



CHAPTER 23

Management Tab Overview

Revised: March 14, 2017, 78-17020-01

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.

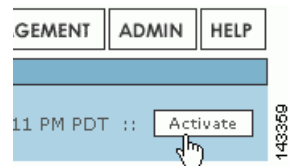
Activating

In general, you need to activate changes in the Management tabs if the changes are part of a rule.

To activate a set of management additions or changes

Step 1 When changes (or additions) are complete, activate them by clicking **Activate**.

Figure 23-1 Clicking the Activate Button



Event Management

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

On the Event Management page, you can search 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**.
-

To view a list of all currently supported CVEs

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

Event Groups

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

To filter by event groups or severity

From the appropriate list, select the group or severity.

Edit a Group of Events



Note

You can not 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 highlight it. Click it again to de-highlight it.
 - Step 4** Click **Add** or **Remove** to move highlighted items as needed.
 - Step 5** Click **Submit**.
-

Add a 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 highlight it. Click it again to de-highlight 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.

Search for an Address, Network, Variable, or Host

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

Filter by Groups

From the **Select Group** list, select the group.

Edit a 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 highlight it. Click it again to de-highlight it.
- Step 5** Click **Add** or **Remove** to move highlighted items as needed.
- Step 6** Click **Submit**.
-

Add a 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 highlight it. To de-highlight 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 23-2 Add a Network, IP Range, or Variable

Type: Network

Network IP: [] [] [] []

IP Mask: [] [] [] []

Cancel Submit

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

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 breached.

Because of 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 more information, see [Define Vulnerability Assessment Information, page 10-12](#).

**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 2-19](#) 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 23-3 General Information for a Host

Type:

↓

| General | Vulnerability Assessment Info | | | | | | | | | | | | |
|---|---|---|--|---------------------|--|-------|-------------|---------------|--|---------------------------------|---|---|--|
| → *Device Name: <input type="text"/> → Access IP: <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> → Operating System: <input type="text" value="Windows"/> → NetBIOS Name: <input type="text"/> | | | | | | | | | | | | | |
| Enter interface information: <table border="1"> <thead> <tr> <th colspan="2">Add Interface</th> <th colspan="2">Remove Interface/IP</th> </tr> <tr> <th>Name:</th> <th>IP Address:</th> <th>Network Mask:</th> <th></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> <td><input type="button" value="Add IP/Network Mask"/></td> </tr> </tbody> </table> | | Add Interface | | Remove Interface/IP | | 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"/> |
| Add Interface | | Remove Interface/IP | | | | | | | | | | | |
| 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 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 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, 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** Add as many IP address and masks to the interface by clicking **Add IP/Mask**.
- Step 9** Under Enter Interface Information, enter the values for the interface name, IP address, and network mask.
- Step 10** If you have a dual-homed host, you can add additional interfaces by clicking **Add Interface**.
- Step 11** To specify vulnerability assessment information, continue with [Define Vulnerability Assessment Information](#), page 10-12.

Edit Host Information

- Step 1** Select **Management > IP Management**.
- Step 2** Check the box next to the host that you want to edit.
- Step 3** If you are editing interface or IP mask information, make your changes here and click **Submit**.

- Step 4** If you need to edit the host's properties, click **Properties**.
 - Step 5** Make changes to the operating system as necessary, and click **Next**.
 - Step 6** To make changes to service or application, remove the old service by select its radio button, and click **Delete**.
 - Step 7** Click **Add Service**, and continue with Step 3.
-

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.

Search for a Service

-
- Step 1** Enter the text that you want to search for in the **Search** field.
 - Step 2** Click **Search**.
To filter by service groups
From the appropriate list, select the group.
-

Add a Group of Services

-
- Step 1** Click **Add**.
 - Step 2** In the **Name** field, enter a name for the group.
 - Step 3** In the **Available** field, click items to select them, and click them again to de-select them.
 - Step 4** Click **Add**.
 - Step 5** Click **Submit**.
-

Edit a Group of Services



Note You can not 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 highlight it. Click it again to de-highlight it.
 - Step 4** Click **Add** or **Remove** to move the highlighted items as needed.
 - Step 5** Click **Submit**.
-

Add a Service

- Step 1** Click **Add**.
 - Step 2** Enter the service's details.
 - Step 3** Click **Submit**.
-

Edit a Service

- Step 1** Check the box next to the service.
 - Step 2** Click **Edit**.
 - Step 3** Make your changes, and click **Submit**.
-

Delete a Service

- Step 1** Check the box next to the service.
 - Step 2** Click **Delete**.
 - Step 3** On the confirmation page, click **Yes**.
-

User Management

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

The User Management page allows 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 access to specific features of the web interface. You can define user-specific notification settings for the user, such as a valid e-mail address or pager number. Some system-wide settings, such as 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* 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* 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* has read only privileges. Users in this role cannot define new users or change passwords, even of their own user account.
- *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 [Create a User Group, page 23-12](#) and [Add or Remove a User from a User Group, page 23-12](#).

Good security practices suggest 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.

Add a New User

Defining a new user involves specifying the user name, 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 23-4](#).

Figure 23-4 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** field, select a **Role** for the user.

- **Admin:** has full use of Local Controller.
- **Notification Only:** for a non-user of the Local Controller 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
- 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, “[Add a Service Provider \(Cell phone/Pager\)](#)”, otherwise click **Submit** to complete the procedure for adding a user.

Add a Service Provider (Cell phone/Pager)

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

- Step 1** From the **Service Provider** field, select **New Provider**. Additional fields appear, as shown in [Figure 23-5](#).

The pull-down menu is populated as you add new service providers.

Figure 23-5 Select a New Provider and Provide Contact Details

Provider Name:

Provider Phone No: (e.g: 9,18002345678)

Provider Baudrate:

143372

- Step 2** In the **Provider Name** field, enter the name of the service provider.
- Step 3** In the **Provider Phone No** field, enter 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).
- Step 4** In the **Provider Baudrate** field, enter 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.
- Step 5** Click **Submit** to close the User Configuration page and return to the **User Management** tab.

Search for a User

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

Edit or Remove a User

-
- Step 1** Form the **Management User tab**, check the box next to the user's name.
 - Step 2** Click **Delete** to delete the user.
 - Step 3** Click **Edit** to change the user's configuration information. The User Configuration page appears.
 - Step 4** Edit the User Configuration page.
 - Step 5** Click **Submit**.
-

Create 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**.
-

Add or Remove a User from a User Group

To add or remove a user from a custom User Group, do the following steps:



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.

-
- 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.
-

Filter by Groups

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

