



CHAPTER 6

Management Tab Overview

Use the management features in the Local Controller to assign: event, addressing, service, and user information. This information is used in rules, queries, and to determine false positives.

This chapter contains the following topics:

- [Understanding the Activate Button, page 6-1](#)
- [Event Management, page 6-2](#)
- [Using Event Groups, page 6-2](#)
- [IP Management, page 6-3](#)
- [Service Management, page 6-8](#)
- [User Management, page 6-11](#)

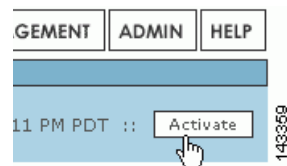
Understanding the Activate Button

In general, you need to activate changes in the Management tabs if the changes are part of a rule. If a change is made that requires activation, the color of the Activate button turns from gray to red. If you plan to make a series of changes, it may be more efficient to perform all of the changes and then click **Activate**. Activate instructs the MARS Appliance to pick up changes and apply them to the running system.

To activate a set of management additions or changes, follow these steps:

-
- Step 1** Make one or more changes.
- Step 2** When changes (or additions) are complete, activate them by clicking Activate.

Figure 6-1 Clicking the Activate Button



The MARS Appliance picks up the changes and applies them to the running system

Event Management

To open the Event Management sub-tab, click the **Management > Event Management** tabs.

On the Event Management page, you can search for and filter events and event groups, and work with groups of events.

Search for an Event Description or CVE Names

You can search for partial matches of event descriptions or Common Vulnerabilities and Exposures (CVE) names.

-
- Step 1** Enter the text that you want to search for in the **Search** field.
 - Step 2** Click **Search** .
-

View a List of All Currently Supported CVEs

You can generate a list of all Common Vulnerabilities and Exposures (CVEs) currently supported.

-
- Step 1** Enter CVE into the **Search** field.
 - Step 2** Click **Search**.
-

Using Event Groups

Using and creating event groups is one of the most powerful ways to employ rules. You can take any of the events presented here, group them, and then use them with rules to concentrate your searches for attacks.

Filtering by Event Groups or Severity

From the appropriate list, select the group or severity.

Edit a Group of Events



Note You cannot edit system-defined groups.

- Step 1** Select the group in the Select Group list.
- Step 2** Click **Edit Group**.

- Step 3** Click each group in the Chosen and Available fields to select it. Click it again to deselect it.
- Step 4** Click **Add** or **Remove** to move highlighted items as needed.
- Step 5** Click **Submit**.
-

Add an Event Group

- Step 1** Click **Add**.
- Step 2** In the Name field, enter a name for the group.
- Step 3** In the Available field, click each group that you want to add to select it. Click it again to deselect it.
- Step 4** Click **Add**.
- Step 5** Click **Submit**.
-

IP Management

The IP Management page, accessed by clicking **Management > IP Management**, enables the definition of network assets that you use as building blocks for inspection rules, drop rules, reports and queries, topology discovery schedules, and in defining reporting devices and mitigation devices. You can define assets as networks, IP ranges, or hosts. You can also defined named variables for use within inspection rules.

The vulnerability assessment information that you define for a host—specifically the operating system type and patch level and the known services that run on the host—assists MARS in determining false positives.



Tip

You can filter the list of objects displayed by the View list box. This selection allows you to filter to hosts, networks, IP ranges, or variables.



Note

A Global Controller pushes any global IP Management Groups to the active Local Controllers that it manages.

This section contains the following topics:

- [Search for an Address, Network, Variable, or Host, page 6-4](#)
- [Filter IP Management List, page 6-4](#)
- [Edit an IP Group, page 6-4](#)
- [Add an IP Group, page 6-4](#)
- [Add a Network, IP Range, or Variable, page 6-5](#)
- [Add a Host to a Local Controller, page 6-5](#)
- [Edit Host Information on a Local Controller, page 6-7](#)

Search for an Address, Network, Variable, or Host

- Step 1** Select **Management > IP Management**
 - Step 2** Enter the text that you want to search for in the **Search** field.
 - Step 3** Click **Search**.
-

Filter IP Management List

The IP Management tab includes the filter options for view and group that you can use to display a shorter, filtered list.

Perform either of the following filter steps, as desired:

- Step 1** From the **View** dropdown list, select a view. Choices include the following:
 - Variable
 - Network
 - IP Range
 - Host
 - All
 - Step 2** From the **Select Group** dropdown list, select a group.
-

Edit an IP Group

- Step 1** Select **Management > IP Management**.
The IP Management page appears.
 - Step 2** Select the group in the **Select Group** list.
 - Step 3** Click **Edit Group**.
 - Step 4** Click each group in the **Chosen** and **Available** fields to select it. Click it again to deselect it.
 - Step 5** Click **Add** or **Remove** to move highlighted items as needed.
 - Step 6** Click **Submit**.
-

Add an IP Group

- Step 1** Select **Management > IP Management**.
The IP Management page appears.

- Step 2** Click **Add Group**.
- Step 3** In the **Name** field, enter a name for the group.
- Step 4** In the **Available** field, click a group to select it. To deselect an item, click it again.
- Step 5** Click **Add** to move the selected Event Type Groups into the Chosen field.
- Step 6** Click **Submit**.

Add a Network, IP Range, or Variable

- Step 1** Select **Management > IP Management**.
The IP Management page appears.

Figure 6-2 Add a Network, IP Range, or Variable

Type:

- Network
- IP Range
- Variables

Network IP: . . .

IP Mask: . . .

143375

- Step 2** Click **Add**.
- Step 3** In the **Type** list select network, IP range, or variable.
- Step 4** For each type, enter the appropriate information.
- **Network**—name, network IP, network mask
 - **IP range**—name and range
 - **Variable**—variable name
- Step 5** Click **Submit**.

Add a Host to a Local Controller

Within MARS, a host is manually or automatically defined as the result of one of the following options:

- A reporting device or mitigation device defined under the Admin > Security and Monitoring Devices tab.
- A host managed by a reporting device defined under the Admin > Security and Monitoring Devices tab, such as a host running Cisco Security Agent and discovered by MARS when processing the logs provided by the CSA Management Console.

- An asset that you want to identify for the purpose of actively interacting with that host from the MARS system, such as third-party syslog sever to which you want to forward syslog messages using alerts.
- A host that is discovered by the system as part of topology discovery. For example, when processing the ARP cache table on a Cisco Catalyst Switch.
- A host involved in a session that, at one time or another, was considered suspicious, such as a potential target of an attack. In this case, MARS will have performed a Nessus and nmap port sweep of the host to identify whether it was likely it had been breached.

Due to these various options, you can have a large number of hosts defined on the IP Management page in the web interface. If you do not have a vulnerability assessment package that is compatible with MARS, you should consider providing as much information as possible about these hosts. For information on configuring the QualysGuard API Server for vulnerability assessment, see the chapter [Qualys QualysGuard Devices](#) in the *Device Configuration Guide for Cisco Security MARS, Release 6.x*.

**Note**

If you are attempting to add a host and you are detecting a conflict with a previously defined host, see [Delete a Device, page 3-14](#) for additional troubleshooting information.

To manually add a host, follow these steps:

Step 1 Select **Management > IP Management**.

The IP Management page appears.

Step 2 Click **Add**.

Step 3 In the Type list select **host**.

Figure 6-3 General Information for a Host

Type:

↓

General	Vulnerability Assessment Info									
<p>→ *Device Name: <input type="text"/></p> <p>→ Access IP: <input type="text"/>.<input type="text"/>.<input type="text"/>.<input type="text"/></p> <p>→ Operating System: <input type="text" value="Windows"/></p> <p>→ NetBIOS Name: <input type="text"/></p> <p>Enter interface information:</p> <table border="1"> <thead> <tr> <th>Name:</th> <th>IP Address:</th> <th>Network Mask:</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> ether0</td> <td><input type="text"/>.<input type="text"/>.<input type="text"/>.<input type="text"/></td> <td><input type="text"/>.<input type="text"/>.<input type="text"/>.<input type="text"/></td> </tr> <tr> <td colspan="3" style="text-align: right;"><input type="button" value="Add IP/Network Mask"/></td> </tr> </tbody> </table> <p style="text-align: center;"> <input type="button" value="Add Interface"/> <input type="button" value="Remove Interface/IP"/> </p>		Name:	IP Address:	Network Mask:	<input type="checkbox"/> ether0	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="button" value="Add IP/Network Mask"/>		
Name:	IP Address:	Network Mask:								
<input type="checkbox"/> ether0	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>								
<input type="button" value="Add IP/Network Mask"/>										
<input type="button" value="Done"/> <input type="button" value="Apply"/>										

143370

- Step 4** In the **Device Name** field, enter the host's name.
- Step 5** In the **Access IP** field, identify the address used to pull log events from this host, or is used to connect to when performing dynamic vulnerability assessments while investigating detected attacks.
- Step 6** If the host is running a variety of Windows, Solaris, or Linux, select the corresponding value in the **Operating System** field. Otherwise, verify that **Generic** is selected.
- Step 7** If you are running NetBIOS on your network, in the **NetBIOS Name** field enter the name associated with this host.
- NetBIOS provides name registration and resolution services. MARS uses this setting to provide attack path analysis and address resolution.
- Step 8** Under Enter Interface Information, enter the values for the interface Name, IP Address, and Network Mask.
- Step 9** Add additional IP addresses and masks to the interface, as necessary, by clicking **Add IP/ Network Mask**.
- Step 10** If you have a dual-homed host, you can add additional interfaces by clicking **Add Interface**.

Edit Host Information on a Local Controller

- Step 1** Select **Management > IP Management**.
- Step 2** From the View dropdown list, select **Host**.
- Step 3** Check the box to the left of the host that you want to edit.

- Step 4** Click **Edit**.
- Step 5** Make changes, as necessary, to the following fields:
- Device Name
 - Access IP
 - Operating System
 - NetBIOS Name
- Step 6** To enter or edit interface information for the selected host, you have the following choices:
- a. To add another interface, click **Add Interface** . Then, on the new line that appears, specify the Name, IP Address, and Network Mask.
 - b. To remove an interface or IP, check the box to the left of an interface and click **Remove Interface/IP**.
 - c. To add an IP or Network Mask to an interface, click **Add IP/Network Mask**. Then specify the IP Address, and Network Mask.
- Step 7** Click **Done** when you are finished editing.
- Step 8** After you have made all the changes desired for this administrative session, click **Activate**.

**Tip**

If you are adding or editing several devices, it is better for the system that you click Activate for several changes rather than for each individual change.

Service Management

To open the Service Management sub-tab, click the **Management > Service Management** tabs.

Service is a combination of source port, destination port, and protocol. The Service Management page displays services and their descriptions, ports, and protocols. On the Service Management page, you can work with the services on your networks.

This section contains the following topics:

- [Search for a Service, page 6-8](#)
- [Add a Group of Services, page 6-9](#)
- [Edit a Group of Services, page 6-9](#)
- [Add a Service, page 6-10](#)
- [Edit a Service, page 6-10](#)
- [Delete a Service, page 6-10](#)

Search for a Service

- Step 1** Click the **Management > Service Management** tabs.
- Step 2** Enter the text that you want to search for in the Search field.
- Step 3** Click **Search**.



Tip To filter by service groups, select the group you want from the Select Group list.

Add a Group of Services

-
- Step 1** Click the **Management > Service Management** tabs.
- Step 2** Click Add Group.
- Step 3** In the Name field, enter a name for the group.
The Service Group page appears, with available services listed in the box on the right.
- Step 4** Check the box next to the services to select them (you can click them again to de-select them).
- Step 5** Click <<**Add**.
- The services are listed in the box on the left.
- Step 6** Click **Submit**.
The new group is established and available in the Select Group list.
-

Edit a Group of Services



Note You cannot edit system-defined groups.

To edit the services included in a group of services, follow these steps:

-
- Step 1** Click the **Management > Service Management** tabs.
- Step 2** Select the group in the **Select Group** list.
- Step 3** Click **Edit Group**.
- Step 4** To add an item to the group, check the box next to the service to select it, then click <<**Add**.



Tip Clicking again deselects the item.

The service(s) are listed in the box on the left.

- Step 5** To remove a service from the group, click on a service (or services) to select it, then click **Remove>>**.
The services are relisted in the box on the right.
- Step 6** When finished editing the list click **Submit**.
-

Add a Service

Step 1 Click the **Management > Service Management** tabs.

Step 2 Click **Add**.

The Define Service page appears.

Step 3 Enter the service's details, including:

- Name
- Description (your own description)
- Protocol (select from list)
- Source Port (entered either as a value or as a range with high and low values specified)
- Destination Port Port (entered either as a *Value* or as a *Range* with high and low values specified)

Step 4 Click **Submit**.

The service is added.

Edit a Service

Step 1 Click the **Management > Service Management** tabs.

Step 2 Select the checkbox to the left of the service you want to edit.

Step 3 Click **Edit**.

Step 4 Make changes as required and then click **Submit**.

Delete a Service

Step 1 Click the **Management > Service Management** tabs.

Step 2 Select the checkbox to the left of the service you want to delete.

Step 3 Click **Delete**.

Step 4 On the confirmation page, click **Yes**.

User Management

MARS supports local authentication of MARS users; user credentials are stored on the MARS Appliance in SHA-1 cryptographic hash format. Each MARS Appliance only has one Administrative account that is named *pnadmin*. This is the only account with privileges to access the command line interface via SSH or direct console connection.

This section contains the following topics:

- [Basic User Management, page 6-11](#)
- [Global and Local Controller User Management Functions, page 6-12](#)
- [User Credentials, page 6-12](#)
- [Adding a New User, page 6-12](#)
- [Adding a Service Provider \(Cell phone/Pager\), page 6-14](#)
- [Searching for a User, page 6-14](#)
- [Editing or Removing a User, page 6-15](#)
- [Creating a User Group, page 6-15](#)
- [Adding or Removing a User from a Custom User Group, page 6-15](#)
- [Filtering by Groups, page 6-16](#)
- [Promoting Global User Roles on Local Controller, page 6-16](#)

Basic User Management

The User Management page enables you to manage other users and administrators of the MARS system, including the roles and groups to which those users belong. On this page, you can define new user accounts, enabling their access to specific features of the web interface. You can also define user-specific notification settings for the user, such as a valid e-mail address or pager number. Some system-wide settings—including pager and cell phone service provider settings—are also accessible exclusively through this page. To access the User Management page, click either **Management > User Management** or **Admin > User Management**.

In MARS, four separate user roles exist that can be assigned to any user who needs to access the web interface:

- **Admin**—This user role has full read/write privileges. Users in this role can define new users with any desired role. Users in the role can change the password settings of the accounts in any user role.
- **Security Analyst**—This user role has full read privileges but is restricted to write for reports privileges. Users in this role can only define new users (and change passwords of users) with the Notifications Only role.
- **Operator**—This user role has read only privileges. Users in this role cannot define new users or change passwords, even of their own user account. However, users in this role can resubmit reports.
- **Notifications Only**—This user role has no permissions to access to the MARS web interface; use this role to identify users who will receive notifications, such as e-mail, SMS, or pager notifications.

No limit exists on the number of user accounts that can be defined in MARS.

While roles are system defined, you can define, edit, and delete user groups. For more information, see [Creating a User Group, page 6-15](#) and [Adding or Removing a User from a Custom User Group, page 6-15](#).

Global and Local Controller User Management Functions

Users created on the Global Controller are propagated down to the Local Controller with one notable exception: the user “padmin” is always local to the Global Controller or Local Controller on which it is first created.

When you create users with the same login name or the same first name/last name combination on both the Global Controller and a Local Controller, both appear in the list of users on the Local Controller: once as a local user, once as global.

Global users are maintained only on the Global Controller; local users are maintained only on individual Local Controllers. Users created on Local Controllers are not propagated up to the Global Controller. If you want a user of a Local Controller to have access to the Global Controller or any of its information, you must also create that user at the Global Controller level.

User Credentials

Good security practices dictate strong passwords for use with the MARS Appliances. When defining user names and password, keep the following guidelines in mind:

Login names and passwords:

- Can be alphanumeric characters
- Can contain special characters (!, @, #, etc.)
- *Cannot* contain single or double quotes (‘or “)
- Are case sensitive

Login names can have up to 20 characters. Passwords can have up to 64 characters.

Adding a New User

Defining a new user involves specifying the username, password, role, contact information, and notification information.

To add a new user, follow these steps:

-
- Step 1** From the **Management > User Management** tab, click **Add**. The User Configuration page appears, as shown in [Figure 6-4](#).

Figure 6-4 User Configuration Page

Role: Admin

Login: padmin

Password:

Re-enter password:

First Name:

Last Name:

Organization:

Email:

SMS:

Work Phone:

Home Phone:

Fax:

Pager: (Cell phone or pager number e.g: 4082345678)

Service Provider:

143791

- Step 2** From the **Role** list, select one of the following values for the user.
- **Admin**—has full use of Local Controller.
 - **Notification Only**—for a non-user of the appliance, use this to send alerts to people who are not admins, security analysts, or operators.
 - **Operator**—has read-only privileges.
 - **Security Analyst**—has full use of Local Controller, except cannot access the Admin tab.
- Step 3** Create or change the user's password if necessary.
- Step 4** Enter the user's credentials and personal information. The information can include the following:
- First name
 - Last name
 - Organization name
 - Email address
 - PGP Key (on Global Controller only)
 - Short Message Service (SMS) number—for example, 8885551212@servprov.com
 - Work telephone number
 - Home telephone number
 - FAX number
 - Pager number— may also be a mobile telephone number, for example, 5552345678

- Step 5** If you are creating a notification by pager, go to the next section, [Adding a Service Provider \(Cell phone/Pager\)](#), page 6-14, otherwise click **Submit** to complete the procedure for adding a user.

Adding a Service Provider (Cell phone/Pager)

When configuring a notification by pager, add a service provider (cell phone or pager company) by performing the following procedure:

- Step 1** From the **Service Provider** field, select **New Provider** from the list. Additional fields appear, as shown in [Figure 6-5](#).

The drop-down list is populated as you add new service providers.

Figure 6-5 Select a New Provider and Provide Contact Details

- Step 2** Specify values for the following fields:
- **Provider Name**—The name of the service provider.
 - **Provider Phone No**—The service provider’s telephone number. This is the number the service provider uses for accepting alpha-numeric messages using the IXO/TAP protocol. The format is like a regular phone number, such as: 18001234567. The format of 1-800-1234567 is also acceptable. If dialing “9” is required to access a number outside your private branch exchange, type a “9,” before the full telephone number (for example, 9,1-800-1234567).
 - **Provider Baudrate**—The baud rate specified by the provider. This is the baud rate the service provider requires for the specified phone number. Common values are 1200, 2400, 4800, and 9600. Consult your service provider’s website for more information on their baud rates, if necessary.
- Step 3** Click **Submit** to close the User Configuration page and return to the User Management tab.

Searching for a User

- Step 1** Enter the text that you want to search for in the **Search** field.
- Step 2** Click **Search**.

Editing or Removing a User

-
- Step 1** From the **Management > User Management** tab, check the box next to the user's name.
- Step 2** Do one of the following:
- Click **Delete** to delete the user.
 - Click **Edit** to change the user's configuration information. The User Configuration page appears. Edit the User Configuration page, as necessary.
- Step 3** Click **Submit**.
-

Creating a User Group

-
- Step 1** Click **Add Group**.
- Step 2** In the Name field, enter a name for the group.
- Step 3** To add to the group, check the users from the list on the right hand side. Click **Add**.
The checked names move to the lefthand side of the dialog box.
- Step 4** To remove users from the group, select the users from the left hand side with **Ctrl+click** . Click **Remove**.
The selected names move to the righthand side of the dialog box.
- Step 5** Click **Submit**.
-

Adding or Removing a User from a Custom User Group



Note *Admin, Operator, Notification, and Security Analyst* are system groups and cannot be edited. The user is automatically added to the User Group that corresponds to their role.

To add or remove a user from a custom User Group, follow these steps:

-
- Step 1** Select the User Group from the **Select Group** field.
The members of the group are displayed.
- Step 2** Click **Edit Group**.
The User Group dialog box appears.
- Step 3** To add to the group, check the users from the list on the right hand side. Click **Add**.
The checked names move to the lefthand side of the dialog box.
- Step 4** To remove users from the group, select the users from the left hand side with **Ctrl+click** . Click **Remove**.
The selected names move to the righthand side of the dialog box.
- Step 5** Click **Submit**.

You are returned to the User Management tab.

Filtering by Groups

From the **Select Group** list, select a group. Only the members of the selected group are displayed.

Promoting Global User Roles on Local Controller

A global “Admin” user can log into the Local Controller and promote a global “System Analyst” or “Operator” user to a higher role. For example, a global “Operator” can be promoted to become an “Admin” or “System Analyst” on the Local Controller. However, his/her role as an “operator” on the Global Controller remains the same as the changes remain on the local controller and do not get pushed up to the Global Controller. Once these users get promoted to a higher role, they cannot be demoted afterward.

Global “Notification” users cannot be promoted given that these users have no login password information.