



CHAPTER 2

Initial MARS Appliance Configuration

Revised: March 4, 2009, OL-16776-01

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

This chapter contains the following sections:

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

Checklist for Initial Configuration

Initial configuration of the appliance accomplishes several goals:

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

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

✓	Task
☐	<p>1. Establish a console connection to the appliance.</p> <p>Initial configuration requires a console connection to access the CLI. You should establish this connection with the power turned off on the MARS Appliance. Three console connection options exist:</p> <ul style="list-style-type: none"> • A direct console connection to the appliance using a keyboard and monitor • A standard serial console connection between a computer and the appliance using a terminal emulation package • An Ethernet console connection between a computer and the appliance using a terminal emulation package <p>After you configure your console connection, you must power up the appliance.</p> <p><i>Result:</i> The appliance is powered up and you can see the command line prompt through your console connection.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> • Establishing a Console Connection, page 2-4
☐	<p>2. Command Line Configuration: Setting the system administrative account's default password and configuring the interfaces.</p> <p>The command line configuration is separated into three tasks, each task being separated by a reboot of the appliance. The first task involves performing three to four procedures:</p> <ul style="list-style-type: none"> • Collect the information required to configure the appliance to operate optimally on your network. • Log in to the appliance and change the password associated with the system administrative account (pnadmin). • Configure the eth0 network interface, specifying the default gateway and IP address and network mask pair for that interface. • (Optional) Configure the eth1 network interface, specifying the IP address and network mask pair for that interface. <p>Each MARS Appliance has two Ethernet interfaces: eth0 and eth1. Your default gateway (applies to eth0) 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 the appropriate interface.</p> <p>Tip As a best practice, dedicate one interface to collecting event data and logs from your network and use the other for an out-of-band management (OOBM) network or for a console connection.</p> <p>MARS can use both interfaces to receive event data and logs as long as the subnetwork and gateway are correctly configured. To determine whether too many packets are being dropped, use the ifconfig command. If you see numerous dropped packets, you may want to configure the appliance to receive traffic on both interfaces.</p> <p>Note The MARS Appliance does not allow you to configure both of its interfaces on the same network.</p> <p><i>Result:</i> The default password is no longer associated with the system administrative account and the appliance is more secure. Also, one or more interfaces are configured to communicate on your network. When you complete the IP address configuration changes for either interface, the appliance reboots.</p> <p>For more information, see:</p> <ul style="list-style-type: none"> • Configuring Basic Network Settings at the Command Line, page 2-6 • Change the Default Password of the System Administrative Account, page 2-6 • Specify the IP address and Default Gateway for the Eth0 Interface, page 2-7. • (Optional) Specify the IP Address for the Eth1 Interface, page 2-8

✓	Task
☐	<p>3. Command Line Configuration.</p> <p>The second task of the CLI configuration involves setting the hostname of the appliance. The hostname identifies which appliance collects a specific log and which appliance fires an inspection rule. This unique identity is important in an environment where Global Controller is running. To complete this task, you must:</p> <ul style="list-style-type: none">• Log in to the appliance using the system administrative account and the new password.• Set the hostname of the appliance. <p><i>Result:</i> The hostname is configured for the appliance. The appliance reboots.</p> <p>For more information, see:</p> <ul style="list-style-type: none">• Specify the Appliance Hostname, page 2-9.
☐	<p>4. Command Line Configuration.</p> <p>The third and final task of the initial CLI configuration involves specifying those settings that help ensure the integrity of the event correlation and complete your network connection, allowing access to the appliance from other hosts on the network. After you complete this phase, you can connect to and complete the appliance configuration using a non-console connection from any host on your network. To complete this task, you must:</p> <ul style="list-style-type: none">• Log in to the appliance using the system administrative account and the new password.• Set any additional static routes.• Set the clock.• Set the NTP server settings.• Set the DNS domain name.• Connect the appliance to the network (that is, plug in the Cat 5 cables.) <p><i>Result:</i> Now you have network connectivity. You can access the CLI interface using an Secure Shell (SSH) client on any host that can reach the appliance, and you can log in to the web interface to complete the initial configuration.</p> <p>For more information, see:</p> <ul style="list-style-type: none">• Specify the Time Settings, page 2-10• Set Up Additional Routes, page 2-9• Completing the Cable Connections, page 2-11

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

Establishing a Console Connection

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

The four initial console connection options are:

- **Direct Console.** Directly attach a keyboard and monitor the appliance. This option provides the most console feedback of the three console connection options, and it does not require any additional software, such as a terminal emulator or SSH client.
- **Serial Console.** Before powering on the appliance, connect a computer to the serial port using the appropriate cable. For the location of the serial port, see the backplane figure corresponding to your appliance model in the *Cisco Security MARS Hardware Installation Guide*. Configure your terminal emulation communication software (such as Hyper Terminal) to operate with the following settings:
 - Baud = 9600
 - Databits = 8
 - Parity = None
 - Stops = 1
 - Flow control = None
- **Ethernet Console.** Before powering on the appliance, connect a computer to eth1 using a crossover CAT5 cable, configuring the computer's local TCP/IP settings to be on the 192.168.0.0 network. Pick an IP address other than 192.168.0.100 and 192.168.0.101, which are the default addresses assigned to eth0 and eth1, respectively. As a best practice, reserve the eth1 port for administrative connections, such as the Ethernet console. For the location of the eth1 port, see the backplane figure corresponding to your appliance model in the *Cisco Security MARS Hardware Installation Guide*. Once configured, use an SSH client to connect as described below.

**Tip**

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

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

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

- Step 1** Select from among the direct, serial, or ethernet console connection options and configure according to the information provided under that description.
- Step 2** Power on the MARS Appliance and the console, and if required by the option, open your terminal emulation communication software on the console.
The login prompt appears.
- Step 3** Enter **padmin** as the username and the password associated with that account.
By default, the password is padmin.

**Note**

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

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

Configuring Basic Network Settings at the Command Line

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

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

To configure the MARS Appliance, follow these steps:

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

Change the Default Password of the System Administrative Account

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

**Note**

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

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

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



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

Step 2 Log in using the system administrative account and password (pnadmin/pnadmin).

The system displays the [pnadmin]\$ prompt.

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

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

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

```
? for list of commands
```

```
[pnadmin]$
```

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



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

The system displays the `New password:` prompt.

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

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

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

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

The system displays the [pnadmin]\$ prompt.

Specify the IP address and Default Gateway for the Eth0 Interface

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

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

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

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

The system displays the [pnadmin]\$ prompt.

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

The system displays the following message on the console:

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

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

The system displays the following message on the console:

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



Note

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

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

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

Specify the IP Address for the Eth1 Interface

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

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

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

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

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

The system displays the [pnadmin]\$ prompt.

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

The system displays the following message on the console:

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

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

The system displays the following message on the console:

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



Note

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

Specify the Appliance Hostname

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

To specify the hostname, follow these steps:

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

**Tip**

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

The system displays the following message on the console:

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

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

The system displays the following message on the console:

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

**Note**

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

Set Up Additional Routes

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

**Caution**

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

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

Add a Static Route

This command permanently changes the MARS routing table.

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

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

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

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

Delete a Static Route

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

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

To delete a host at `192.168.0.101`, enter:

```
route del -host 192.168.0.101
```

Specify the Time Settings



Caution

You must configure NTP on the Global Controller and on each Local Controller to ensure that rules fired by the Local Controller are properly propagated to the Global Controller. For more information on configuring NTP, see [ntp, page 1-33](#).

After you have the basic connection settings, you must specify the time, date, and timezone of the appliance. Use the console connection to 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.
- Set each Local Controller to the same timezone as the reporting devices that it monitors. Set the Global Controller to the Global Controller's local time zone. The **timezone set** command uses a sequence of menu selections to set the timezone. The menu order is continent/country/region. The option to set a POSIX TZ variable is also available.
- 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.
 - If an NTP server is unavailable, manually specify the date and time for this appliance as follows:
 - a. Enter **date** to specify the date in *mm/dd/yyyy* format.
 - b. Enter **time** to specify the time in *hh:mm:ss* format.

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

Completing the Cable Connections

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

Completing the Configuration using MARS web interface

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

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

Licensing the Appliance

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

Licensing the 6.x Software

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

**Note**

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

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

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

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

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

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

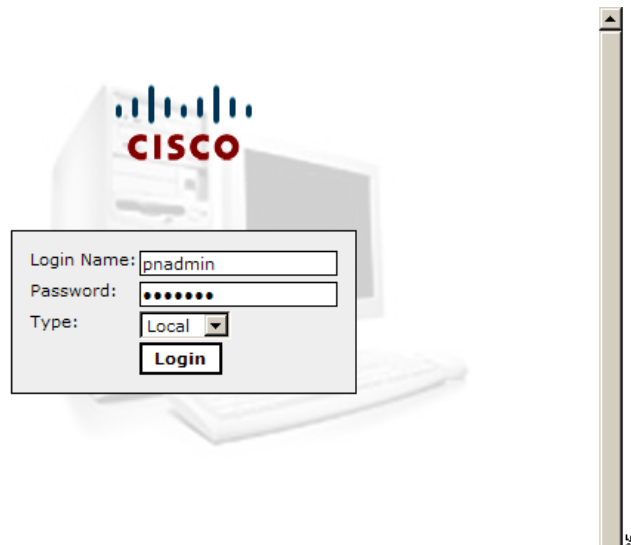
**Note**

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

**Note**

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

Figure 2-1 MARS Login Page



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

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

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

**Note**

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

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

Figure 2-2 Click the License Key Link

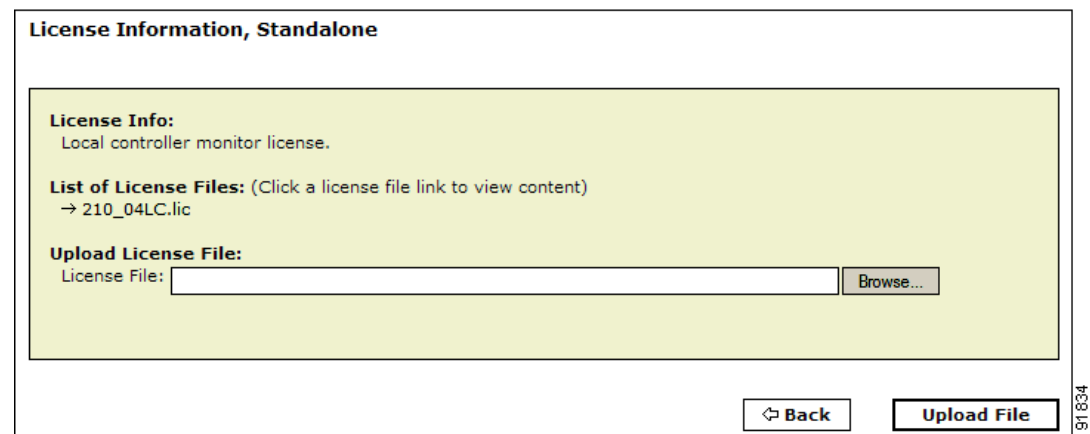


- Step 7** Click the link that directs you to load the license key file on the System Maintenance > License Key, Upgrade, and Certificates > Set License page.

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

The License Information page displays.

Figure 2-3 Import the License Key



- Step 8** Click **Browse** under Upload License Files, select the .lic file on your local computer, and click **Open**. The license key file is uploaded appears under List of License Files. The license key information field is populated based on the information found in the license file.
- Step 9** To view the content of an uploaded license file, click the link of the license filename under the List of License Files.

**Note**

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

Verifying and Updating Network Settings

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

To configure the necessary settings, follow these steps:

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

The Device Configuration page displays.

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

CS-MARS Device Config

The screenshot shows the 'CS-MARS Device Config' page with the following configuration details:

- Name:** GC181-DSF
- Interface IP Address, Net Mask, Default Gateway:**

Interface Name	IP Address	Net Mask	Default Gateway
eth0	10.2.3.181	255.255.255.0	10.2.3.1
eth1	192.168.1.100	255.255.255.0	
- Zone:**
 - Name:** default_global_zone
 - Description:** Default global zone
- Mail Gateway:**
 - IP:Port:** mailgw : 25
 - Email domain name:** cisco.com (ex: Enter 'domain1' for user@domain1)
 - Email Format:** Full graphics Minimal graphics (Recommended for Lotus Notes clients)

Step 2 Verify the following information is correct:

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



Note

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

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

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

**Note**

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

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

Specifying the DNS Settings

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

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

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

Figure 2-5 Domain Name Server Information

DNS Config

→ DNS Address
DNS Search Path

Primary DNS:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input style="width: 100%;" type="text" value="cisco.com"/>
Secondary DNS:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	
Tertiary DNS:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	

Search Domain:

132962

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

**Note**

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

Configuring E-mail Settings for the System Administrative Account

One of the required settings for MARS is the e-mail address for the system administrative account, pntadmin. 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 (pntadmin), and click **Edit**.

Result: The User page appears.

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

Configuring TACACS/AAA Login Prompts

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

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

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

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

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

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

Updating the Appliance to the Most Recent Software

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

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

Next Steps

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

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

This configuration includes:

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

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