **pnstatus** to view the list of services). You can access this setting in the web interface by selecting **Admin > System Maintenance > Set Runtime Logging Levels**.

pnlog setlevel cpdebug { **0** | **3** | **9** }

The **pnlog setlevel cpdebug** command sets the output level of the CheckPoint discovery process. You must specify one of three levels: 0, 3, or 9, where 0 disables Check Point debug logging, 3 enables all OPSEC debug logs, and 9 enables all CPMI debug logs. This command is used together with **pnlog show cpdebug** command to study the raw output of CheckPoint Discovery (CPMI) and CheckPoint Log (LEA) sessions. Cisco recommends the use of *9* for debugging and *0* when not actively debugging.

Examples

To view the backend service logs at the console, enter:

```
pnlog show backend
```

To send e-mail to bob@exmple.com from admin@example.com using the 192.168.101.5 mail server, enter:

```
pnlog mailto 192.168.101.5 admin@example.com bobc@example.com
```

To set the log level of the MARS Appliance services to debug, enter.

```
pnlog setlevel debug
```

To set the log level of the CheckPoint discovery process to debug, enter:

```
pnlog setlevel cpdebug 9
```

pnreset

To restore the appliance to the factory default settings (except for the pnadmin account) or to reset a Local Controller to standalone mode, use the **pnreset** command:

pnreset {-h} | {-g} | {-o} | {-j} | {-s}

Syntax Description

none	Default. With no options **pnreset** restores the appliance to factory defaults and purges all configuration and event data (certificate and fingerprints stored to validate reporting devices, topology settings, archived logs, and the license key information).
-h	Displays usage information.
-g	Removes the Global Controller data from a Local Controller, leaving all Local Controller-specific data untouched.
-o	Resets the *tnsnames.ora* file to factory default. The *tnsnames.ora* file is required for the Oracle client to connect to the Oracle server.
-j	Resets the web server scheduler depending on Local Controller's running mode. A restart of web server is enforced.
-s	Resets a Local Controller to standalone mode. It removes the same data as the **-g** option, and in addition, removes the Global Controller connectivity data from the Local Controller and the default Global Controller zone information.

Command History

Release	Modification
4.1.0	This command was introduced with **-g**, **-h**, -**o**, and **-j** options.
4.2.2	The **-s** option was introduced.

Usage Guidelines

The pnreset Command Without Options

The **pnreset** command restores the appliance to factory settings by deleting system configuration and event data stored in the appliance database. This reset process can take between 30 and 60 minutes to complete, depending on the model of the appliance. The **pnreset** command does not reset the password that you have defined for the Administrator (pnadmin) account. To reset the password to factory defaults, you must re-image the appliance using the Recovery DVD.

The **pnreset** command does not re-image the MARS Appliance. You should reimage the appliance when receiving a new appliance not running the most current version of the software or when you need to restore the administrator password to the factory default. For more information on reimaging, refer to Recovery Management, page 6-32.

Before entering the **pnreset** command without an option, disconnect the appliance from the network by unplugging the Ethernet cables from the appliance. Disconnecting from the network ensures that the cursor will return from the command upon completion. You must run **pnreset** without an option using a *direct console* connection, not an ssh console or other network-based connection. This requirement does not apply to **pnreset** when used with one of the options. For more information on console connections, see Establishing a Console Connection, page 5-4.

Caution Before executing the **pnreset** command without an option, write down the license key of the appliance. The license key is cleared during the reset process. You must provide this license key during the initial configuration following a reset operation, and it is not restored as part of archived data. This caution does not apply to **pnreset** when used with one of the options.

The -g Option

The **-g** option should be used only when a Global Controller recovery is required. The **-g** 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 Global Controller information from the Local Controller, use the ***-s*** option.

The **pnreset -g** command clears the global inspection rules and global user accounts from the Local Controller, which prepares the Local Controller to be managed by the reimaged Global Controller. 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.

The -o Option

Resets the *tnsnames.ora* file to factory defaults. The *tnsnames.ora* file is required for the Oracle client to connect to Oracle server. If MARS does not pull logs from the Oracle client, this option should never be used. If the *tnsnames.ora* file contains invalid data, MARS may be unable to connect to its internal Oracle database. This option should only be used when errors indicated that MARS has failed to setup an external Oracle server, errors are reported during that setup, and the **pnstatus** command fails to execute due to these connectivity issues.

Caution Do not use the **-o** option to troubleshoot all Oracle client issues. Using this command clears all Oracle client settings from the MARS Appliance, requiring that you re-enter all Oracle client setting using the web interface. Use this option only on direction from the Cisco TAC.

The -j Option

Resets the web server scheduler depending on the Local Controller's running mode. A restart of web server is enforced.

The -s Option

The **-s** option (4.2.2 and more recent) resets a Local Controller to Standalone mode from Monitor mode when the Global Controller cannot completely uncouple from (that is, delete) a Local Controller because of an unreliable network connection. It removes the same data as the **-g** option, removes the Global Controller connectivity data from the Local Controller, and removes the default Global Controller zone information. Use this option in the following cases:

- To reset a Local Controller when a Global Controller that was not running in archive mode crashes. If you plan to restore the Global Controller from an archive, use the **-g** option.
- If the Global Controller is not available or is unable to connect to the Local Controller, preventing you from successfully deleting the Local Controller entry from the Global Controller.
- If a Local Controller delete operation from the Global Controller fails.

Note If the Global Controller is operating properly and there is Global Controller-to-Local Controller connectivity, we recommend deleting the Local Controller entry from the Global Controller.

Examples

To restore the MARS Appliance to the factory defaults, enter:

```
pnreset
```

To prepare for a Global Controller reset or recovery, enter the following command on each Local Controller monitored by the Global Controller:

```
pnreset -g
```

To remove the Global Controller communication information and reset a Local Controller to standalone mode, enter the following command on the target Local Controller:

```
pnreset -s
```

Note You must also delete the Local Controller entry on the Global Controller.

Related Commands

Command	Description
pnstatus	Displays the status of each module running as part of the MARS application.
pnupgrade	Upgrades the software running on the MARS Appliance.

pnrestore

The **pnrestore** command restores data that has been archived using a network attached storage (NAS) device. You can specify the archival settings from the GUI using **Admin > System Maintenance > Data Archiving (see** Configure the Data Archive Setting for the MARS Appliance, page 6-30**)**. For more information on the archive file structure and how the archive works, see Configuring and Performing Appliance Data Backups, page 6-19. For more guidance on restoring, see Guidelines for Restoring, page 6-40.

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 the **pnrestore** command, you can restore three types of data:

- **MARS OS—**Restores the operating system (OS), including any upgrades that applied before the most recent archive was performed.

Note 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 re-image the MARS Appliance to version 4.1.4, not older or newer, before using the **pnrestore** command to recover the system configuration and events.

- **System configuration data—**Restores system configuration data, such as network settings, reporting devices, custom inspection rules, event types, reports, administrative accounts, archival settings, cases, and any other data that you have entered. It also, as of 4.2.1, includes the specific incident and event data associated with cases. It does not restore all dynamic data, just that data associated with cases.
- **Dynamic data—**Restores real event data that came from reporting devices, including incidents generated from events.

Note Prior to 4.2.1, performing a restore of just the configuration data resulted in incomplete data required to reconstruct existing cases: all open cases reference incidents and sessions. If this dynamic data is not restored, the cases could reference invalid incident and session IDs. To restore cases for releases prior to 4.2.1, you perform a full restore (mode 2).

To restore archived appliance data, use the **pnrestore** command:

`pnrestore -m 1 -p` *NFSSeverIP***:/***archive_path* **`-t`** *start_time*

—or—

`pnrestore -m 2 -p` *NFSSeverIP***:/***archive_path* **`-t`** *start_time*

—or—

`pnrestore -m 3 -r 1 -p` *NFSSeverIP***:/***archive_path* **`-t`** *start_time* **[-e** *end_time* **-s** *NFSSeverIP***:/***stagingAreaPath***]**

—or—

pnrestore -m 4-r 1 -p *NFSSeverIP*:/*archive_path* **-t** *start_time* [**-e** *end_time* **-s** *NFSSeverIP*:/*stagingAreaPath*]

—or—

pnrestore -m 5

Command History

Release	Modification
4.1.1	Mode 5 appears (*-m 5* option).
5.2.4	End time (*-e*), stage path area (*-s*), and *-r 1* options appear.

Syntax Description

noneThe default behavior of this command displays the command's usage guidelines.

*-m*Restoring mode. Three modes are available: 1 (default), 2, or 5. The mode determines what type of data is restored and from where the data is restored. Table A-2 identifies what data is restored for each option.

Note Mode 5 restores from a backup in the local database; you cannot use it to restore from a NFS archive. As such, you 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.

*-h*Displays the detailed command's usage guidelines.

*-t*Restores the data dated from this time through the most current archive date. Use *mm*/*dd*/*yy*:*hh* format. This option is required when you select mode r 2.

-e(5.2.4 and later) Used in conjunction with -t and -s, this parameter allows you to specify the end time (endTime) of the data restore range. Used to restore a past range of data.

-s(5.2.4 and later) Used in conjunction with -t and -s, this parameter allows you to specify the path (stagePath) on the NFS server to which to copy the range of data. This option is used to create a staging area from which you can restore a past range of data.

*-p*Name of the directory where the archived data is stored. You must identify the NFS server by IP address, separated by a :/ and then the pathname `NFSSeverIP:/archive_path`.

Where *NFSSeverIP* 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**. For more information on these settings, see Configure the Data Archive Setting for the MARS Appliance, page 6-30.

-r 1(5.2.4 and later) Used in conjunction with modes 3 and 4 only. Skips restoring the OS binary; instead only the configuration and dynamic data is restored. Because the version used to write out the archive for a particular time slice may predate the version most recently stored on the NFS server, these modes prevent MARS from overwriting the OS installed in the appliance to read the specified time slice's data.

Table A-2 pnrestore Mode Description

Restore Mode	Restore OS?	Restore System Configuration?	Restore Dynamic Data?
1 (default)	Yes	Yes	Partial[1]
2	Yes	Yes	Yes
3 -r 1	No	Yes	No
4 -r 1	No	Yes	Yes
5	No	Yes[2]	No

1. The incident and event data associated with cases is restored; however, other dynamic data is not.
2. Mode 5 restores data from a local configuration file on the MARS Appliance, not an NFS server.

Examples

You can use the restore feature to complete different restoring tasks, such as:

- Perform a partial restore on the same MARS Appliance using the local backup of the configuration data; it essentially restores the previous days' configuration backup. Use the **pnrestore** command, mode 5. For example, in the CLI menu of the appliance, enter:

  ```
  pnrestore -m 5
  ```

- Perform a partial restore on the same MARS Appliance using the archived data (including the OS and all data), but restoring only the event data generated since January 2, 2006 through the current date. Use the **pnrestore** command, mode 2. For example, in the CLI menu of the appliance, enter:

  ```
  pnrestore -m 2 -p 192.168.1.1:/archive/CS_MARS1 -t 01/02/06:0
  ```

- Archive and restore data to the same MARS Appliance or a different MARS Appliance of the same model. From the appliance where you want to archive the data, use the GUI to configure archiving. From the appliance to which you want to copy the archived data, use the **pnrestore** command.

  For example, if you only want to copy the OS and the system configuration data, you should use mode 1 of the restore command. For example in the CLI menu of the new appliance, enter:

  ```
  pnrestore -m 1 -p NFSSeverIPOfOldBox:/archive/CS_MARS1
  ```

Caution When restoring Local Controller data, problems can arise if you attempt to restore dynamic data from a bigger appliance to a smaller appliance. In such cases, use mode 1.

- Create a staging area that contains a range of data and determine the correct version of MARS to use when restoring the selected data. Depending on the generation of hardware that generated the archive, pnrestore copies the data range to a target directory. Upon completion, pnrestore displays the version of MARS to use to stage the ranged restore as well as the correct restore parameter and NFS directory to use.

Note Upon completion of a staged restore, use the web interface to change the hostname, IP address, and license settings of the MARS Appliance to the appropriate values.

For example, if you want to stage data between 10/01/06 and 11/01/06 to the corresponding directory under the *stageAreaPath* directory, enter:

```
pnrestore -t 10/01/06:00 -e 11/01/06:00 -p nfsIp:/archive -s nfsIp:/stageAreaPath
```

- Restore only the configuration and runtime data from October 1, 2006 at midnight to November 1 2006 at midnight, with the archive at 10.1.1.1 and the corresponding directory under the *stageAreaPath* directory at 10.1.10.15.

```
pnrestore –m 4 –r 1 -t 10/01/06:00 -e 11/01/06:00 -p 10.1.1.1:/archive -s
10.1.10.15:/stagingArea
```

pnstart

To manually start the MARS application running on the appliance from the serial console, use the **pnstart** command.

pnstart

Syntax Description

This command has no arguments or keywords.

Examples

The following command starts the MARS application running on the appliance:

```
pnstart
```

pnstatus

To show the status of each module running as part of the MARS application from the serial console, use the **pnstatus** command.

pnstatus

Note For a description of the processes and services, see List of Backend Services and Processes, page B-11.

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

Syntax Description

This command has no arguments or keywords.

Examples

The following command shows the status of each module of the MARS application running on the appliance:

```
[pnadmin]$ pnstatus
Module  State   Uptime
DbIncidentLoaderSrvRUNNING01:12:18
KeywordQuerySrvRUNNING01:12:18
autoupdateRUNNING01:12:18
csdam   RUNNING 01:12:18
csiosipsRUNNING01:12:18
csips   RUNNING 01:12:18
cswin   RUNNING 01:12:18
device_monitorRUNNING01:12:18
discoverRUNNING01:12:18
graphgenRUNNING01:12:18
pnarchiverRUNNING01:12:18
pndbpurgerRUNNING01:12:18
pnesloaderRUNNING01:12:18
pnmac   RUNNING 01:12:18
pnparserRUNNING01:12:19
process_event_srvRUNNING01:12:19
process_inlinerep_srvRUNNING01:12:19
process_postfire_srvRUNNING01:12:19
process_query_srvRUNNING01:12:19
superV  RUNNING 01:12:20
```

pnstop

To stop the MARS application running on the appliance from the serial console, use the **pnstop** command.

pnstop

Syntax Description

This command has no arguments or keywords.

Examples

The following command stops the MARS application running on the appliance:

```
pnstop
```

pnupgrade

To upgrade the software running on the MARS Appliance, use the **pnupgrade** command. This command supports upgrade from an Internal Upgrade Server and from a CD-ROM. See Checklist for Upgrading the Appliance Software, page 6-6, for details on obtaining upgrade images and preparing the Internal Upgrade Server. The **pnupgrade** command supports the following syntaxes:

pnupgrade cdrom://*path***/pn-***version***.pkg**

pnupgrade https://*path***/pn-***version***.pkg** [*user*] [*password*]

pnupgrade http://*path***/pn-***version***.pkg** [*user*] [*password*]

pnupgrade ftp://*path***/pn-***version***.pkg** [*user*] [*password*]

pnupgrade [*proxyServerIP*:*proxyServerPort proxyUser*:*proxyPassword*]
https://*path***/pn-***version***.pkg [user] [password]**

Note When using the HTTPS syntax, if the certificate of the upgrade server changes between upgrades, you are prompted by pnupgrade to accept the new certificate before the upgrade continues.

As of 4.1.3, the **pnupgrade log** command is also supported. This command provides a log of each step that was performed during the most recent upgrade. This log is useful in determining which step fails or hangs during a failed upgrade.

pnupgrade log

Syntax Description

proxyServerIP(Optional) Identifies the IP address of the proxy server that resides between your appliance and the Internal Upgrade Server. This option is only valid with the `https` transport. If you specify a proxy server, you must specify a corresponding port and a proxy server username/password pair.

*proxyServerPort*Identifies the port on which the proxy server listens for connection requests.

*proxyUser*Identifies the username that the appliance uses to connect to and authenticate to the proxy server.

*proxyPassword*Identifies the password that corresponds to the *proxyUser* account.

*path*Identifies the path required to access the package file using the selected access upgrade method. For protocols, this is often the URL and path.

*version*Displays the version number of the upgrade package, for example, 3.3.4.

*user*Identifies the username that the appliance uses to connect to and authenticate to the Internal Upgrade Server.

*password*Identifies the passwords that corresponds to the *user* account.

Examples

pnupgrade cdrom://342files/pn-342.pkg

pnupgrade https://www.example.com/upgrades/pn-342.pkg csAdmin B12e25s

pnupgrade http://www.example.com/upgrades/pn-342.pkg csAdmin 13a12Co13

pnupgrade ftp://www.example.com/upgrades/pn-342.pkg csAdmin 13c14u2020

pnupgrade 192.168.1.1:2642 psAdmin:12o22E13 https://www.example.com/upgrades/pn-342.pkg csAdmin M15m13Y

pnupgrade log

```
-------------------------------------
   4.1.3 2070   -->  4.1.3 2072
-------------------------------------
1 Preparing upgrade start
  1.1 Load the step table start
  1.1 Load the step table end
  1.2 Stop pnmonitor start
  1.2 Stop pnmonitor end
  1.3 Stop jboss start
  1.3 Stop jboss end
  1.4 Stop other applications start
  1.4 Stop other applications end
1 Preparing upgrade end
2 Upgrade OS start
  2.1 Patch OS start
  2.1 Patch OS end
2 Upgrade OS end
4 Upgrade MARS applications start
  4.1 Untar MARS executable binary start
  4.2 Untar MARS executable binary end
  4.3 Modify janus.conf start
  4.3 Modify janus.conf end
```

raidstatus (5.x)

To view the status of the RAID array and of the individual hard drives, use the **raidstatus** command.

raidstatus

Syntax Description

This command has no arguments or keywords.

Command History

Release	Modification
5.2.4	This command was introduced in the 5.X release train.
5.3.2	Support for the MARS 55 was added.

Usage Guidelines

This command description section is valid for the MARS Appliance models 55, 110R, 110, 210, GC2 and GC2R.

The **raidstatus** command is used with the **hotswap** command to replace component hard drives of the MARS Appliance Raid array.

For information on RAID hotswapping procedures and hard drive alerts, see the chapter, "System Maintenance" in the *User Guide for Cisco Security MARS Local Controller* at the following URL:

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/5.3/user/guide/local_controller/maintain.html

Examples

The following example displays a MARS 55 with a failed hard drive:

```
[pnadmin]$ raidstatus
RAID Controller Information:
-----------------------------------------------------
Product Name    : Intel Embedded Server RAID Technology
Driver Version  : 05.08y
Controller Type : SATA

Adapter  Raid Type  Status         Stripe    Size
-----------------------------------------------------
 a0      Raid 1     Degraded       64 KB     476772 MB

Port Status       Size        Model            Serial #        Write Cache
-------------------------------------------------------------------------
0    Online       476772 MB   HDS725050KLA360  KRVN0AZBH5R3LJ  Enabled
1    Failed       476772 MB   HDS725050KLA360  KRVN0AZBH5R8RJ  Enabled
```

In the following example, the MARS 210 RAID array is fully operational and redundant, that is, adapter a0 Raid-10 status is optimal, and all of the hard drives are online.

```
[pnadmin]$ raidstatus
Adapter Information:
-----------------------------------------------------
Product Name     : Intel(R) RAID Controller SROMBSAS18E
Firmware Version :  1.03.00-0211
BIOS Version     : MT30

Adapter RaidType        Status  Stripe  Size          Cache
```

```
-------------------------------------------------------------
a0      Raid-10         Optimal 64kB    2097151MB     Enabled

PD     Status  Size & Block                          Model                    Serial#
-----------------------------------------------------------------------------------------
p0     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          CQD017CET
p1     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02EMY
p2     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02ELS
p3     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02D0A
p4     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD01T1P
p5     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02BZ7
```

In the following example, the MARS 210 RAID array is shown degraded because hard drive 3 (p3) has failed. The RAID array is functional, but not fully redundant because the p2+p3 RAID 1 pair is compromised.

```
[pnadmin]$ raidstatus
Adapter Information: ------------------------------------------------
Product Name     : Intel(R) RAID Controller SROMBSAS18E
Firmware Version : 1.03.00-0211
BIOS Version     : MT30
Adapter RaidType        Status          Stripe  Size            Cache
-------------------------------------------------------------------------------
a0      Raid-10         Optimal         64kB    2097151MB       Enabled

PD     Status  Size & Block                          Model                    Serial#
-----------------------------------------------------------------------------------------
p0     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          CQD017CET
p1     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02EMY
p2     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02ELS
p3     Failed  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02D0A
p4     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD01T1P
p5     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02BZ7
```

In the following example, hard drive 3 has been replaced with the **hotswap** command, and is being rebuilt into the the MARS 210 Raid Array. The Array remains degraded until p3 has Online status. The progress message at the bottom shows percentage complete and time elapsed in the rebuild process.

```
[pnadmin]$ raidstatus
Adapter Information: C3QD02C0K
-------------------------------------------------------
Product Name     : Intel(R) RAID Controller SROMBSAS18E
Firmware Version :  1.03.00-0211
BIOS Version     : MT30

Adapter RaidType        Status  Stripe  Size          Cache
-------------------------------------------------------------
a0      Raid-10         Degraded 64kB    2097151MB     Enabled

PD     Status  Size & Block                          Model                    Serial#
-----------------------------------------------------------------------------------------
p0     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          CQD017CET
p1     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02EMY
p2     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02ELS
p3     Rebuild 715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02C0K
p4     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD01T1P
p5     Online  715404MB [0x575466f0 Sectors]   ATA    ST3750640AS   E          C3QD02BZ7

Rebuild Progress on Device at Enclosure 20, Slot 2 Completed 71% in 279 Minutes.
```

Table A-3 describes the output fields of the **raidstatus** command.

Table A-3 raidstatus CLI command for MARS 55, 110R, 110, 210, GC2R, and GC2

Output Field	Description
RAID Controller Information Fields	
Product Name	RAID controller manufacturer and serial number
Firmware Version : 1.02.00-0119	Indicates version of the RAID controller firmware
BIOS Version : MT25	Indicates the RAID BIOS version. This is different from the system BIOS version.
RAID Array Information Fields (The RAID 10 Virtual Drive Information)	
Adapter	Identifier for the physical RAID controller.
RaidType	RAID Level of Array.
Status	The current state of the RAID virtual drive. • Optimal—All component HDDs are operating as configured. • Degraded—At least one of the component HDDs has failed or is offline. Troubleshooting is advised to prevent possible data loss. • Offline—The array is not available or is unusable.
Stripe	The data stripe is always 64 KB.
Size	The available storage in megabytes of the RAID array.
Cache (not displayed for the MARS 55)	The MARS RAID cache is always enabled.
Individual Hard Drive Information Fields	
PD (Port for MARS 55)	p0–p5. The physical hard drive numbers. 0 or 1 for the MARS 55

Table A-3 raidstatus CLI command for MARS 55, 110R, 110, 210, GC2R, and GC2 (continued)

Output Field	Description
Status **Note** Only **Online**, **Failed**, **Rebuild,** and **Undefined** are supported on the MARS 55.	The current state of the physical HDD. • **Online**—The HDD is functioning normally within the RAID 10 array. • **Rebuild**—The HDD is being reimaged from its RAID 1 partner to restore full redundancy to a the virtual disk. The RAID 10 array efficiency is not yet optimal. • **Failed**—The HDD originally was Online, but now has an unrecoverable error. An email alert is sent to the administrator. • **Offline**—The HDD was removed by executing a **hotswap remove** command, but the HDD was not physically removed from the slot**.** An email alert is sent to the administrator. • **Unconfigured Good**—The HDD is usable, but the RAID information is out of sync with the RAID 1 partner. An email alert is sent to the administrator. • **Unconfigured Bad**— The firmware detected a media error on the hard drive. An online HDD was probably removed or inserted without executing a **hotswap** sequence and the HDD now has a media error. An alert is sent to the administrator. • **Undefined**—(MARS 55 only) A new HDD has been added but is not RAID 1 formatted, "Undefined" may appear briefly before "Rebuild." • **N/A**—There is no HDD in the slot. An email alert is sent to the administrator.
Size & Block (not displayed for MARS 55)	Size of the usable storage on the HDD
Model	The model number of the physical HDD
Serial#	The serial number of the physical HDD. The string, "This Drive is Foreign" is appended to the serial number when an HDD formatted with metadata from a different RAID controller is introduced. The message is removed when the HDD is assimilated into the array.
Write Cache (MARS 55 only)	RAID 1 Write Cache is always enabled.
Progress Messages	

Table A-3 raidstatus CLI command for MARS 55, 110R, 110, 210, GC2R, and GC2 (continued)

Output Field	Description
`Rebuild Progress on Device at Enclosure 0, Slot 1 Completed 8%`	(MARS 55) Indicates the slot number and percentage complete of the physical drive being rebuilt.
`Rebuild Progress on Device at Enclosure 20, Slot 2 Completed 71% in 279 Minutes.`	Indicates the status, elapsed rebuilding time, and slot number of each physical drive being rebuilt.

Related Commands

Command	Description
hotswap	Specifies that a designated hard drive is to be removed or added to a RAID array.

reboot

To reboot the MARS Appliance from the serial console, use the **reboot** command.

reboot

Caution The reboot is immediate and you are not prompted to confirm.

Syntax Description

This command has no arguments or keywords.

Examples

The following command reboots the appliance:

```
reboot
```

route

The **route** command manipulates the MARS Appliance's IP routing tables. Its primary use is to set up static routes to specific hosts or networks via an interface after it has been configured with the **ifconfig** command.

When the add or del options are used, the **route** command modifies the routing tables. Without these options, the **route** command displays the current contents of the routing tables.

To list the kernel routing tables, enter:

route [**-nNve**] [**-FC**]

To add a route to the routing table, enter:

route [**-v**] [**-FC**] **add** [**-net** | **-host**] *target* [*netmask*] [*gateway*] [**metric** *N*] [**mss** *M*] [**window** *W*] [**irtt** *I*] [**reject**] [**mod**] [**dyn**] [**reinstate**] [[**dev**] *inf_local*]

To delete a route from the routing table, enter:

route [**-v**] [**-FC**] **del** [**-net** | **-host**] *target* [*netmask*] [*gateway*] [**metric** *N*] [[**dev**] *inf_local*]

To display detailed usage syntax for the command, enter:

route -h

To display version/author information and exit, enter:

route -V

Syntax Description

noneThe default behavior *of this command* displays the command's usage guidelines.

addAdd a route to the table.

delDelete the specified route from the table.

-netIdentifies the route as a network route.

-hostIdentifies the route a host route.

targetIP address of the host or network for which you are defining a route.

netmaskNetwork mask that corresponds to the *ip_addr* value.

gatewayIP address of the gateway for this route.

mms *M*Set the TCP Maximum Segment Size (MSS) for connections over this route to M bytes. The default is the device MTU minus headers, or a lower MTU when path mtu discovery occurred.

window WSet the TCP window size for connections over this route to *W* bytes.

irtt I Set the initial round trip time (irtt) for TCP connections over this route to *I* milliseconds (1-12000). If omitted, the default value is 300ms.

rejectInstall a blocking route, which forces a route lookup to fail. Use this feature, for example, to mask out networks before using the default route. Do not use for firewalling.

mod, dynReinstate install a dynamic or modified route. These flags are for diagnostic purposes, and are generally only set by routing daemons.

-*h*Displays the detailed command's usage guidelines.

-vDisplay verbose information.

-nDisplay numeric values for addresses; don't resolve hostnames.

-eDisplay extended information.

-FDisplay Forwarding Information Base (FIB), which is the default.

-CDisplay routing cache instead of FIB.

script

Use the restricted script command mode to execute provided script:

script [-b] ***program***

Syntax Description

*program*Identifies the name of the script to run.

Command History

Release	Modification
4.3.1	This command was introduced in the 4.3.1 release.
5.3.1	This command was introduced in the 5.3.1 release.

Usage Guidelines

The following scripts are available from the restricted script command mode:

- **get_mars_summary_info.sh**— Gather high level statistics about the configuration and topology for the MARS Appliance.

Examples

The following example gathers high level statistics about the 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 Sep 14 05:50:10 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 Sep 14 05:50:10 PDT 2007
[pnadmin]$
```

show healthinfo

To display the operational status of key components in the appliance use the **show healthinfo** command.

show healthinfo

Syntax Description

There are no arguments or keywords for this command.

Command History

Release	Modification
5.2.4	This command was introduced in the 5.X release train.

Usage Guidelines

The **show healthinfo** command displays the operational status of critical components, such as fans, CPUs, hard drives, Ethernet interfaces, power supplies, backup battery units, memory usage, and the operating system.

Power Supply

In the command output for Power Supply, PS1 is the lower power supply, PS2 is the upper power supply. In normal operation, PS1 supplies most of the power requirements, and PS2 is the redundant power supply.

Ethernet Card Status

In the command output for Ethernet, eth0 is integrated NIC 1, eth1 is integrated NIC 2; eth2 and eth3 are not supported.

Raid Battery Backup Unit

In the command output for BBU, the relative state of charge is directly proportional to the battery backup time ($100\%_{charge} = 72_{hours}$).

For more information on RAID BBU and power supply procedures, see the chapter, "System Maintenance" in the *User Guide for Cisco Security MARS Local Controller* at the following URL:

http://www.cisco.com/en/US/products/ps6241/products_user_guide_chapter09186a008084f072.html

Examples

The following example dispays the health monitoring information on a MARS 110.

```
[pnadmin]$ show healthinfo
CPU Information:
Processor       Vendor ID       Model   CPU(MHZ)
 0 GenuineIntel Intel(R) Xeon(R) CPU            5130  @ 2.00GHz 1995.024
 1 GenuineIntel Intel(R) Xeon(R) CPU            5130  @ 2.00GHz 1995.024
 2 GenuineIntel Intel(R) Xeon(R) CPU            5130  @ 2.00GHz 1995.024
 3 GenuineIntel Intel(R) Xeon(R) CPU            5130  @ 2.00GHz 1995.024

Memory Information:
MemTotal: 4137832 kB    MemFree: 18812 kB

Fan ID  RPM             Status
----------------------------------
Fan 1   7052 RPM        ok
```

```
Fan 2   7611 RPM        ok
Fan 3   7095 RPM        ok
Fan 4   7568 RPM        ok
Fan 5   10416 RPM       ok
Fan 6   9610 RPM        ok

CPU     Temperature     Status
-------------------------------
CPU1 VRD Temp   0x00    ok
CPU2 VRD Temp   0x00    ok
CPU1 Vcc OOR    0x00    ok
CPU2 Vcc OOR    0x00    ok

Power Supply            Value   Status
---------------------------------------
PS1 AC Current  2.36 Amps       ok
PS2 AC Current  0.12 Amps       ok
PS1 +12V Current        21 Amps ok
PS2 +12V Current        0 Amps  ok
PS1 +12V Power  248 Watts       ok
PS2 +12V Power  0 Watts ok
PS1 Status      0x01    ok
PS2 Status      0x09    ok

Ethernet card status
eth0 is up
eth1 is up
eth2 is down
eth3 is down

Flash driver is Online

BBU information :
Relative state of charge : 93 %
Full charge capacity : 920 mAh
Remain capacity : 858 mAh

OS information :
Linux SJ-LC-17 2.6.9-42.0.2.ELsmp #1 SMP Thu Aug 17 18:00:32 EDT 2006 i686 i686 i386
GNU/Linux
```

Related Commands

Command	Description
ifconfig	Displays or modifies the IP address and network mask of the network interfaces.
show inventory	Displays identifying details of essential components in the appliance.

show inventory

To display an inventory and serial numbers of essential components in the MARS Appliance, use the **show inventory** command.

show inventory

Syntax Description

There are no arguments or keywords for this command.

Command History

Release	Modification
5.2.4	This command was introduced.

Usage Guidelines

The **show inventory** command displays the part identification string (PID) and serial numbers of the chassis, hard drives, RAID battery backup unit, and power supplies.

Examples

The following example displays the inventory of a MARS 110 Local Controller:

```
[pnadmin]$ show inventory
NAME: "Chassis",  DESCR: "CS-MARS-110 Local Controller"
PID: CS-MARS-110,       VID: V01,       SN: M1100000027

RAID Information:
NAME: "Hard Disk Drive", DESCR: "Barracuda ES - Serial ATA II - 3.0Gps - 500GB"
PID: CS-MARS-S500-HD,   VID:    ,       SN:  5QG02GFH

NAME: "Hard Disk Drive", DESCR: "Barracuda ES - Serial ATA II - 3.0Gps - 500GB"
PID: CS-MARS-S500-HD,   VID:    ,       SN:  5QG00KH4

NAME: "Hard Disk Drive", DESCR: "Barracuda ES - Serial ATA II - 3.0Gps - 500GB"
PID: CS-MARS-S500-HD,   VID:    ,       SN:  5QG02GCH

NAME: "Hard Disk Drive", DESCR: "Barracuda ES - Serial ATA II - 3.0Gps - 500GB"
PID: CS-MARS-S500-HD,   VID:    ,       SN:  5QG02GE4

NAME: "Hard Disk Drive", DESCR: "Barracuda ES - Serial ATA II - 3.0Gps - 500GB"
PID: CS-MARS-S500-HD,   VID:    ,       SN:  5QG02GHJ

NAME: "Hard Disk Drive", DESCR: "Barracuda ES - Serial ATA II - 3.0Gps - 500GB"
PID: CS-MARS-S500-HD,   VID:    ,       SN:  5QG02GGV

RAID Battery Backup Unit Information:
NAME: "Battery", DESCR: "MARS110/210/GC2 RAID Controller Back-Up Battery"
PID: CS-MARS-X10-BB,     VID:   ,       SN: 313

Power Supply Information:
NAME: "Power supply",  DESCR: "MARS110/210/GC2 Power Supply Module"
PID: CS-MARS-D750-PS,    VID:   ,        SN:  DLD0636022220

NAME: "Power supply",  DESCR: "MARS110/210/GC2 Power Supply Module"
PID: CS-MARS-D750-PS,    VID:   ,        SN:  DLD0621008449
```

Related Commands

Command	Description
show healthinfo	Displays operational status of appliance components.

shutdown

To shut down the appliance and turn off the power from the serial console, use the **shutdown** command.

shutdown

Caution The shutdown is immediate and you are not prompted to confirm.

To turn on the appliance after executing the **shutdown** command, you must have physical access to it. For more information, see Powering on the Appliance and Verifying Hardware Operation, page 4-8.

Syntax Description

This command has no arguments or keywords.

Examples

The following command shuts down the appliance:

```
shutdown
```

snmpwalk

The **snmpwalk** command loads an SNMP application that uses SNMP GETNEXT requests to query a network entity for a tree of information.

To use snmpwalk, enter:

snmpwalk [*options*...] <*hostname*> {<*community*>} [<*objectID*>]

Syntax Description

noneThe default behavior *of this command* displays the command's usage guidelines.

-hThe default behavior *of this command* displays the command's usage guidelines.

*hostname*Identifies the DNS name of the device against which the snmpwalk command will be run. Typically, this device is a router or switch. This device must have SNMP management access enabled and the MARS Appliance must be a valid management host.

*community*Identifies the community string for SNMP transactions.

*objectID*An object identifier (OID) may be given on the command line. This OID specifies which portion of the object identifier space to search using GETNEXT requests. If no OID argument is present, the **snmpwalk** command searches MIB-2.

ssh

To access the SSH client that resides on the appliance, use the **ssh** command.

ssh [*options*] **host** [*command*]

Syntax Description

noneThe default behavior *of this command* displays the command's usage guidelines.

-*h*Displays the detailed command's usage guidelines.

-l userLog in using this username.

-nRedirect input from /dev/null.

-F configConfig file (default: ~/.ssh/config).

-AEnable authentication agent forwarding.

-aDisable authentication agent forwarding (default).

-XEnable X11 connection forwarding.

-xDisable X11 connection forwarding (default).

-i fileIdentity for public key authentication (default: ~/.ssh/identity).

-tTty; allocate a tty even if command is given.

-TDo not allocate a tty.

-vVerbose; display verbose debugging messages. Multiple -v increases verbosity.

-VDisplay version number only.

-qQuiet; do not display any warning messages.

-fFork into background after authentication.

-e chaSet escape character; "none"' = disable (default: ~).

-c cipherSelect encryption algorithm.

-m macsSpecify MAC algorithms for protocol version 2.

-p portConnect to this port. Server must be on the same port.

-L listen-port:host:port

Forward local port to remote address

-R listen-port:host:port

Forward remote port to local address.

These cause ssh to listen for connections on a port, and forward them to the other side by connecting to host:port.

-D portEnable dynamic application-level port forwarding.

-CEnable compression.

-NDo not execute a shell or command.

-gAllow remote hosts to connect to forwarded ports.

-1Force protocol version 1.

-2Force protocol version 2.

-4Use IPv4 only.

-6 Use IPv6 only.

-o 'option' Process the option as if it was read from a configuration file.

-sInvoke command (mandatory) as SSH2 subsystem.

-b addrLocal IP address.

sslcert

Use the **sslcert** command to generate a new self-signed SSL certificate and reboot the JBoss Application Server.

To use this command, you will be prompted to provide the following information:

- The common name of the MARS Appliance
- The name of your organizational unit (OU)
- The name of your organization (O)
- The name of your City or Locality (L)
- The name of your State or Province (SP)
- The two-letter country code for the unit (C)

To generate a new self-signed certificate for use with this MARS Appliance, use the **sslcert** command:

```
sslcert
```

Syntax Description

*none*The default behavior *of this command* launches an interactive program that collects the information required to generate a certificate. You are prompted to verify that you want to generate a new self-signed certificate. Enter **YES** to begin the interview process that will collect the data required to generate the certificate. Enter **NO** to cancel without generating a new certificate.

Examples

The following command generates a new self-signed certificate:

```
[pnadmin]$ sslcert
Sslcert command will generate a new ssl certificate and restart jboss.
Please type YES if you want to proceed: YES
What is the common name of this device? (CN)
[Unknown]: hostname
What is the name of your organizational unit? (OU)
[Unknown]: test
What is the name of your organization? (O)
[Unknown]: cisco.com
What is the name of your City or Locality? (L)
[Unknown]: San Jose
What is the name of your State or Province? (SP)
[Unknown]: CA
What is the two-letter country code for this unit? (C)
[Unknown]: US
Certificate stored in file <server.cert>
Certificate was added to keystore
Restarting jboss ... OK
```

ssllist

Use the ssllist command to display the list of ssl certificates that exist in your keystore.

ssllist

Syntax Description

There are no arguments or keywords for this command.

Command History

Release	Modification
5.2.4	This command was introduced in the 5.2.4 release.

Examples

The following command displays the SSL certificates:

```
[pnadmin]$ ssllist

Keystore type: jks
Keystore provider: SUN

Your keystore contains 2 entries

global, Dec 29, 2006, trustedCertEntry,
Certificate fingerprint (MD5): 85:2A:05:46:4E:6B:AB:15:B4:EE:77:FE:3C:4A:EE:65
server, Dec 28, 2006, trustedCertEntry,
Certificate fingerprint (MD5): 6A:C8:50:8C:FA:65:BB:E2:08:F1:75:80:A4:69:47:90
```

syslogrelay setcollector

To set, change, or clear the IP address of a host to which the Local Controller forwards the syslog messages it receives, use the **syslogrelay setcollector** command.

syslogrelay {setcollector | unsetcollector} *ip_address*

Command History

Release	Modification
4.3.1	This command was introduced in the 4.X release train.
5.3.1	This command was introduced in the 5.X release train.

Syntax Description

setcollector	Indicates the provided IP address is the collector.
unsetcollector	Clears the provided IP address, and disables the syslog relay feature.
ip_address	Indicates one IP address. You cannot define more than one collector.

Usage Guidelines

The **syslogrelay setcollector** command allows you to specify the IP address of the syslog server to which syslog messages should be forwarded. This command must be used in conjunction with the syslogrelay src command, which designates the reporting devices for which syslog messages should be forwarded.

Examples

The following example specifies that the Local Controller should forward the syslog messages to 192.168.1.25, which is the designated address of the collector.

```
[pnadmin]$ syslogrelay setcollector 192.168.1.25
```

```
The following example changes the address of the collector defined in the previous
example.
[pnadmin]$ syslogrelay setcollector 192.168.1.26
syslogrelay setcollector 192.168.1.26
Changing collector ip from 192.168.1.25 to 192.168.1.26. Continue? [y/n]:
```

The following example clears the address of the collector defined in the previous example, effectively disabling the syslog relay feature until a new collector address is set.

```
[pnadmin]$ syslogrelay unsetcollector 192.168.1.26
```

Related Commands

Command	Description
syslogrelay src	Add to, exclude from, or clear the list of IP addresses for which the Local Controller forwards syslog messages to the collector.
syslogrelay list	Displays the list of IP addresses used by the syslogrelay. This list includes the collector, as well as reporting devices in the include and/or exclude lists.

syslogrelay src

To add to, remove from, or clear the lists of sources (reporting devices) for which the Local Controller forwards the syslog messages it receives to the collector, use the **syslogrelay src** command.

syslogrelay src {include | exclude} {ANY | *ip_address***}**

syslogrelay src reset

Command History

Release	Modification
4.3.1	This command was introduced in the 4.X release train.
5.3.1	This command was introduced in the 5.X release train.

Syntax Description

include	Indicates that syslog messages received by MARS from the listed IP addresses to be relayed to the configured collector.
exclude	Indicates that syslog messages received by MARS from the listed IP addresses should *not* be forwarded to the configured collector.
ANY	Adds all IP addresses to the selected source list.Used in conjunction with either the **include** or **exclude** parameter.
ip_address	Indicates between one and ten IP addresses in a comma separated list. Used in conjunction with the **include** and **exclude** parameters. You can only add up to ten addresses at one time; however, you can use the command repeatedly to add to the list.
reset	Clears the active syslog relay source configuration—both the include and exclude lists. If a syslog relay source is configured, the following prompt appears: `One or more device addresses are currently configured. Proceed further? [yes/no]:` Enter **yes** to clear the source configuration or **no** to cancel.

Usage Guidelines

The **syslogrelay src** command designates the set of reporting devices for which the Local Controller forwards the syslog messages it receives to the collector. You can exclude all addresses, defining the few exceptions for which the syslog messages should be forwarded; or you can enable all addresses, and define the exceptions that should not be forwarded.

The **ANY** token cannot be used simultaneously in both the **include** and **exclude** lists. If the value is set on one list, and you apply it to the other list, it is removed from the first.

The **syslogrelay src include ANY** command indicates that all syslog messages received by MARS be relayed to the configured collector, excepting those that originate from the addresses configured as exclusions. If exclusions are configured, the following prompt appears:

```
One or more device ip addresses are currently excluded. Proceed further? [y/n]:
```

Enter **y** to retain the current exclusions and forward the syslog messages of from all other reporting devices, or enter **n** to cancel.

The **syslogrelay src exclude ANY** command indicates that all syslog messages received by MARS should *not* be forwarded to the configured collector, excepting those that originate from addresses configured as inclusions. If inclusions are configured, the following prompt appears:

```
One or more device ip addresses are currently included. Proceed further? [y/n]:
```

Enter **y** to retain the current inclusions and prevent the forwarding of syslog messages from all other devices, or enter **n** to cancel.

Examples

The following example specifies that the Local Controller should forward the syslog messages it receives from any reporting device to the collector (as long as the source IP address of the message is not in the source exclude list).

```
[pnadmin]$ syslogrelay src include ANY
```

The following example specifies that the Local Controller should not forward the syslog messages it receives from 192.168.1.1 or 192.168.2.1 to the collector.

```
[pnadmin]$ syslogrelay src exclude 192.168.1.1, 192.168.2.1
```

The following example clears the source include and exclude lists of all values:.

```
[pnadmin]$ syslogrelay src reset
One or more device ip addresses are currently configured. Proceed further?[yes/no]: yes
```

Related Commands

Command	Description
syslogrelay setcollector	Set or clear the IP address that identifies the syslog collector to which the Local Controller forwards syslog messages. If the address is cleared, this feature is turned off.
syslogrelay list	List syslog relay configuration. Displays the list of IP addresses used by the syslogrelay. This list includes the collector, as well as reporting devices in the include and/or exclude lists.

syslogrelay list

To display the IP addresses of the reporting devices to which the Local Controller forwards the syslog messages as well as the IP address of the collector to which they are sent, use the **syslogrelay list** command.

syslogrelay list [all | collector | src]

There are no arguments or keywords for this command.

Command History

Release	Modification
4.3.1	This command was introduced in the 4.X release train.
5.3.1	This command was introduced in the 5.X release train.

Syntax Description

-h	Displays usage guidelines
all	(default) Displays the IP address of the collector and the union of those sources on the include list and exclude list.
collector	Displays the IP address of the collector, or destination, of the forwarded messages.
src	Displays the IP addresses of the sources on the include list and exclude list.

Usage Guidelines

Using the **syslogrelay list** command, you can verify the list of addresses in the include and exclude lists. If a reporting device device appears in the include list, the Local Controller forwards any syslog messages that it receives from that device to the syslog collector. The exclude list identifies the IP addresses for which the Local Controller does not forward the syslog messages. The collector identifies the IP address to which the specified syslog messages are forwarded. This address represents a syslog server or other collector as defined in *RFC 3164: The BSD syslog Protocol*.

If the collector address is not set, the syslogrelay feature is disabled.

Examples

The following example displays the t syslog relay configuration.

```
[pnadmin]$ syslogrelay list all
[Collector]
192.168.1.1

[Inclusions]
ANY

[Exclusions]
192.168.2.1
182.168.3.1
```

Related Commands

Command	Description
syslogrelay setcollector	Set or clear the IP address that identifies the syslog collector to which the Local Controller forwards syslog messages. If the address is cleared, this feature is turned off.
syslogrelay src	Add to, exclude from, or clear the list of IP addresses for which the Local Controller forwards syslog messages to the collector.

sysstatus

The **sysstatus** command is a system-defined alias for the Linux **top** command, which displays and updates information about the top CPU processes. It provides a real-time view of the processor activity. It lists the most CPU-intensive tasks on the system, and can provide an interactive interface for manipulating processes. It can sort the tasks by CPU usage, memory usage, and runtime.

To view the current CPU activities, enter:

sysstatus -hvbcisqS -d delay -p *pid* **-n** *iterations*

If you execute the command and you do not select the batch mode option, you are running in an interactive environment. In this environment, you can interact with the output as follows:

- Press **H** or **?** to get the list of interactive commands.
- Press the **space** key to refresh the data immediately.
- Press **Ctrl+L** to erase and redraw the screen.
- Press **K** to kill a specific process ID (pid).
- Press **Q** to quit viewing the real-time data and return to the command prompt.
- Press **Ctrl+C** to break the batch mode display.
- Press **I** to toggle ignoring idle and zombie processes.
- Press **N** or **#** to specify the number of processes to display on the screen. The value of zero (0) restores the default, which is the number of processes that fit on the screen.
- Press **S** to toggles the cumulative mode, the equivalent of -S, that includes a process's defunct children as part of the CPU times.
- Press **f** or **F** to add fields or remove fields from the display.
- Press **o** or **O** to change the order of the displayed fields.
- Press **L** to toggle the display of load average and uptime information.
- Press **M** to toggle the display of memory information.
- Press **T** to toggle the display of processes and CPU states information.
- Press **C** to toggle the display of command name or full command line.
- Press **N** to sort the tasks numerically by pid.
- Press **A** to sort the tasks by age (newest first).
- Press **P** to sort the tasks by CPU usage (default).
- Press **M** to sort the tasks by resident memory usage.
- Press **T** to sort the tasks by time/cumulative time.

Syntax Description

noneThe default behavior *of this command* displays the current CPU activities.

-hDisplays the detailed command’s usage guidelines.

-dSpecifies the delay between screen updates. You can change this delay using the -s interactive command.

-pMonitors only those processes with the given process id. This flag can be given up to twenty times. This option is not available interactively.

-qThis causes sysstatus to refresh without any delay.

-SSpecifies cumulative mode, where each process is listed with the CPU time it has spent. It also lists the CPU time of the dead children for each process.

-sTells sysstatus to run in secure mode. This option disables the potentially dangerous interactive commands.

-iStart sysstatus ignoring any idle or zombie processes.

-CDisplay total CPU states in addition to individual CPUs. This option only affects SMP systems.

-cDisplay the command line instead of the command name only. The default behavior has been changed as this seems to be more useful.

-nNumber of iterations. Update the display this number of times and then exit.

-bBatch mode. Useful for copying output from sysstatus to a file. In this mode, sysstatus does not accept command line input. It runs until it reaches the number of iterations specified by the n option or until killed. Output is plain text suitable for display on a dumb terminal.

tcpdump

Tcpdump prints out the headers of packets on a network interface that match the boolean expression. To analyze packet headers, enter:

tcpdump [**-adeflnNOpqRStuvxX**] [**-c** *count*] [**-i** *interface*] [**-s** *snaplen*] [**-T** *type*] [**-U** *user*] [*expression*]

Note For more information on this command and its use, please refer to a Linux manual or man page.

Syntax Description

noneThe default behavior *of this command* displays current CPU activities.

-hDisplays the detailed command's usage guidelines.

-i *interface*Identifies the interface to sniff.

-c *count*Exit after receiving *count* number of packets.

Ctrl+c Exit the tcpdump screen.

telnet

The **telnet** command is used to communicate with another host using the TELNET protocol. In this mode, it accepts and executes the commands listed below. If it is invoked with arguments, it performs an open command with those arguments.

telnet [**-8**] [**-E**] [**-L**] [**-S** *tos*] [**-a**] [**-c**] [**-d**] [**-e** *char*] [**-l** *user*] [**-n** *tracefile*] [**-b** *hostalias*] [**-r**] [*hostname* [*port*]]

Syntax Description

noneIf telnet is invoked without the host argument, it enters command mode, indicated by its prompt (telnet>).

-hDisplays the detailed command's usage guidelines.

-8Specifies an 8-bit data path, which forces telnet to attempt to negotiate the BINARY option on both input and output.

-EStops any character from being recognized as an escape character.

-LSpecifies an 8-bit data path on output. This causes the BINARY option to be negotiated on output.

-aAttempt automatic login. The name used is that of the current user.

-b *hostalias*Uses bind on the local socket to bind it to an aliased address (see ifconfig and the "alias" specifier) or to the address of another interface than the one naturally chosen by connect. This can be useful when connecting to services which use IP addresses for authentication and reconfiguration of the server is undesirable (or impossible).

-cDisables the reading of the user's .telnetrc file.

-dSets the initial value of the debug toggle to TRUE.

-e *escapechar*Sets the initial telnet escape character to escapechar. If escapechar is omitted, there will be no escape character.

-l *user*When a host connects to the remote system, if the remote system understands the ENVIRON option, the user will be sent to the remote system as the value for the variable USER. This option implies the -a option. This option may also be used with the open command.

-n *tracefile*Opens tracefile for recording trace information.

-rSpecifies a user interface similar to rlogin. In this mode, the escape character is set to the tilde (~) character, unless modified by the -e option.

*hostname*Indicates the official name, an alias, or the Internet address of a remote host.

*port*Indicates a port number (address of an application) used to connect on the remote host. If a number is not specified, the default telnet port is used.

time

To display the current time, enter:

timezone

To set the time to 11:15 p.m., enter:

time [*hh*:*mm*:*ss*]

Note Time changes on the appliance are immediate, which can affect active incident correlation. If you change the time by greater than one half hour, you should restart your appliance to ensure that all processes synchronize using the new time.

Syntax Description

*hh:mm:ss*Identifies the time in *hh*:*mm*:*ss* format, where *hh* is 01-24, *mm* is 00-59 and *ss* is 00-59.

Examples

To display the current time, enter:

timezone

To set the time to 11:15 p.m., enter:

time 23:15:00

timezone

To display the current timezone setting, enter:

timezone

To set a new timezone, enter:

timezone set

When configuring a Global Controller\Local Controller hierarchy, you should ensure that all the Local Controllers are set to the same timezone as the reporting devices that they are monitoring.

Note Time changes on the appliance are immediate, which can affect active incident correlation. If you change the time by greater than 30 minutes, you should restart your appliance to ensure that all processes synchronize using the new time.

Syntax Description

*set*Displays a menu system that allows you to select the appropriate timeszone based on continent/country/region or using the POSIX TZ format.

Examples

To display the current timezone setting, enter:

timezone

To set the timezone to CST, enter:

timezone set

traceroute

To display the network route that packets take to reach a specified host, enter:

traceroute [*hostname* | *ip_address*]

Traces the route that IP packets take from the MARS appliance to another host on a network by listing the intermediate gateways that the packet traverses to reach the host.

Traceroute displays the IP address and hostname (if possible) of the gateways along the route taken by the packets. Traceroute is used as a network debugging tool. If you are having network connectivity problems, traceroute will help you diagnose where the trouble might exist along the route.

Syntax Description

noneThe default behavior *of this command* displays the command's usage guidelines.

*hostname*Identifies the host by hostname for which you want to trace the route.

*ip_address*Identifies the host by IP address for which you want to trace the route.

unlock

Use the **unlock** command to restore access to the MARS Appliance GUI for all or specified user accounts after login failures.

unlock {**-a**} | {{**-l** | **-g** | **-b** } *login_name*}

Command History

Release	Modification
4.3.1/5.3.1	This command was introduced.

Syntax Description

-a	Unlocks all accounts on the MARS Appliance.
-l	Unlocks the local account for the specified login name.
-g	Unlocks the global account for the specified login name.
-b	Unlocks global and local accounts for the specified login name.
login_name	Specifies the login name of the account to be unlocked.

Usage Guidelines

For both Local or AAA authentication methods, GUI access is prevented (locked) for an account upon login failure, which occurs when a specified number of incorrect password entries are made for a single login name. The administrator GUI access can be locked like any other account.

The CLI access through the console or through SSH is never locked. The **unlock** CLI command can unlock GUI access for some or all accounts.

Unlocking is not replicated through Global Controller–Local Controller communications, it applies only to the local appliance. An account locked on a Global Controller does not replicate the locked status to global accounts on Local Controllers. A global account locked on two different appliances must be unlocked manually on each appliance.

For more information on account locking and login failure, see the section, "Information About Authenticating MARS User Accounts with External AAA Servers" at the following URL: http://www.cisco.com/en/US/products/ps6241/products_user_guide_chapter09186a00808bcdd1.htm

Examples

The following example unlocks GUI access for a local account with the login name bleistiftansatz:

```
[pnadmin]$ unlock -l bleistiftansatz
```

Related Commands

Command	Description
passwd	Changes the password of the system administrative account (pnadmin) associated with the appliance.

version

To display the version of MARS software that is running on the appliance, use the version command. The version number appears in the following format: *major.minor.patch* (*build no*.)

Syntax Description

This command has no arguments or keywords.

Examples

To display the current version, enter:

```
version
```

APPENDIX **B**

Troubleshooting

Revised: September 14, 2007, OL-14672-01

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

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.

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 1-9.

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 6-33.

Cannot Delete a Device from MARS

See Delete a Device, page 2-19.

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 2-19.

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 2-19.

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 2-19.

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.** As of 4.3.1 and 5.3.1 releases, 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 yourselff. 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 A-38.
- In the GUI, you can use the **Help > Feedback** option. For more information on using this option, see Submitting Feedback and Reporting Errors, page B-3

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

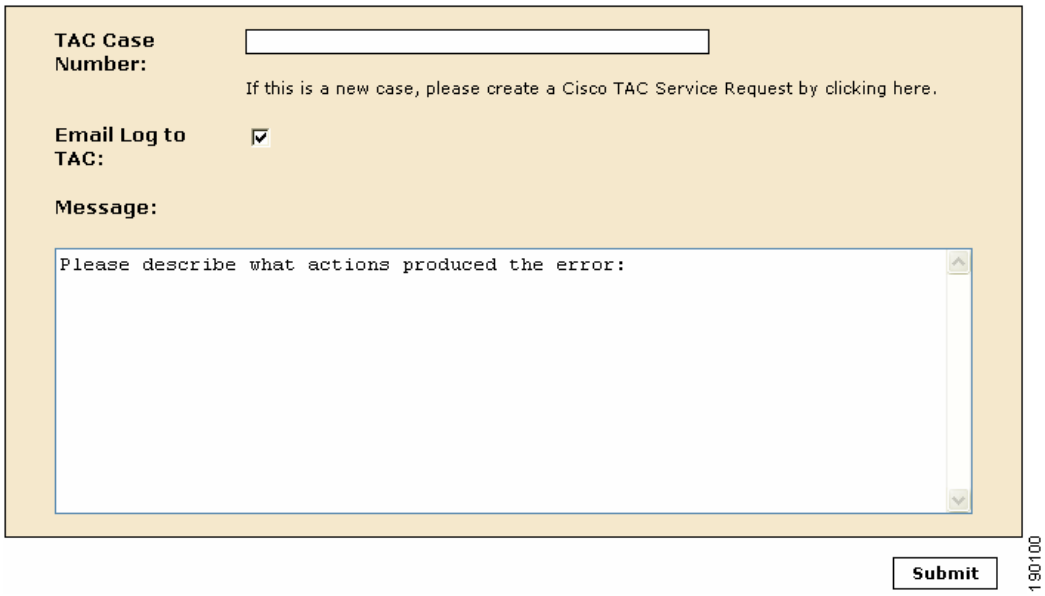
No passwords or network information is included in the error-logs.tar.gz file.

Submitting Feedback and Reporting Errors

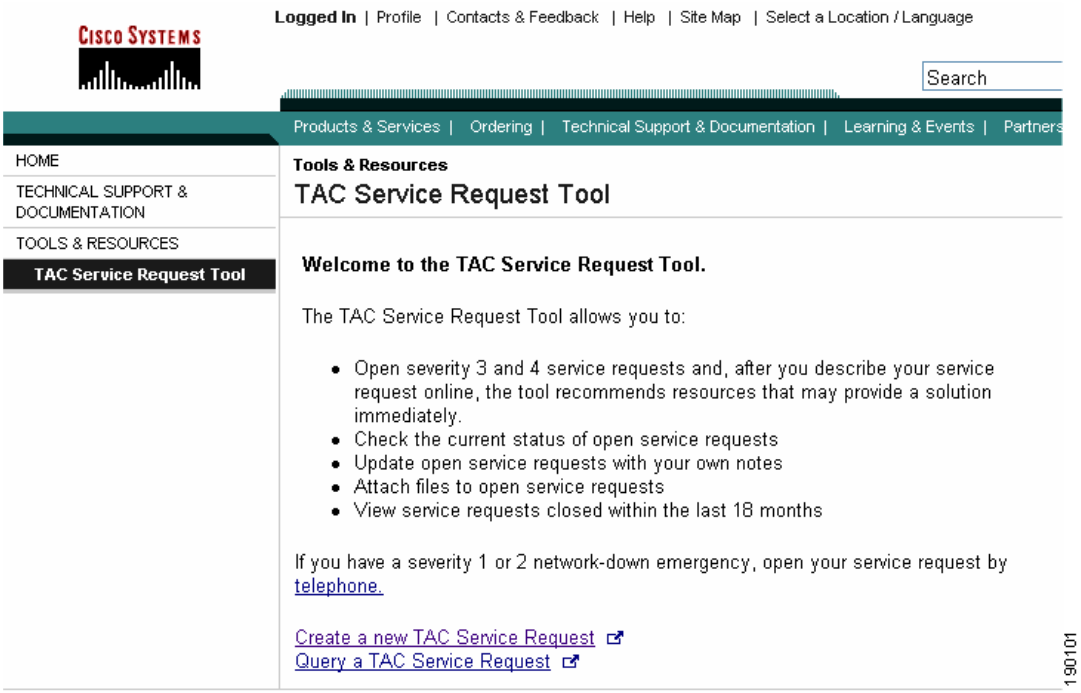
If you receive an error in the web interface and the system recovers, a pink page appears allowing you to report the error to Cisco.

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.



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.



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 Hardware Descriptions—MARS 25R, 25, 55, 110R, 110, 210, GC2R, and GC2, page 1-4

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 5-7, and Specify the IP Address and Default Gateway for the Eth1 Interface, page 5-8. 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 5-7.

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

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 2-1 of *User Guide for Cisco Security MARS Global Controller*.

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.

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 2-10
- **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 2-3Local Controller Status Messages on Zone Controller Page, page 2-5.

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.	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 B-8 **Possible causes**: 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. A high usage MARS Appliance may not have adequate bandwidth between Local Controller/ Global Controller to ensure that the system stays synchronized.
Data is not synchronizing and the Local Controller and Global Controller were disconnected.	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. Configuration and topology data does not take as long as report and incident data, and it should synchronize in a reasonable amount of time. **Note** Communication link speeds vary; a saturated link could slow synchronization greatly relative to a lab environment.

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.	Verify Activate was clicked. You must click **Activate** for Local Controller-based topological changes to be pushed to the Global Controller
No incidents appear in the Global Controller	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.
I deleted a Local Controller from the Global Controller when there were communication problems. How do I restore the Local Controller?	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. For more information, see pnreset, page A-40.
A replacement Global Controller appliance has been restored. How do I restore communications with the Local Controllers?	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 A-40. **Note** Use this option only when a Global Controller recovery is required.

Symptom	Possible Resolution
The topology diagram is missing a device or other information.	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. To manually re-synchronize the topology data, perform the following steps from the Global Controller web interface: 1. Click **Admin > Local Controller Management**. 2. Select the Local Controller that has the issues and click the **Topo Sync Start/Stop** button. 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 2-4. 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. **Note** Deleting and re-adding the Local Controller restarts this process and is not recommended
A topology change does not appear, the state is Active, and a reasonable amount of time has passed.	Initiate a full topology synchronization to re-push all topology. **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.

Symptom	Possible Resolution
Configuration data (users, report definitions, rules, and event types) does not replicate from a Global Controller to Local Controller	If the severs were disconnected, this symptom can result because it takes time to clear the backlog created during the downtime. 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 following your technical support escalation process.
None of the previous suggestions correct the error.	Use the **pnlog** command to collect log data and submit it to technical support to identify exceptions that may have the caused the error. See Collect Support Information, page B-2.

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 B-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 B-1 MARS Services and Processes Descriptions

Service/Process Name	Description
pnparser	The pnparser 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.
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.

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

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.
process_postfire_srv	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: • 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
LOADER service	The LOADER service efficiently stores the events and incidents into the database and compresses the data to be stored for archival purposes.
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.
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.
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.
REPORTGEN service	The REPORTGEN service generates and sends the reports for the users. The service uses the JBOSS/Tomcat application server framework.

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

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 syncrhonized is: • 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
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.
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.
device_monitor	The PNMONITOR service acts as a software watchdog for JBOSS and SUPERV. The operating system watches the health of PNMONITOR service.
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.
csdam	This backend process is 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. For more information on DTM, see "How DTM Works" in *Technology Preview: Configuring Distributed Threat Mitigation with Intrusion Prevention System in Cisco Security MARS*. This process was introduced in 4.1.
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.

Table B-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.
cswin	This backend process uses MS-RPC to pull alerts 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 introducted in version 4.2.2.
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.
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.
DbIncidentLoaderSrv	This process stores event/session data for fired incidents into the database after process_postfire_srv has performed false positive analysis.
pnesloader	This process stores event and session data in the database after pnparser has parsed and sessionized the recoeved data.
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_query_srv	This process computes the results for multi-lined queries (queries that look like multi-line rules. For example, X followed by Y).

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 6-24.

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 or 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

B

C

D

E

F

G

H

I

L

M

N

P

R

S

T

U

V

W

Z