



CHAPTER 23

Sending Alerts and Incident Notifications

A Cisco Systems MARS alert action is a signal transmitted to people or devices 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. MARS can transmit alerts by the methods listed in [Table 23-1](#).

Table 23-1 MARS Incident Notification Methods

Alert Notification Type	Description
<p>Sent in Human-Readable Format</p> <ul style="list-style-type: none"> • E-mail • XML Notification • Short Message Service (SMS) • Pager 	<p>E-mail, SMS, and pager alerts send the incident ID, matched rule name, severity, and incident time in email, SMS and pager formats respectively. You must login to the MARS to view all the incident details.</p> <p>XML notification sends an email notification of an incident with an attached XML data file (see Example 23-2). 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 <code>CS-MARS-Incident-13725095.xml</code>. 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 Appendix A, “Cisco Security MARS XML API Reference,” for further information on the MARS XML notification schema and usage guidelines.</p> <p>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>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>
<p>Sent to a Device</p> <ul style="list-style-type: none"> • SNMP trap • Syslog • Distributed Threat Mitigation 	<p>These alerts send the incident ID, matched rule severity, and incident time to devices or applications, all of which must be properly configured within the MARS device administration pages. See the section, Reporting and Mitigation Devices Overview, page 2-1 for information on configuring individual devices to work with MARS.</p>

Table 23-2 provides links and description of related Alert Action configuration procedures. Although some of these procedures are documented elsewhere in this user guide, they are duplicated here for your convenience.

Table 23-2 Alert Notification Procedures

Alert Related Procedures	Description
Configure the E-mail Server Settings	To send Email, SMS, and XML notifications, MARS requires that you configure the E-mail Server settings.
Configure a Rule to Send an Alert Action	Complete this procedure to create or modify an alert action.
Create a New User—Role, Identity, Password, and Notification Information	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
Create a Custom User Group	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.
Add a User to a Custom User Group	Complete this procedure to include a newly created user account into a MARS user group.

Example 23-1 shows a typical email alert notification. Example 23-2 shows an XML notification with its attached XML data file. When compression is configured, the XML data file arrives as a GZIP compressed file.



Note

Alert notifications cannot be customized.

Example 23-1 MARS Notification by Email

```
-----Original Message-----
From: notifier.Latest@serviceprovider.cisco.com [mailto:notifier.MyLatest@cisco.com]
Sent: Monday, May 15, 2006 8:48 AM
To: Naliza Mahda (Nalmah)
Subject: Incident Notification (green, Rule Name: System Rule: CS-MARS Database Partition Usage)
```

The following incident occurred:

```
Start time:      Mon May 15 08:47:26 2006
End time:        Mon May 15 08:47:26 2006
Fired Rule Id:   134473
Fired Rule:      System Rule: CS-MARS Database Partition Usage
Incident Id:     597842933
```

For more details about this incident, please go to:

https://MyLatest/Incidents/IncidentDetails.jsp?Incident_Id=597842933

```

https://MyLatest.cisco.com/Incidents/IncidentDetails.jsp?Incident_Id=597842933
https://10.2.3.7/Incidents/IncidentDetails.jsp?Incident_Id=597842933
https://192.168.1.101/Incidents/IncidentDetails.jsp?Incident_Id=597842933

```

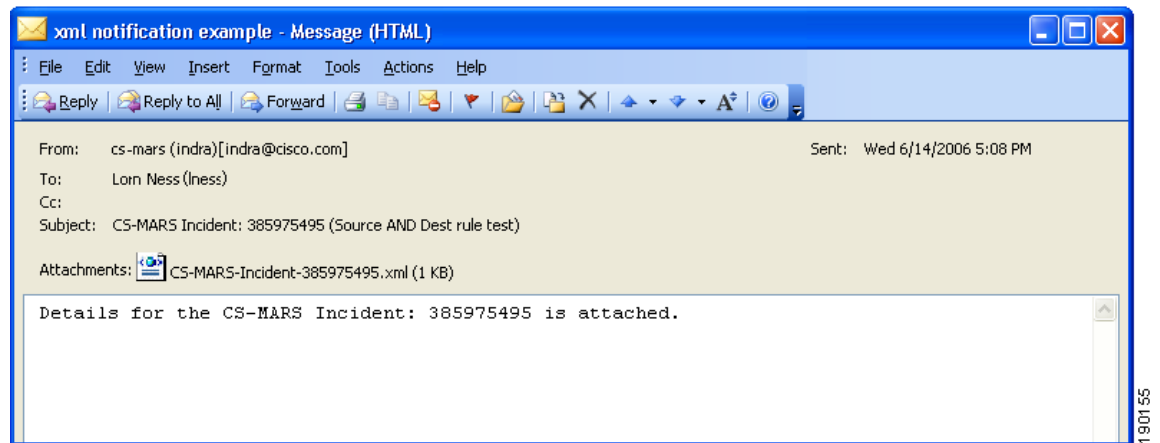
For all recent incidents, please go to:

```

https://MyLatest/Incidents/
https://MyLatest.cisco.com/Incidents/
https://10.2.3.7/Incidents/
https://192.168.1.101/Incidents/

```

Example 23-2 MARS XML Notification Email Attachment



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 23-1](#).

Figure 23-1 MARS Device Configuration Window

CS-MARS Device Config

→ Name: LC20-Doc

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 64.101.176.33 : 25

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

- 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.

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

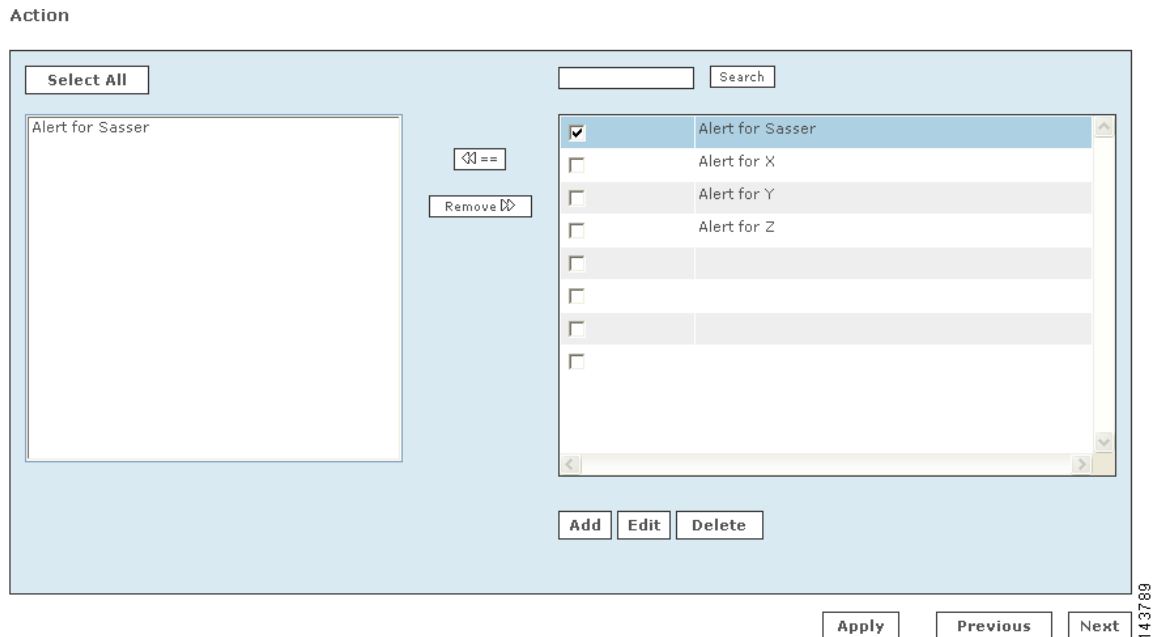
Drop rules do not have Action parameters and cannot trigger alerts.

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 23-2](#), appears below the rule description table. All previously 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 23-2 Action Selection Dialog



Step 3 Do one of the following five actions:

1. Remove an alert action currently applied to the rule.
 - 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.
 - Proceed to Step 13 to complete the procedure.
- Apply an existing alert action to the rule.
 - 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.
 - Proceed to Step 13 to complete the procedure.
- Delete an existing alert action from MARS.
 - Click the check box of the alert action in the right-hand area, then click **Delete**.
A delete verification window appears.
 - Click **Yes**.
The alert action is deleted from the right-hand area.
 - Proceed to Step 13 to complete the procedure.
- Edit an existing alert action.
 - 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 23-3.
 - Proceed to Step 4 to complete the procedure.
- Create a new alert action.
 - Click **Add**.
The Alert recipients page appears in a new window, as shown in Figure 23-3.

- Proceed to Step 4 to complete the procedure.

Figure 23-3 Alert Recipients Window

Name:
 Description:

Email

Syslog

Page

SNMP

SMS

Distributed Threat Mitigation

Alarm Drop Reset
 Deny Attacker Deny Flow

XML Email

Compress

143790

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.

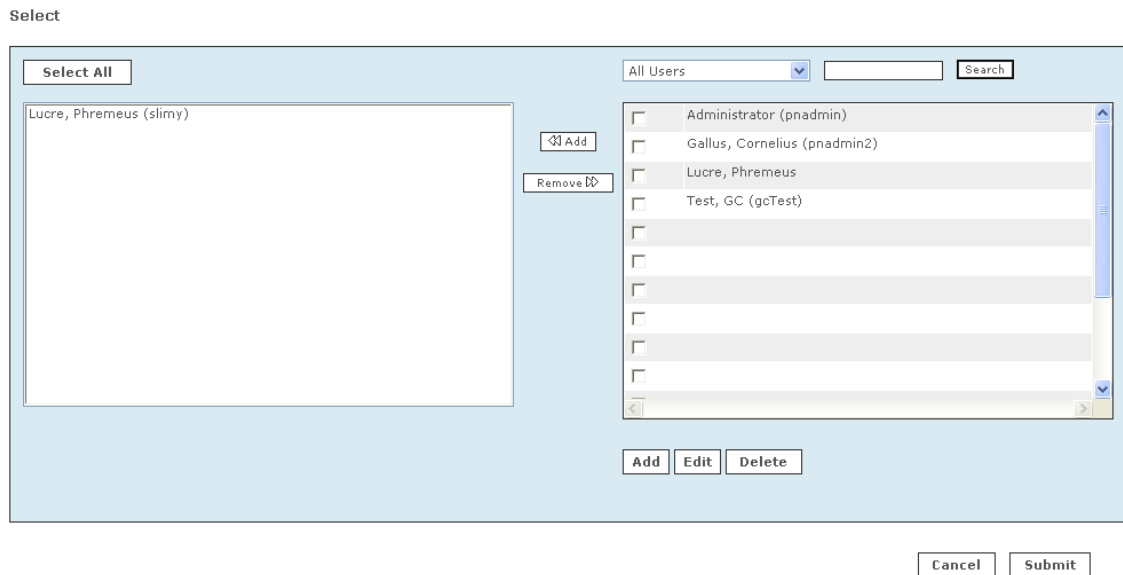
- **XML Email**—Users or groups can receive an email message with incident details appended in an XML data file. Click the **Compress** check box to send the XML data file as a compressed gzip file. For more information on this feature, see [Appendix A, “Cisco Security MARS XML API Reference.”](#)
- **Syslog**—Specified devices can receive syslog messages.
- **SNMP**—Specified devices can receive SNMP trap information.
- **Distributed Threat Mitigation**—Not supported at this time.

**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 23-4](#).

Figure 23-4 Select Recipient Dialog Box



143782

For Syslog and SNMP, the **Select** (device) dialog box appears, as shown in [Figure 23-5](#).

Figure 23-5 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 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 23-6](#).
 - Enter the User Configuration information then click **Submit**.
You are returned to the [Select Recipient Dialog Box](#).
For reference on user configuration fields, see the section, “[Create a New User—Role, Identity, Password, and Notification Information](#)”
 - Add the new user to the recipient list as described in [Step 7](#).
- Step 9** Click **Submit**.
You are returned to the [Alert Recipients Window](#).
- Step 10** Repeat [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 [Action Selection Dialog](#). 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**.

This ends the [Configure a Rule to Send an Alert Action](#) procedure.

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

To create a new MARS user, complete the following steps:

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).

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”](#) section on page 23-5.

The User Configuration page appears, as shown in [Figure 23-6](#).

Figure 23-6 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 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, 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 23-7](#).

Figure 23-7 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** to close the User Configuration page and return to the **User Management** tab.

This ends the [Create a New User—Role, Identity, Password, and Notification Information](#) procedure.

Create a Custom User Group

To create a custom user group in addition to the default groups created by MARS, complete the following procedure:

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.

This ends the [Create a Custom User Group](#) procedure.

Add a User to a Custom User Group

To include a user in a custom User Group, complete the following steps:

**Note**

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

-
- 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.
This ends the [Add a User to a Custom User Group](#) procedure.
-

