



## CHAPTER 5

# Alerts and Incident Notifications

---

A Cisco Security Monitoring, Analysis, and Response System (MARS) alert action is a signal transmitted to people or devices, or both, as notification that a MARS rule has fired, and that an incident has been logged. Alert actions can only be configured through the Action parameter of a rule. An alert action determines which alert notification types are sent to which MARS user accounts or user groups.

This chapter contains the following topics:

- [Notification Methods, page 5-1](#)
- [Configure the E-mail Server Settings, page 5-7](#)
- [Configure a Rule to Send an Alert Action, page 5-8](#)
- [Create a User—Role, Identity, Password, and Notification Information, page 5-13](#)
- [Create a Custom User Group, page 5-15](#)
- [Add a User to a Custom User Group, page 5-16](#)

## Notification Methods

The content of alert notifications is fixed and cannot be customized. The XML notification contains the most information of all the alert notification types.

MARS can transmit alerts by the methods listed in [Table 5-1](#).

Table 5-1 MARS Incident Notification Methods

Alert Notification Type	Description
<p data-bbox="342 327 667 359"><b>Sent in Human-Readable Format</b></p> <ul data-bbox="358 373 732 537" style="list-style-type: none"> <li data-bbox="358 373 472 401">• E-mail</li> <li data-bbox="358 422 597 449">• XML Notification</li> <li data-bbox="358 470 732 497">• Short Message Service (SMS)</li> <li data-bbox="358 518 456 546">• Pager</li> </ul>	<p data-bbox="911 373 1476 653">E-mail notifications send the incident ID, matched rule, severity, incident time, Top 3 source-destination address pairs, Top 3 source IPs, Top 3 destination IPs, Top 3 destination TCP/UDP ports, Top 3 event types, and Top 3 reporting devices in the body of the email. For Botnet Traffic Filter rules, Botnet Site information is included in the email (when available).</p> <p data-bbox="911 674 1476 793">SMS, and pager alerts send the incident ID, matched rule name, severity, and incident time in SMS and pager formats respectively. You must login to the MARS to view all the incident details.</p> <p data-bbox="911 814 1476 1318">XML notification sends an email notification of an incident with an attached XML data file (see <a href="#">Figure 5-1</a>). The XML data file contains the same incident details that can be viewed from the GUI, except for path and mitigation information. The XML data file can be sent as a plain-text file or as a compressed gzip file. The XML data filename is constructed with the incident ID number, for example: CS-MARS-Incident-13725095.xml. You can parse and extract data from the XML file with a custom application. For example, you can integrate the XML data with trouble ticketing software. See <a href="#">Appendix D, “Cisco Security MARS XML API Reference”</a> for further information on the MARS XML notification schema and usage guidelines.</p> <p data-bbox="911 1339 1476 1459">MARS SMS text message notifications can be up to 160 characters in length. Because the MARS SMS incident notification exceeds 160 characters, it is sent in three segments.</p> <p data-bbox="911 1480 1476 1728">Pager messages are sent through the MARS internal modem. MARS dials a carrier’s IXO/TAP number and uses SNPP to transmit the alpha-numeric page. Pager notifications are still possible when the network is down. Pagers can often receive messages in places where mobile phones are inoperative or forbidden (for instance, hospitals).</p>

**Table 5-1 MARS Incident Notification Methods (Continued)**

<b>Sent to a Device</b>	
<ul style="list-style-type: none"> <li>• SNMP trap</li> <li>• Syslog</li> </ul>	<p>These alerts send the incident ID, matched rule, severity, incident time, Top 3 source-destination address pairs, Top 3 destination TCP/UDP ports, Top 3 event types, and Top 3 reporting devices to MARS devices or applications, all of which must be properly configured within the MARS device administration pages. See the section, <a href="#">Chapter 2, “Security Threat Mitigation (STM) Task Flow Overview”</a> for information on configuring individual devices to work with MARS.</p>

Alert Notification Procedures [Table 5-2](#) provides links and descriptions of related Alert Action configuration procedures.

**Table 5-2 Alert Notification Procedures**

<b>Alert Related Procedures</b>	<b>Description</b>
<a href="#">Configure the E-mail Server Settings, page 5-7</a>	To send Email, SMS, and XML notifications, MARS requires that you configure the E-mail Server settings.
<a href="#">Configure a Rule to Send an Alert Action, page 5-8</a>	Complete this procedure to create or modify an alert action.
<a href="#">Create a User—Role, Identity, Password, and Notification Information, page 5-13</a>	Alert notifications can be sent only to user accounts configured on MARS. A new user account can be configured from the User Management tab, or when creating an alert action for a rule. This is where you enter the service provider phone numbers and email addresses for E-mail, SMS, Pager, and XML notification.
<a href="#">Create a Custom User Group, page 5-15</a>	Complete this procedure to create a MARS user group other than the default MARS user groups. Unlike default user groups, custom groups can be edited.
<a href="#">Add a User to a Custom User Group, page 5-16</a>	Complete this procedure to include a newly created user account into a MARS user group.

## MARS Incident Notification Examples

This section contains examples of the following notifications:

- [MARS Email Notification, page 5-4](#)
- [MARS Syslog Notification, page 5-5](#)
- [MARS SNMP Trap Notification, page 5-6](#)
- [MARS XML Notification Email Attachment, page 5-6](#)
- [MARS SMS Notification Example, page 5-7](#)

Incident notifications all report Rule ID, Rule Name, incident ID, incident start/end time and Incident Severity. Where applicable, notifications also report the following categories.

- Top 3 source IP and destination IP pairs
- Top 3 Source IP Addresses
- Top 3 Destination IP Addresses
- Top 3 TCP/UCP destination ports
- Top 3 reporting devices
- Top 3 event types
- Top 3 Botnet Sites (Botnet Traffic Filter incidents only)

The following considerations apply:

- Notifications are sent only from the Local Controller.
- Alert notifications cannot be customized.
- The Rule ID number is for internal use only, it has no correspondence to any rule attribute viewable from the MARS GUI or CLI.
- The Top 3 Source IP and Destination IP Pairs category is sorted first by session severity and then by count.
  - If the source or destination IP address is 0.0.0.0, it displays as “N/A.”
- The Top 3 Destination TCP/UCP ports category is sorted first by session severity and then by count.
  - If the source port and destination ports are “0” the destination port displays “N/A” otherwise it displays the actual port number or “0” for port number.
- Top 3 Reporting Devices category is sorted by session count.
- Top 3 Event Types category is sorted first by session severity and then by count.
- All “Top 3” categories display  $x$  of  $y$  occurrences. where  $x$  can be 1 to 3, and  $y$  can be 1 to  $n$ .
- The field “Count” is the always the count of the firing events that match the rule criteria.
- Because of space limitations, the syslog and SNMP incident notifications do not explicitly label botnet site information.

## MARS Email Notification

[Example 5-1](#) shows a typical email alert notification triggered by a Botnet Traffic Filter incident.



### Note

---

The Sudden Increase in Ports category is listed after the Top 3 Reporting Devices when applicable.

---

### **Example 5-1 Email Notification With Botnet Site Information**

```
From: notifier.pnmars@cisco.com [mailto:notifier.pnmars@cisco.com]
Sent: Friday, June 19, 2009 2:49 PM
To: Lavim Busa (labusa)
Subject: CS-MARS Incident Notification (yellow, Rule Name: labusa-notif)
```

The following incident occurred on "pnmars"

```
Start time:      Fri Jun 19 14:46:22 2009
End time:        Fri Jun 19 14:46:29 2009
```

```

Fired Rule Id: 328056
Fired Rule: labusa-notif
Incident Id: 607632
Incident Severity:yellow

Top 3 src-dest address pairs sorted by severity and count (showing 3 of 9):
1. N/A -> N/A Severity: yellow Count: 54
2. 1.2.3.4 -> 4.5.6.7 Severity: yellow Count: 6
3. 11.22.33.44 -> 41.52.63.74 Severity: yellow Count: 3

Top 3 src ip's address sorted by severity and count (showing 3 of 6):
1. N/A -> Severity: yellow Count: 54
2. 1.2.3.4 -> Severity: yellow Count: 6
3. 11.22.33.44 -> Severity: yellow Count: 5

Top 3 dest ip's address sorted by severity and count (showing 3 of 9):
1. N/A -> Severity: yellow Count: 54
2. 4.5.6.7 -> Severity: yellow Count: 6
3. 41.52.63.74 -> Severity: yellow Count: 3

Top 3 dest TCP/UDP ports sorted by severity and count (showing 2 of 2):
1. 80 Severity: yellow Count: 11
2. 80 Severity: green Count: 8

Top 3 event types sorted by severity and count (showing 3 of 16):
1. Download failed for dynamic filter data file from updater server Severity: yellow Count:9
2. Authentication failure with dynamic filter updater server Severity: yellow Count:9
3. Decryption of downloaded dynamic filter data file failed Severity: yellow Count:9

Top 3 reporting devices sorted by count (showing 1 of 1):
1. asa82 Count: 100

Top 3 sites sorted by count (showing 3 of 3):
1. cisco.com (Type: black) Count: 6
2. whitecisco.com (Type: white) Count: 6
3. altavista.com (Type: grey) Count: 5

For more details about this incident please go to:
https://pnmars/Incidents/IncidentDetails.jsp?Incident\_Id=607632
https://pnmars.mars.cisco.com/cisco.com/Incidents/IncidentDetails.jsp?Incident\_Id=607632
https://192.168.1.10/Incidents/IncidentDetails.jsp?Incident\_Id=607632
https://10.2.4.1/Incidents/IncidentDetails.jsp?Incident\_Id=607632

For all incidents occurred recently please go to:
https://pnmars/Incidents/
https://pnmars.mars.cisco.com/cisco.com/Incidents/
https://192.168.1.10/Incidents/
https://10.2.4.1/Incidents/

```

## MARS Syslog Notification

The rule name, reporting device name and event type is limited to 100, 50 and 50 characters respectively.

[Example 5-2](#) shows a MARS syslog notification.

### Example 5-2 MARS Syslog Notification

```

10.2.3.196 Wed Feb 4 14:48:40 2009 <34>Wed Feb 4 14:44:09 2009 %MARS-1-101: Rule 306498
(any) fired and caused green Incident 287020054, starting from Wed Feb 4 14:43:15 2009 to
Wed Feb 4 14:43:19 2009 on gVaAdGOCEW, Top 3 src dest addr pairsshowing 3 of 6 ;; N/A ->
N/A Severity: green Count: 4 ;; 10.4.11.10 -> 10.1.1.16 Severity: green Count: 1 ;;
10.4.11.10 -> 10.1.1.17 Severity: green Count: 1, Top 3 dest ports showing 3 of 4 ;; 21

```

```
Severity: green Count: 1 ;; 22 Severity: green Count: 1, Top
3 event types showing 3 of 3 ;; Built/teardown/permitted IP connection Severity: green
Count: 4 ;; Unknown Device Event Type Severity: green Count: 4 ;; CS-MARS Miscellaneous
authentication message Severity: green Count: 1, Top 3 reporting devices showing 3 of 6 ;;
gq_2 Count: 4 ;; d1_1 Count: 1 ;; d1_3 Count: 1
```

## MARS SNMP Trap Notification

All fields use the same enterprise OID, PROTEGO\_ENTERPRISE\_NUMBER:16686 but use different sub-OIDs, as follows:

```
enterprises.16686.1.0 string "MARS-1-101"
enterprises.16686.2.0 string "<alert_content>"
enterprises.16686.3.0 string "<optional_port_list_for_sudden_traffic_increase_incident>"
enterprises.16686.4.0 string "<Top 3 src-dest address pairs>"
enterprises.16686.5.0 string "<Top 3 dest TCP/UDP ports>"
enterprises.16686.6.0 string "<Top 3 event types>"
enterprises.16686.7.0 string "<Top 3 reporting devices>"
```

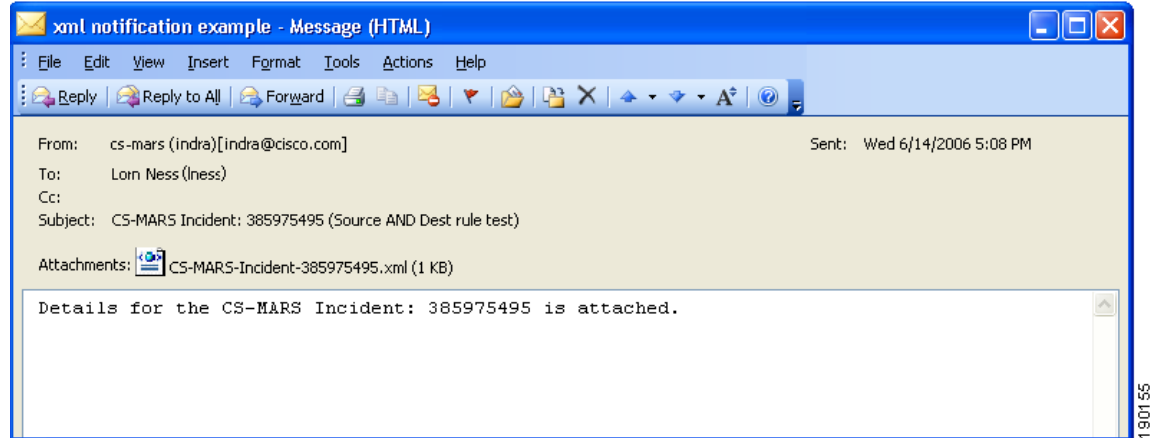
Example 5-3 shows a MARS SNMP trap notification message.

### Example 5-3 MARS SNMP Notification

```
SNMPv2-SMI::enterprises.16686.10.2.3.196 SNMPv2-SMI::enterprises.16686.1.0 "MARS-1-101"
SNMPv2-SMI::enterprises.16686.2.0 "<34>Wed Feb 4 14:44:09 2009 %MARS-1-101: Rule 306498
(any) fired and caused green Incident 287020054, starting from Wed Feb 4 14:43:15 2009 to
Wed Feb 4 14:43:19 2009 on gVaAdGOCE-W" SNMPv2-SMI::enterprises.16686.4.0 "Top 3 src-dest
address pairs sorted by severity and count showing 3 of 6, N/A -> N/A Severity: green
Count: 4, 10.4.11.10 -> 10.1.1.16 Severity: green Count: 1, 10.4.11.10 -> 10.1.1.17
Severity: green Count: 1" SNMPv2-SMI::enterprises.16686.5.0 "Top 3 dest TCP/UDP Ports
sorted by severity and count showing 3 of 4, 21 Severity: green Count: 1, 22 Severity:
green Count: 1, 23 Severity: green Count: 1" SNMPv2-SMI::enterprises.16686.6.0 "Top 3
event types sorted by severity and count showing 3 of 3, Built/teardown/permitted IP
connection Severity: green Count: 4, Unknown Device Event Type Severity: green Count: 4,
CS-MARS Miscellaneous authentication message Severity: green Count: 1"
SNMPv2-SMI::enterprises.16686.7.0 "Top 3 reporting devices sorted by count showing 3 of
6, gq_2 Count: 4, d1_1 Count: 1, d1_3 Count: 1"
```

## MARS XML Notification Email Attachment

Figure 5-1 shows an XML notification with its attached XML data file. When compression is configured, the XML data file arrives as a GZIP compressed file.

**Figure 5-1 MARS XML Notification Email Attachment**

## MARS SMS Notification Example

Example 5-4 shows a Simple Message Service notification.

### Example 5-4 MARS SMS Notification

```
From: notifier.gVaAdGOCEW@cisco.com [mailto:notifier.gVaAdGOCEW@cisco.com]
Sent: Wednesday, February 04, 2009 2:05 PM
To: Yi Lin (yilin)
Subject: CS-MARS Incident Notification(yellow,Rule Name:System Rule: DoS: Network -
Attempt)
Incident Id:287020048
```

## Configure the E-mail Server Settings

To send alert actions, MARS must be configured to communicate with an e-mail server.

To configure the e-mail server settings, follow these steps:

---

**Step 1** Click **Admin > Configuration Information**.

The Device Configuration window appears, as shown in [Figure 5-2](#).

Figure 5-2 MARS Device Configuration Window

CS-MARS Device Config

→ Name:

→

Interface Name	IP Address				Net Mask				Default Gateway			
eth0	10	89	149	151	255	255	255	128	10	89	149	254
eth1	192	168	1	100	255	255	255	0				

→ Mail Gateway:

IP:Port  :

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

143792

- Step 2** In the **IP:Port** field of the Mail Gateway section, enter the IP address and **Email Domain Name** of your Mail Gateway server.
- Step 3** Click the **Update** button at the bottom of the page to update the MARS configuration. The e-mail server settings for sending alert actions are configured.

## Configure a Rule to Send an Alert Action

To send alert notifications to individual users or groups of users, configure the Action parameters of a rule to create an alert action. This procedure configures alerts for pre-existing rules. When you create a rule, the Action parameters are configured after the count number parameter.



**Note** Drop rules do not have Action parameters and cannot trigger alerts.

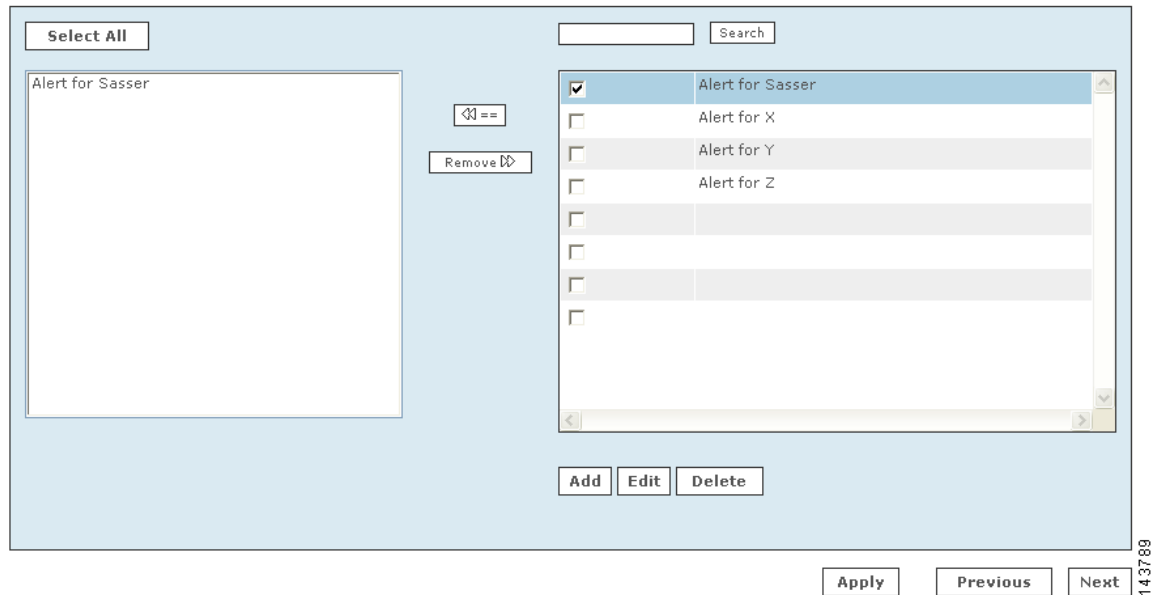
To modify or create an alert for an existing rule, follow these steps:

- Step 1** Click the **RULES** tab to navigate to the Inspection Rules page.
- Step 2** Identify the Rule to configure, and click the value displayed in the **Action** field.

The Action Selection dialog box, as shown in [Figure 5-3](#), appears below the rule description table. All defined alert actions are listed in the right-hand area of the Action dialog box. An alert action determines which alert notifications are sent to which users or user groups when the rule fires. You can edit or delete existing alert actions or create a new one.

**Figure 5-3** Action Selection Dialog

Action

**Step 3** Perform one of the following sub-procedures:

- Remove an alert action that is applied to the rule.
  - a. In the left-hand area, pick the alert actions to remove with Ctrl+Click, then click **Remove >>**.  
The alert action is deleted from the left-hand area.
  - b. Proceed to [Step 13](#) to complete the procedure.
- Apply an existing alert action to the rule.
  - a. In the right-hand area, click the check boxes of the alert actions you require, then click **<<==**.  
The alert action appears in the left-hand area.
  - b. Proceed to [Step 13](#) to complete the procedure.
- Delete an existing alert action from MARS.
  - a. Click the check box of the alert action in the right-hand area, then click **Delete**.  
A delete verification window appears.
  - b. Click **Yes**.  
The alert action is deleted from the right-hand area.
  - c. Proceed to [Step 13](#) to complete the procedure.
- Edit an existing alert action.
  - a. Click the check box of the alert action in the right-hand area, then click **Edit**.  
The Alert recipients page appears in a new window, as shown in [Figure 5-4](#).
  - b. Proceed to [Step 4](#) to complete the procedure.
- Create a new alert action.
  - a. Click **Add**.

The Alert recipients page appears in a new window, as shown in [Figure 5-4](#).

- b. Proceed to [Step 4](#) to complete the procedure.

**Figure 5-4** Alert Recipients Window

Name:

Description:

Email

Syslog

Page

SNMP

SMS

XML Email

Compress

Lucre, Phremeus

Lucre, Phremeus

251096

**Step 4** For a new alert enter a name and description in the **Name** and **Description** fields. If editing an existing alert, you can modify the name or description.

**Step 5** Click the check box of a notification type to select or deselect it.

Recipients for the notification types are as follows:

- **E-mail**—Users or user groups can receive an e-mail.
- **Page**—Users or user groups can receive an alpha-numeric electronic page on their pagers or pager-enabled mobile telephones.
- **SMS**—Users or groups can receive a text message on their SMS-enabled mobile telephones.

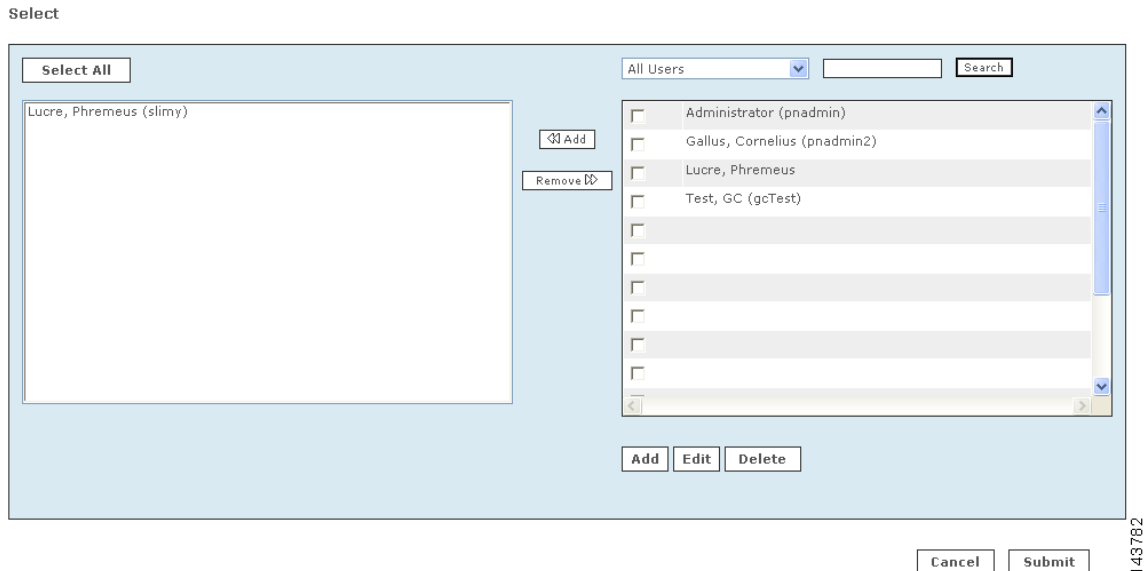
- **XML Email**—Users or groups can receive an email message with incident details appended in an XML data file. Click the **Compress** check box to send the XML data file as a compressed gzip file. For more information on this feature, see [Appendix D, “Cisco Security MARS XML API Reference”](#).
- **Syslog**—Specified devices can receive syslog messages. Non-reporting devices, such as a syslog server, are added to MARS as a Software security application on a host, and viewed on the page, **Management > IP Management > Host**
- **SNMP**—Specified devices can receive SNMP trap information. See, Syslog above.



**Note** For SNMP and Syslog, you must configure the receiving systems to receive notifications.

- Step 6** Click the **Change Recipient** button to add or remove a recipient for a notification type. For E-Mail, Page, SMS, and XML Email, the Select (recipient) dialog box appears, as shown in [Figure 5-5](#).

**Figure 5-5** Select Recipient Dialog Box



For Syslog and SNMP, the Select (device) dialog box appears, as shown in [Figure 5-6](#).

Figure 5-6 Device Selection Page



For Distributed Threat Management notification, the Select (IOS-IPS Devices) dialog appears (not shown).



**Tip** If you do not know the group to which a user or device belongs, select **All** from the dropdown list to view all users or devices.

- Step 7** Click the check box next to the users or device you want to receive the notification, then click << **Add**. Your selections appear in the left-hand area. To remove items, Ctrl+click the items in the left-hand area, then click **Remove**. The items are then deleted from the left-hand area.
- Step 8** If you are not adding a user, skip to Step [Step 9](#). To add a new user, do the following substeps:
- Click **Add**.
  - The User Configuration page appears in a separate window, as shown in [Figure 5-7](#).
- Step 9** Click **Submit**.  
You are returned to the [Figure 5-4](#).
- Step 10** Repeat Step [Step 6](#) through [Step 9](#) until you have assigned recipients to all the notification types you have selected.
- Step 11** Click **Submit**.  
You are returned to the [Figure 5-3](#). Any newly created or edited action alert appears in the right-hand area.
- Step 12** Click the check boxes next to the action alerts to be sent when the rule fires. Click << **Add**.  
Your selections appear in the left-hand area.
- Step 13** Click **Next**.  
The Time Range dialog may or may not appear.

- Step 14** Click **Next** if the Time Range dialog appears.  
The Rule Summary table appears.
- Step 15** Click **Submit** to save your changes to the rule.
- Step 16** Verify that the alert actions you selected appear in the Action field of the rule description.



---

**Note** An inactive rule is made active by applying an alert action. To inactivate a rule, select the rule and click **Change Status**.

---

## Create a User—Role, Identity, Password, and Notification Information

New user accounts and user groups are created on the **Management > User Management** tab, or as a substep in creating an alert notification recipient (with the **Add** button on the Select [user] dialog).

To create a MARS user, follow these steps:

- 
- Step 1** Navigate to the User Management page by either of the following methods:
- Click **Add** on the **Management > User Management** tab.
  - Click **Add** on the Select (user) dialog box when creating an alert notification. See [Configure a Rule to Send an Alert Action, page 5-8](#).

The User Configuration page appears, as shown in [Figure 5-7](#).

Figure 5-7 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 the MARS.
- **Notification Only**—for a non-user of the MARS appliance, use this to send alerts to people who are not administrators, security analysts, or operators.
- **Operator**—has read-only privileges.
- **Security Analyst**—has full use of the MARS, except read-only access to the Admin tab.

**Step 3** Create or change the user's password if necessary.

**Step 4** Enter the user's credentials and personal information, which may include any of 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 or ID—may also be a mobile telephone number, for example, 5552345678

**Step 5** If you are not creating a notification by pager, go to [Step 10](#).

**Step 6** For notification by pager, you must specify a service provider (cell phone or pager company). From the Service Provider field, select **New Provider**.

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

Additional service provider information fields appear on the same page, as shown in [Figure 5-8](#).

**Figure 5-8** Service Provider Fields to Add or Change a Service Provider

**Step 7** In the **Provider Name** field, enter the name of the service provider.

**Step 8** In the **Provider Phone No** field, enter the service provider's telephone number.

This is the number the service provider requires 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 9** 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.

**Step 10** Click **Submit**.

The new user is created, the User Configuration page is closed, and you are returned to the **User Management** tab.

## Create a Custom User Group

You can create a custom user group to help organize the user accounts on your system.

To create a custom user group in addition to the default groups created by MARS, follow these steps:

**Step 1** Navigate to the **Management > User Management** tab.

**Step 2** Click **Add Group**.

**Step 3** In the **Name** field, enter a name for the group.

**Step 4** To add users to the group, click the check box of users from the list on the right-hand area. Click **Add**. The checked names appear in the left-hand side of the dialog box.

To remove users from the group, pick the users from the left-hand side with Ctrl+click. Click **Remove**.

The selected names appear in the right-hand side of the dialog box.

**Step 5** Click **Submit**.

You are returned to the User Management tab.

---

## Add a User to a Custom User Group

Once you've defined a custom user group, you can add any users that are already defined to that group.

**Note**

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

---

To include a user in a custom user group, follow these steps:

---

- Step 1** Navigate to the **Management > User Management** tab.
  - Step 2** Select the User Group to edit from the **Select Group** dropdown list.  
The members of the group are displayed.
  - Step 3** Click **Edit Group**. The User Group dialog box appears.
  - Step 4** Check the users to add to the group from the list on the right hand side. Click **Add**. The checked names move to the left-hand area of the dialog box.
  - Step 5** Click **Submit**.  
You are returned to the User Management tab.  
The user is added to the custom user group.
-