



# CHAPTER 10

## Case Management

---

This chapter contains the following topics:

- [Case Management Overview, page 10-1](#)
- [Hide and Display the Case Bar, page 10-3](#)
- [Create a New Case, page 10-5](#)
- [Edit and Change the Current Case, page 10-6](#)
- [Deselecting the Current Case, page 10-6](#)
- [Add Data to a Case, page 10-7](#)
- [Generate and Email a Case Report, page 10-7](#)

## Case Management Overview

The Case Management feature can capture, combine, and preserve user-selected MARS data within a specialized report called a case. The following data can be added to a case:

- Text annotations
- Incident ID page
- Incident device information (source IP address, destination IP address, reporting device)
- Session Information page
- Query Results page
- Build Report page
- Report Results page
- View Case page (the current case can reference another case)

Any user can create or alter any case. You can assign a case to a MARS user on the same machine, and can change the status of a case to assigned, resolved, or closed. The contents of a case are displayed by category on a single GUI page (View Case), and can be automatically assembled into a single HTML case document. You can email the Case Document to any MARS user account or user group.



### Note

---

When a case is closed, you can still email it, annotate it, add device information, and include a reference to another case.

---

Case information collected on incidents, sessions, queries, reports and mitigation logs are forensic evidence pertinent to the following:

- Audits (for example, regulatory compliance audits)
- Justifications for modifying ACLs or policy changes
- Notes for MARS false positive tuning
- Examples of allowed and prohibited behavior.

The case preserves and displays the selected data as it appeared when the data was added to the case, regardless of subsequent changes to the MARS state. For example, MARS data can be purged, topology can change from automatic discoveries or vulnerability scanning, and overall configuration can change when you edit rules or reports, but the data reported in the case remains the same as the time it was captured.



#### Note

As of MARS software version 4.1.1 the Case Management feature replaces the incident escalation feature.

The Case Management homepage is the Cases subtab of the Incidents tab as shown in [Generate and Email a Case Report, page 10-7](#).

**Figure 10-1 Case Management Tab—Local Controller**

The screenshot shows the Cisco MARS Case Management interface. The navigation menu includes SUMMARY, INCIDENTS, QUERY / REPORTS, RULES, MANAGEMENT, ADMIN, and HELP. The INCIDENTS tab is active, and the Cases subtab is selected. A 'Select Case:' dropdown menu is highlighted with a circled '1'. Below it, a table of cases is displayed with columns for Case ID, Status, Owner, Summary, and Created / Updated. The table contains several rows of case data. A circled '2' points to the table headers, and a circled '3' points to the first row of data. At the bottom, there is a pagination control showing '1 to 6 of 6' and '25 per page'.

Case ID	Status	Owner	Summary	Created / Updated
C:1212330	New	Martucci, Francesca (francy)	Confetti Attack	Created: Aug 26, 2005 2:01:43 PM CDT Updated: Aug 28, 2005 4:09:17 PM CDT
C:121284	Closed	Administrator (pnadmin)	New Case	Created: Aug 26, 2005 1:47:39 PM CDT Updated: Aug 26, 2005 1:51:18 PM CDT
C:119753	Assigned	Administrator (pnadmin)	Follow-up	Created: Aug 16, 2005 1:43:06 PM CDT Updated: Aug 30, 2005 12:41:55 PM CDT
C:119662	New	Lundell, Norm (nlundell)	Security Team	Created: Aug 16, 2005 8:52:39 AM CDT Updated: Aug 28, 2005 1:29:44 PM CDT
C:110855	New	Administrator (pnadmin)	New Case	Created: Aug 2, 2005 8:48:16 AM CDT Updated: Aug 30, 2005 9:32:44 AM CDT
C:110320	Assigned	McNutt, Blaine (rbmcnut)	Sample Case for a View	Created: Jul 29, 2005 9:31:15 AM CDT Updated: Aug 2, 2005 8:47:40 AM CDT

1	Case Bar	2	Dropdown Display Filters
3	Individual Cases		

All new, assigned, resolved and closed cases can be accessed from the Cases subtab.

To view the contents of a case, click the Case ID number of a case. The View Case page appears, as shown in [Generate and Email a Case Report, page 10-7](#).

To generate an HTML document of the **View Case** page content that can be emailed, click **View Case Document** at the bottom of the **View Case** page. Graphs and charts plotted from reports are also captured in the Case Document.

Figure 10-2 The View Case Page—Local Controller

**1** → Current Case: C:109418 (Assigned) MARS Defends

**2** → View Case: C:109418

Case ID	Status	Owner	Summary	Created / Updated
C:109418	Assigned	Local: Administrator (pnadmin)	MARS Defends	Created: Aug 16, 2005 11:07:22 AM PDT Updated: Aug 29, 2005 9:50:11 AM PDT

**3** → Case History

User	Action	Comment	Time
Local: Administrator (pnadmin)	Case Opened		Aug 16, 2005 11:07:22 AM PDT
Local: Administrator (pnadmin)	State Changed: Assigned		Aug 16, 2005 11:07:22 AM PDT
Local: Administrator (pnadmin)	Summary Changed	Initial Summary: Case 4 norm	Aug 16, 2005 11:07:22 AM PDT
Local: Administrator (pnadmin)	Owner Changed: Local: Administrator (pnadmin)	Initial Owner: pnadmin	Aug 16, 2005 11:07:22 AM PDT
Local: Administrator (pnadmin)	Priority Changed: Yellow	Initial Priority: Yellow	Aug 16, 2005 11:07:22 AM PDT
Local: Administrator (pnadmin)	Summary Changed	Case 4 norm2	Aug 16, 2005 11:08:04 AM PDT
Local: Administrator (pnadmin)	Comment	c22	Aug 16, 2005 11:08:04 AM PDT
Local: Administrator (pnadmin)	Session Added: S:5458092		Aug 16, 2005 3:12:29 PM PDT
Local: Administrator (pnadmin)	Device Info Added:	3.1.5.5	Aug 16, 2005 3:12:59 PM PDT
Local: Administrator (pnadmin)	Case Referenced: C:108300 (New) New Case1		Aug 16, 2005 3:17:13 PM PDT
Local: Administrator (pnadmin)	Priority Changed: Red		Aug 16, 2005 3:19:22 PM PDT
Local: Administrator (pnadmin)	Report Added: Activity: All - Top Destination Ports (Peak View)		Aug 16, 2005 3:20:32 PM PDT
Local: Administrator (pnadmin)	Summary Changed	MARS Defends	Aug 29, 2005 9:50:11 AM PDT

**4** → Sessions

Display	Session / Incident ID	Events	Source IP/Port	Destination IP/Port	Protocol	Time	Reporting Devices	Path / Mitigation	Tune
<input checked="" type="checkbox"/>	S:5458092, I:5336608@, I:5336612@, I:5336611@, I:5336613@, I:5336610@	Inactive reporting device detected	0.0.0.0	3.1.5.5	N/A	Aug 16, 2005 3:00:02 AM PDT	pluto	N/A	False Positive

Devices

Display	Device
<input type="checkbox"/>	

1	Case Bar—Identifies current case	2	View Case identifier—Shows the attributes of the case
3	Case History—Log of all changes made to the case	4	Summary of data added to the case

## Case Management Considerations for the Global Controller

Case management on the Global Controller differs from the Local Controller implementation as follows:

- Cases are not created on a Global Controller. They can be viewed and modified.
- The Global Controller does not have a Case Bar. All Cases are selected from the Incident -> Cases page.
- The Cases page has an additional dropdown filter to display cases per Local Controller.

## Hide and Display the Case Bar

The Case Bar displays by default. When displayed, the Case Bar appears at the top of each page. The Case Bar must be displayed to create or modify a case.

This section contains the following topics:

- [Hiding the Case Bar, page 10-4](#)
- [Displaying the Case Bar, page 10-4](#)

## Hiding the Case Bar

To hide the Case Bar, follow these steps:

- Step 1** Navigate to the **Cases** subtab (**Incidents > Cases**), as shown in [Figure 10-3](#).

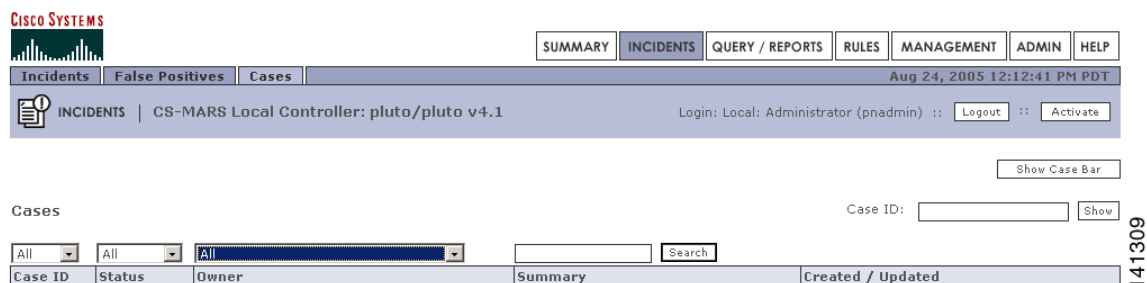
**Figure 10-3** Case Bar Displayed on the Incidents Page



- Step 2** Click **Hide Case Bar**.

The Case Bar no longer appears on all tabs, as shown in [Figure 10-4](#).

**Figure 10-4** Case Bar Hidden on the Incidents Page



## Displaying the Case Bar

To Display the Case Bar, follow these steps:

- Step 1** Navigate to the **Cases** subtab (**Incidents > Cases**) as shown in [Figure 10-4](#).
- Step 2** Click **Show Case Bar**.

The Case Bar, as shown in [Figure 10-3](#) now appears on all pages.

## Create a New Case

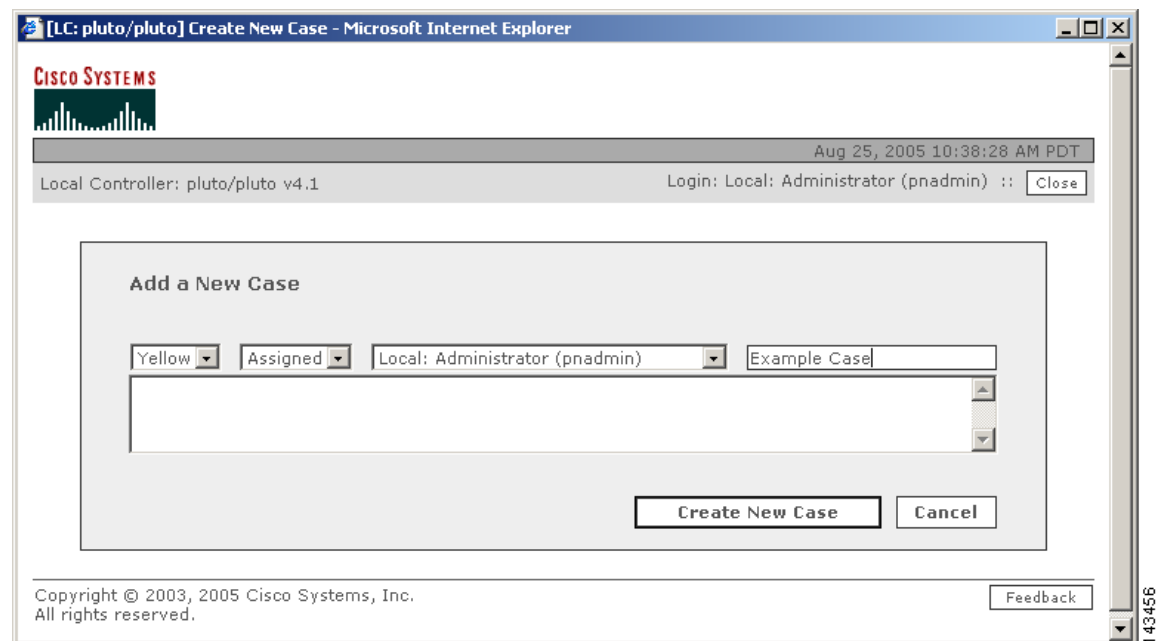
To create a new case, follow these steps:

**Step 1** Display the Case Bar as described in the section [Hide and Display the Case Bar, page 10-3](#).

**Step 2** Click **New Case**.

The Add a New Case Dialog box appears, as shown in [Figure 10-5](#).

**Figure 10-5** Add a New Case Dialog Box



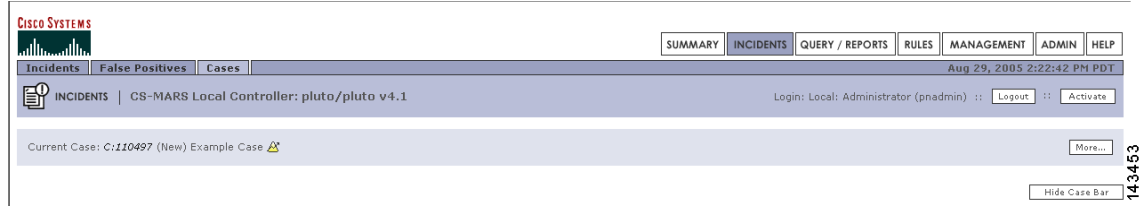
**Step 3** Select a severity color, change the state from new to assigned if appropriate, select the owner, replace the default summary name (default is New Case).

[Figure 10-5](#) shows a case with case summary of Example\_Case, assigned to the administrator with a yellow priority color (default is Green).

**Step 4** Type or paste any annotations into the text space.

**Step 5** Click **Create New Case**.

The newly created case is numbered and becomes the current case displayed in the Case Bar as shown in [Figure 10-6](#).

**Figure 10-6** Case Bar Shows a Newly-Created Case as the Current Case

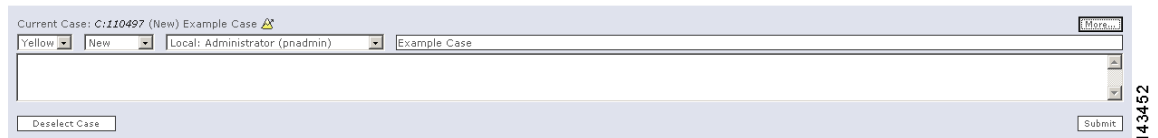
Proceed to the section [Add Data to a Case, page 10-7](#) for steps on how to combine various data into a single case.

## Edit and Change the Current Case

To edit the Current Case, follow these steps:

**Step 1** Display the Case Bar and click **More**.

The Case Bar Expands to expose the editing options, as shown in [Figure 10-7](#). See the section [Hide and Display the Case Bar, page 10-3](#) for procedures to display the case bar.

**Figure 10-7** Expanded Case Bar

**Step 2** Change the severity, status, owner, or summary of the case as required.

**Step 3** Add an annotation in the text box as required.

**Step 4** Click **Submit**.

## Deselecting the Current Case

To replace the Current Case case with another, follow these steps:

**Step 1** Expand the Case Bar as explained in the previous procedure.

**Step 2** Click **Deselect**.

The Case Bar drop-down list displays **No Case Selected...** as shown in [Figure 10-4](#).

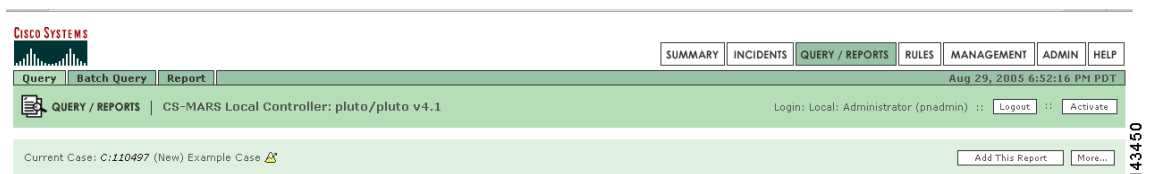
**Step 3** To select a different Current Case, select a case from the Case Bar drop down list.

## Add Data to a Case

To add data to a case, follow these steps:

- Step 1** Select the Current Case. See the section [Edit and Change the Current Case, page 10-6](#) for procedures on selecting the Current Case.
- Step 2** Navigate to the page to be captured in the case. In the example, the Query page is selected.
- Step 3** Click **Add this...** on the Case Bar.

**Figure 10-8 Case Bar Add Button**



- Step 4** To verify that the selected data was added to the case, click the case ID number in the Case Bar to display the View Case page.

In the example shown in [Figure 10-8](#), the selected report should appear in the Reports section of the View Case page. A partial View Case page is shown in [Figure 10-2](#).

## Generate and Email a Case Report

You can generate a case report of the case data and email the report to any MARS user group or individual user account. The email event is logged in the case history listings on the View Case page.

To add a new user account or user group, see [Create a User—Role, Identity, Password, and Notification Information, page 5-13](#).



**Note**

Make sure that the MARS email server is configured. See [Configure the E-mail Server Settings, page 5-7](#) for further information.

To generate a case report and to email it, follow these steps:

- Step 1** Select a case from the Cases page or from the Case Bar dropdown list.
- Step 2** Click the Case ID number to navigate to the **View Case** page.
- Step 3** Click the check box in an item's **Include** field to select or deselect that item for inclusion in the Case Document. By default, all items are selected.

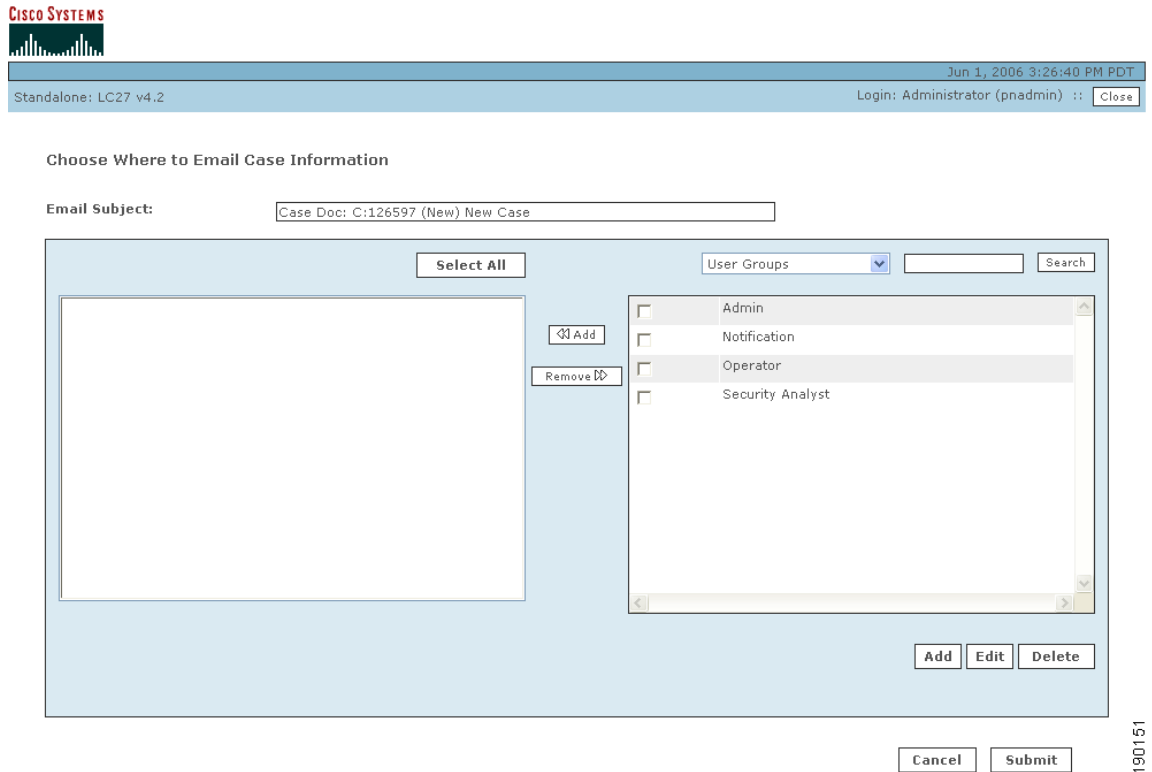


**Tip**

Click **Show Include** to show only those items selected for the Case Document. **Show Include** does not function for cases created in Cisco Security MARS version 4.1.1.

- Step 4** Click **View Case Document** at the bottom of the **View Case** page.  
MARS generates and displays the case report.
- Step 5** Click **Email Case** at the bottom of the report page.  
The Case Email dialog box appears, as shown in [Figure 10-9](#).

**Figure 10-9 Case Management Email Dialog Box**



- Step 6** Click the check box of the user groups or individual users you want to receive the Case Document, then click **<< Add**.



**Tip** Select **All Users** from the dropdown menu to display all individual user accounts.

The selected recipients appear in the left-hand area of the dialog box.

- Step 7** Click **Submit** to send the Case Document to the recipients.  
The email is sent and the case history is updated to show the email event as the latest item of the case history.