CHAPTER 21

Queries and Reports

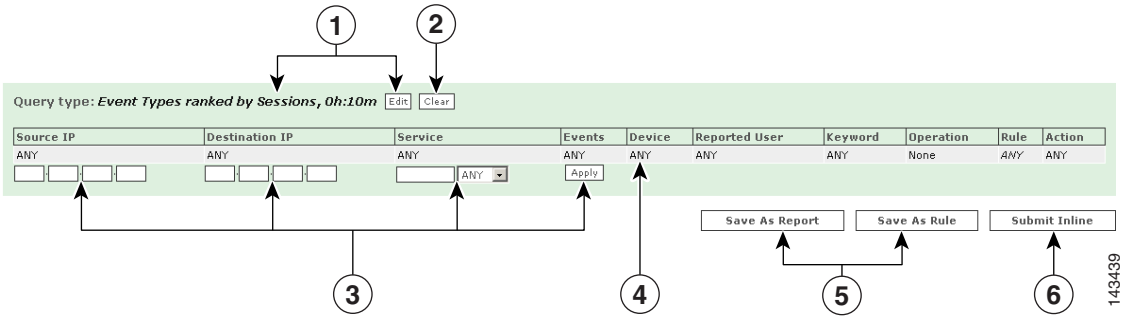
This chapter discusses the following topics:

- Queries
- Viewing Events in Real-time
- Perform a Long-Duration Query Using a Report
- Perform a Batch Query
- Reports

Queries

On the Query page, you can run reports as on-demand queries, or create your own query. Many links from other pages bring you to the query page, which then partially populate the query's criteria. Once you have submitted a query, you can save it as a report or a rule.

Figure 21-1 The Local Controller Query Table



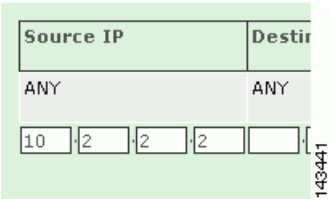
1	Click to set the query type and time range criteria.	**2**	Click **Clear** to return query values to default values.
3	Quick query fields permit entry of values without opening dialog box for the field.	**4**	Click on a field value to open the dialog box for that field.
5	Save the query as a report or as a rule.	**6**	Click **Submit Inline** to run the query**.**

To Run a Quick Query

Step 1 From the **Query** subtab, enter a source IP, destination IP, or a service into the query criteria fields.

Step 2 Click the **Submit Inline** button to run the query.

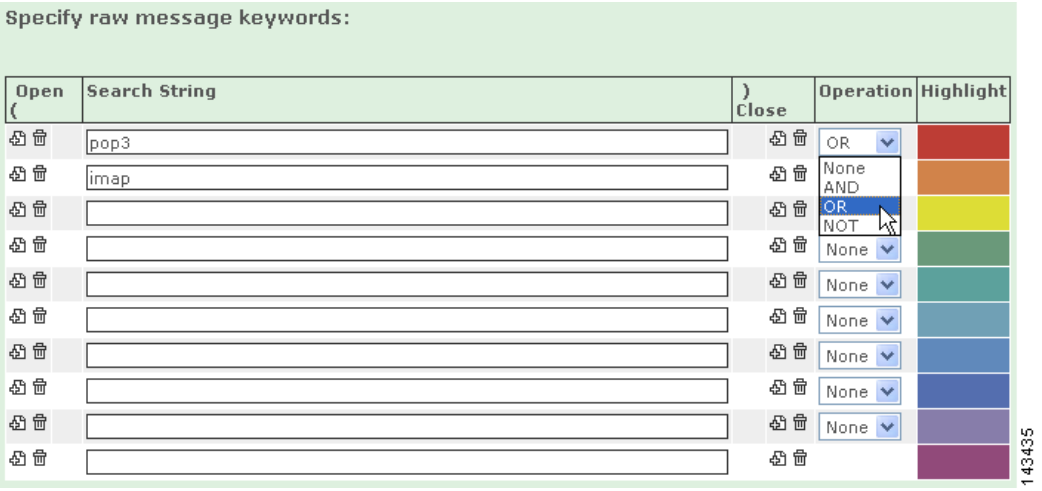
Figure 21-2 Running a Quick Query



To Run a Free-form Query

Step 1 Enter a source IP, destination IP, or a service into the quick query field.

Figure 21-3 Running a free-form query



Step 2 Click the name of the query (**[None]** appears as the name if you have none saved) or Edit to enter the rest of the query. You can also click the parentheses icon ( )to add parentheses for nested queries or click the trash can icon ( ) to remove parentheses.

Step 3 Under Search String enter strings to query; under Operation, select the operation (**AND**, **OR**, **NOT**). For the final item in the list, select **None**.

Step 4 Click the **Apply** button.

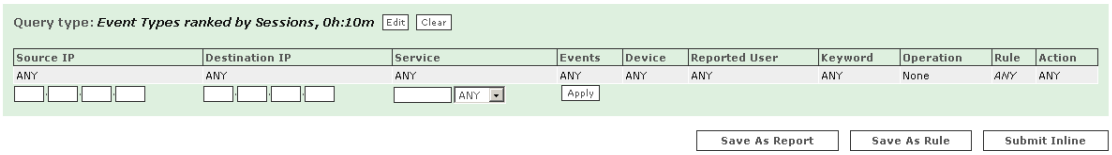
Step 5 Click the **Submit** button to run the query.

Note The free-form query cannot be saved as a rule.

To Run a Batch Query

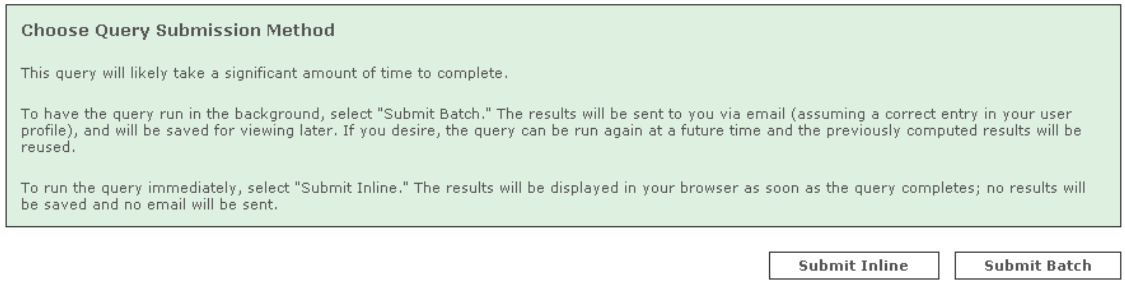
Step 1 Enter your data for either a simple or free-form query. If your query is expected to take a long time to run, instead of **Submit Inline**, you may given the option of having it run as a batch query.

Figure 21-4 Construct a Query to Run in Background (Batch Query)



Step 2 Click **Submit...** to make your selection.

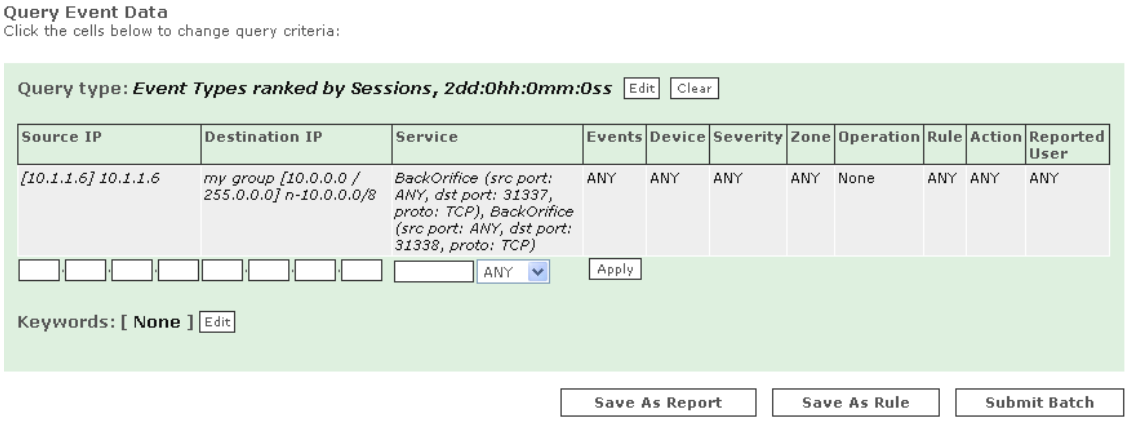
Figure 21-5 Choosing the Query Submission Method



To submit as a standard inline query, click **Submit Inline**.To submit your query as a batch query, click **Submit Batch**. Your query is submitted, and you are automatically taken to the **Batch Query** tab.

If your query is very large, you may only be give the options of **Save as Rule**, **Save as Report**, or **Submit Batch**.

Figure 21-6 Change Query Criteria



To submit your query as a batch query, click **Submit Batch**. Your query is submitted, and you are automatically taken to the **Batch Query** tab.

Figure 21-7 Select Batch Query

Step 3 To watch the status of the query in real-time, you can use the drop-down list to change the **Page Refresh Rate** from **Never** (the default) to 1 minute, 3 minutes, 5 minutes, 10 minutes, 15 minutes, or 30 minutes.

Step 4 To view the results of the batch query as it is running, click **View Results**. This can be done while the query is in progress.

If the email address in your user profile on the MARS is valid, the results of your batch query are emailed to you when the query has completed, and can also be viewed by clicking **QUERY / REPORTS > Batch Query > View Results**.

Note When you click **View Results** while the query is in progress, the results compiled up to that moment are recomputed. This can make the display take longer to appear than after the results are compiled.

To Stop a Batch Query

Step 1 Click **QUERY/REPORTS**, then click the **Batch Query** tab.

Step 2 Click **Stop**. The **Status** of the query changes to **Finished**.

To Resubmit a Batch Query

You can resubmit a batch query if you want to restart it. A resubmitted batch query will use previously computed results, thus resulting in a faster query than one submitted for the first time.

Step 1 Click **QUERY/REPORTS**, then click the **Batch Query** tab.

Step 2 Click **Resubmit**. The **Status** of the query changes to **In Progress**.

To Delete a Batch Query

Step 1 Click **QUERY/REPORTS**, then click the **Batch Query** tab.

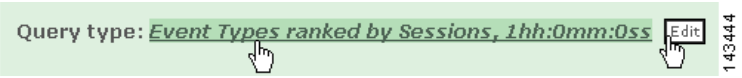
Step 2 Click **Delete**.

Step 3 In the confirmation window, click **Delete** to confirm.

Note You can only see your own batch queries and their results. The batch queries of others and their results are not viewable by you, and your batch queries and their results are not viewable by others.

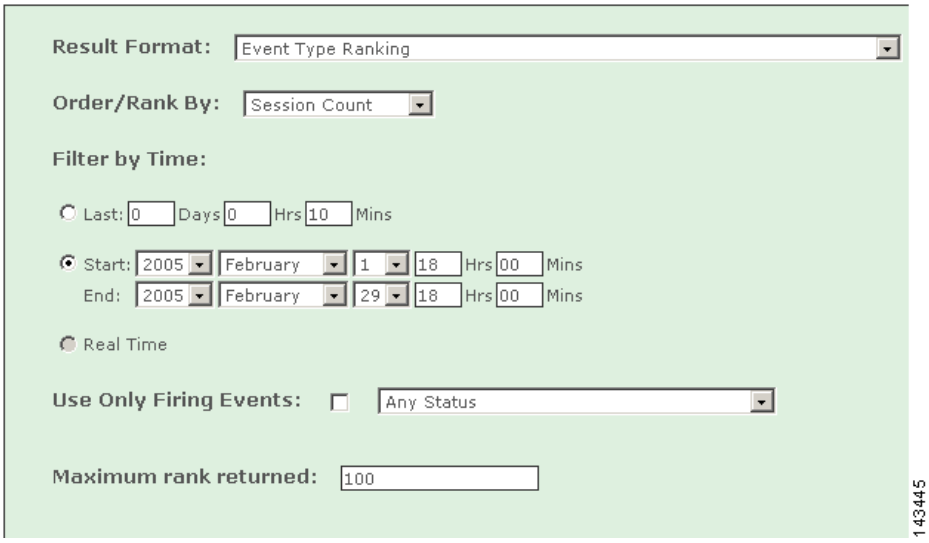
Selecting the Query Type

Figure 21-8 Clicking the Query Type or Edit link



You can select different query criteria by clicking the **Query Type** link or **Edit** button. This lets you determine a query's result format, rank, time, whether it only uses firing events, and the number of rows returned.

Figure 21-9 The Query Criteria: Result Page



Result Format

- *Event Type Ranking*

Returns the most reported event types. Ranked by either: number of sessions containing at least one of the event type or by bytes transmitted in sessions that contain events that meet the query criteria.

- *Event Type Group Ranking*

Returns either pre-defined or user defined grouped event types. Ranked by either: number of sessions containing at least one event type contained in the group or by bytes transmitted in sessions that contain events that meet the query criteria.

- *Source IP Address Ranking*

Returns source IP addresses. Ranked by number of sessions with that source IP address or by bytes transmitted in sessions that contain events that meet the query criteria.

- *Network Ranking*

Returns top networks that exists in MARS. Ranked by either: number of sessions that contain events that meet the query criteria or by bytes transmitted in sessions that contain events that meet the query criteria. If a network is excluded, it is excluded from all results.

- *Network Group Ranking*

Returns top network groups that exists in MARS. Ranked by either: number of sessions that contain events that meet the query criteria or by bytes transmitted in sessions that contain events that meet the query criteria. If a network is excluded, it is excluded from all results.

- *Source Network Ranking*

Returns top source networks that exists in MARS. Ranked by either: number of sessions that contain events that meet the query criteria or by bytes transmitted in sessions that contain events that meet the query criteria. If a network is excluded, it is excluded from all results.

- *Source Network Group Ranking*

Returns top source network groups that exists in MARS. Ranked by either: number of sessions that contain events that meet the query criteria or by bytes transmitted in sessions that contain events that meet the query criteria. If a network is excluded, it is excluded from all results.

- *Destination Network Ranking*

Returns top destination networks that exists in MARS. Ranked by either: number of sessions that contain events that meet the query criteria or by bytes transmitted in sessions that contain events that meet the query criteria. If a network is excluded, it is excluded from all results.

- *Destination Network Group Ranking*

Returns top destination network groups that exists in MARS. Ranked by either: number of sessions that contain events that meet the query criteria or by bytes transmitted in sessions that contain events that meet the query criteria. If a network is excluded, it is excluded from all results.

- *Destination IP Address Ranking*

Returns destination IP addresses. Ranked by either: number of sessions with that destination IP address or by bytes transmitted in sessions that contain events that meet the query criteria.

- *Source Port Ranking*

Returns source ports. Ranked by either: number of sessions with that source port or by bytes transmitted in sessions that contain events that meet the query criteria.

- *Destination Port Ranking*

Returns destination ports. Ranked by either: number of sessions with that destination port or by bytes transmitted in sessions that contain events that meet the query criteria.

- *Protocol Ranking*

Returns most used protocols. Ranked by either: number of sessions with that protocol or by bytes transmitted in sessions that contain events that meet the query criteria.

- *Reporting Device Ranking*

Returns most active reporting devices. Ranked by either: number of sessions that contain events from the device or by bytes transmitted in sessions that contain events that meet the query criteria.

- *Reporting Device Type Ranking*

Returns most active reporting device types. Ranked by either: number of sessions that contain events from a device of that type or by bytes transmitted in sessions that contain events that meet the query criteria.

- *Reported User Ranking*

Returns information about users from reporting devices such as: Windows clients, Solaris clients, etc. Ranked by either: number of sessions that contain events from a reported user or by bytes transmitted in sessions that contain events that meet the query criteria.

- *Matched Rule Ranking*

Returns top firing rules. Ranked by number of incidents.

- *Matched Incident Ranking*

Returns incidents. Ranked by either: number of sessions that contain events that meet the criteria that contributed to the incident or by bytes transmitted real time in sessions that contain events that meet the query criteria.

- *All Matching Sessions*

Returns all sessions that contain events that meet the criteria. Sessions that contain a common set of event types are grouped together. They are also sub-grouped by session source IP address and session destination IP address. Sessions in the same sub-group are ordered by time. Real Time results are available for this Result Type.

- *All Matching Events*

Returns events. Ranked by time with the most current first. Real Time results are available for this Result Type.

- *All Matching Event Raw Messages*

Returns the raw messages associated with events. Ranked by time with the most current first. Real Time results are available for this Result Type.

- *NAT Connection Report*

Returns NAT connections. Ranked by time with the most current first.

- *MAC Address Report*

Returns MAC addresses. Ranked by time with the most current first.

- *Unknown Event Report*

Returns events that are not fully processed by the MARS. In some cases, event information such as the five tuple (source IP, source port, destination IP, destination port, and protocol) might not be present, hence can not be queried in real time.

Order/Rank By

This selection determines the ranking or order of the query's results. These selections are determined by the kind of Result Format that you use when you run the query.

- *Session Count*

The number of sessions that contain events that meet the criteria that contributed to the incident.

- *Bytes Transmitted*

The number of bytes transmitted in sessions that contain events that meet the query criteria.

- *Time*

Most current results appear first.

- *Incident Count*

Largest number of incidents appear first.

Filter By Time

- *Last*

The present time minus the number of days, hours, and minutes entered.

- *Start/End*

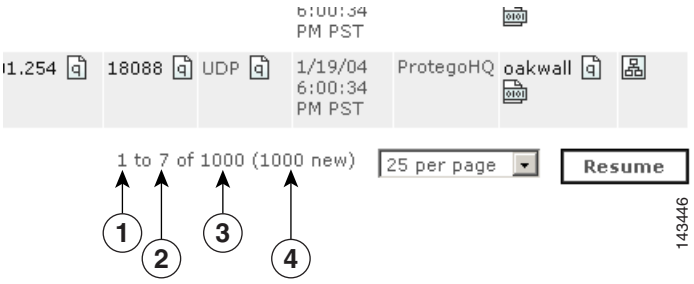
Absolute literal time ranges defined by the date to the minute.

- *Real Time*

Streams rolling real-time results from recent past to current time. Result Formats that work in real time are: •All Matching Sessions, page 21-7, •All Matching Events, page 21-7, and •All Matching Event Raw Messages, page 21-7.

Real Time results appear in a normal browser window. Moving the scroll bar stops the "rolling" behavior. Clicking the Resume button on the bottom of the page allows the scrolling to resume.

Figure 21-10 Click the Resume Button to Start the Page Rolling



1	Top row visible	**2**	Bottom row visible
3	Total rows queried since start	**4**	Number of new queries pulled when this page last refreshed per the **Page Refresh Rate** setting on the **Query/Reports > Batch Query** page.

Use Only Firing Events

Select this if you want only events that fired incidents to return information.

Maximum Number of Rows Returned

Select the number of rows that you want displayed.

Selecting Query Criteria

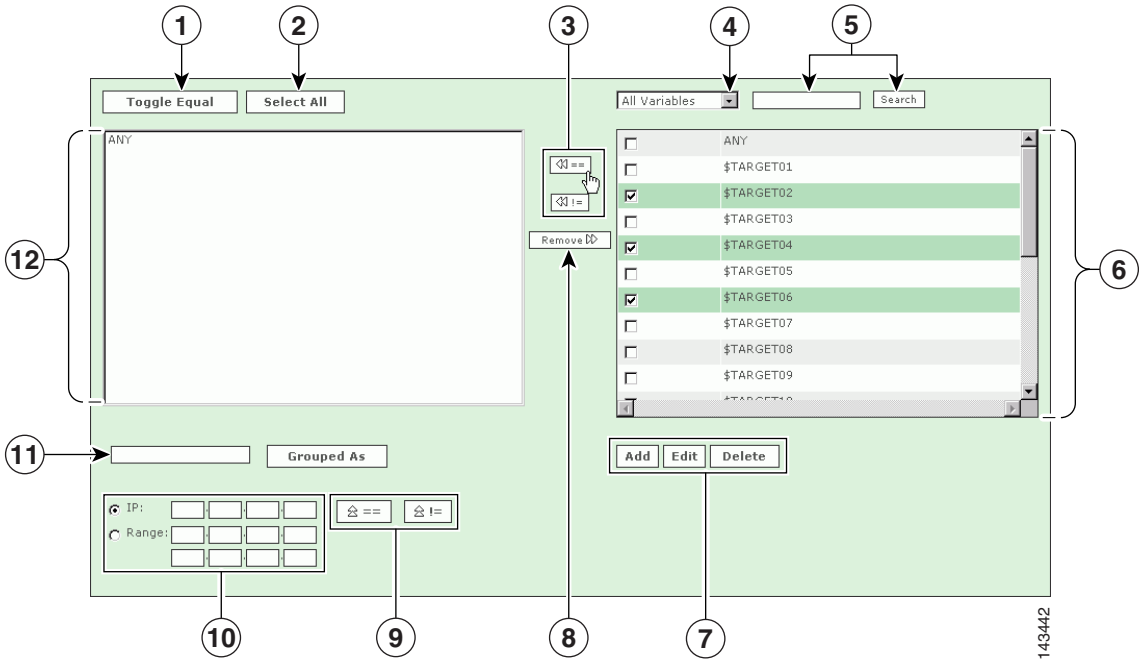
To Select a Criterion

Step 1 Select the criteria that you want to edit by clicking it.

Figure 21-11 Clicking any to narrow your criteria

Step 2 Move the items that you want to query from the right to the left of the filter by selecting the check box next to them, and clicking the Equal and Not Equal buttons.

Figure 21-12 Selecting Variables



Step 3 You can select a variety of different variables, events, devices, addresses from the filter page. The following number correspond with the numbers in the preceding graphic:

1. Check the boxes next to the items in the **Sources Selected** field to select them, and click the **Toggle Equal** button to change them between equal and not equal.
2. Click the **Select All** button to select all items in the **Sources Selected** field. (Note: if you have items highlighted in the Sources Selected field, clicking **Select All** will de-select them.)
3. Use the **Equal** and **Not Equal** buttons to bring highlighted items from the **Sources Available** field into the **Sources Selected** field.
4. Filter sources from this drop-down list.

5. Enter search text, and click **Search** to move items that match the search criteria from the **Sources Available** field to the **Sources Selected** field.
6. To add a new item to the sources, click the **Add** button. To edit or delete an existing source, click the **Edit** or **Delete** button. See IP Management, page 24-3 for more information.
7. Click an item or items in the Sources Selected field, and use the **Remove** button.
8. To move IP values up into the Sources Selected field, click the **Equal** (Up) icon, or the **Not Equal** (Up) icon.
9. Check the radio button next to **IP** or **Range**, and enter an IP address or a range of IP addresses into their respective fields.
10. Select items in the Sources Selected field by clicking them. Enter a group name, and click the **Grouped As** button to group them.
11. Once you have chosen the query criteria that interests you, click **Apply** to return to the Query page.

Repeat this selection process for other query data.

Step 4 Click the **Submit** button to run the query.

Query Criteria

The following list describes the selections in the Query Event Data table.

Source IP

- *Pre NAT source addresses*

Specifies that the constraints entered are the session endpoints.

- *Post NAT source addresses*

Specifies that the constraints entered are the source as appearing at the destination.

- *ANY*

No constraint is placed on the source IP addresses.

- *Variables*

Signify any one IP address, only useful for queries in tandem with the same variable.

- *IP addresses*

IP addresses present on devices in the system or user entered dotted quads.

- *IP ranges*

The range of addresses between two dotted quads.

- *Networks*

Topologically valid networks.

- *Devices*

The hosts and reporting devices present in the system.

Destination IP

- *Post NAT destination addresses*

Specifies that the constraints entered are the session endpoints.

- *Pre NAT destination addresses*

Specifies that the constraints entered are the destination as appearing at the source.

- *ANY*

No constraint is placed on the source IP addresses.

- *Variables*

Any one IP address, only useful for queries in tandem with the same variable.

- *IP addresses*

IP addresses present on devices in the system or user entered dotted quads.

- *IP ranges*

The range of addresses between two dotted quads.

- *Networks*

Topologically valid networks.

- *Devices*

The hosts and reporting devices present in the system.

Service

- *ANY*

No constraint is placed on the source or destination ports or protocol.

- *Service variables*

Any one set of destination port and protocol, only useful for queries in tandem with the same variable.

- *Defined services*

Services on the database.

Event Types

- *ANY*

No constraint on the event type.

- *Event types*

Events that have been merged into types.

- *Event type groups*

Groups of event types.

Device

- *Devices*

The reporting devices present in the system. This restricts the query to a subset of the devices that report to the MARS.

Severity/Zone

- *ANY*

No constraint on the event type severity.

- *Green*

Low-severity events

- *Yellow*

Medium-severity events

- *Red*

High-severity events

- *Zone*

Events reported by devices in the indicated zone.

Operation

- *None*

Defines a single-line query.

- *AND*

Boolean “and” that defines a two or more line query.

- *OR*

Boolean “or” that defines a two or more line query.

- *FOLLOWED-BY*

Time conditional query (e.g.: Y must happen after X) that defines a two or more line query.

Rule

- *Empty field – Rules Chosen field*

When this field is empty, it acts like an ANY selection. No constraint is placed on the sub-set of events.

- *Rule*

Restricts the query to the sub-set of events that contributed to the incidents of the specified rules firing.

Action

- *Empty field – Empty Actions Chosen field*

When this field is empty, it acts like an ANY selection. No constraint is placed on the sub-set of events.

- *Actions*

Restricts the query to the sub-set of events that contributed to the incidents of rules that have the specified notifications as part of their actions. (See Table 22-1Rule Fields and Arguments, page 22-6 for more information.)

Saving the Query

You can save query criteria to re-use as reports or rules.

To save a query as a report

This takes the query that you are using and creates a report. For more information on creating reports, see Reports, page 21-23.

To save a query as a rule

This takes the query to the rules page, populating the rules with the selected query criteria. Likely, you must identify additional criteria to complete the rule. For more information on creating rules, see Rules, page 22-1.

Viewing Events in Real-time

The Real-time Event viewer is a query option that permits you to view real-time events as follows:

- View raw events as they stream to MARS before they are sessionized, with a maximum 5-second delay
- View a sessionized event stream—more delay is possible when there are many events in a session

The real-time events display as a continuously scrolling screen. You can configure query criteria to filter what is displayed. When viewing raw events, sessionization is not impeded, all the parsed raw events are sessionized per normal MARS operation. MARS.

The Real-time Event viewer is available for the following query result formats that support ranking by time (**Order/Rank** field set to **Time**):

- Matched Incident Ranking
- All Matching Sessions
- All Matching Sessions, Custom Columns
- All Matching Events
- All Matching Event Raw Messages
- NAT Connection Report
- MAC Addresses Report
- Unknown Event Report
- Detailed NAC Report

Restrictions for Real-time Event Viewer

The Real-time Event Viewer is available only for Local Controllers.

Real-time event queries should be made *only* from a browser instance that was used to login to MARS. The real-time query will not have reliable results if it is executed from a browser instance spawned from the original login instance (for example, a new browser window launched with **Ctrl+N**, **File>New>New Window**, or **right-click** {link on MARS GUI}>**Open in New Window**).

Multiple real-time queries can operate in multiple browser instances at the same time, but you *must* login to MARS with each browser instance. MARS allocates 1GB of shared buffer for incoming events per query instance. The following restrictions for simultaneous Real-time Event Viewer sessions exist for the specified model:

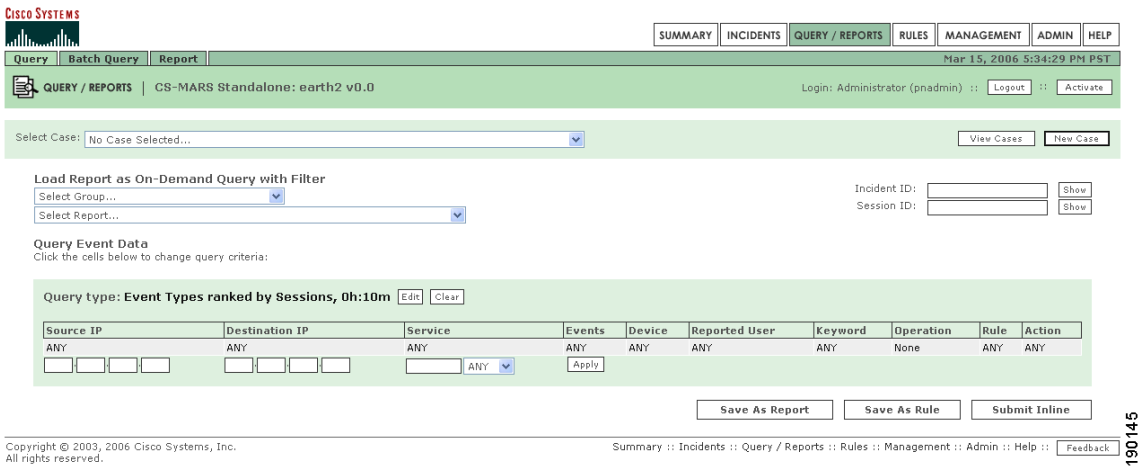
- MARS 20R is limited to 1 Event Viewer
- MARS 20 is limited to 2 Event Viewers
- MARS 50 is limited to 3 Event Viewers
- MARS 100, 100e, 200, 110, 110R, and 210 are limited to 5 Event Viewers

Procedure for Invoking the Real-Time Event Viewer

To invoke the real-time event viewer, complete the following steps:

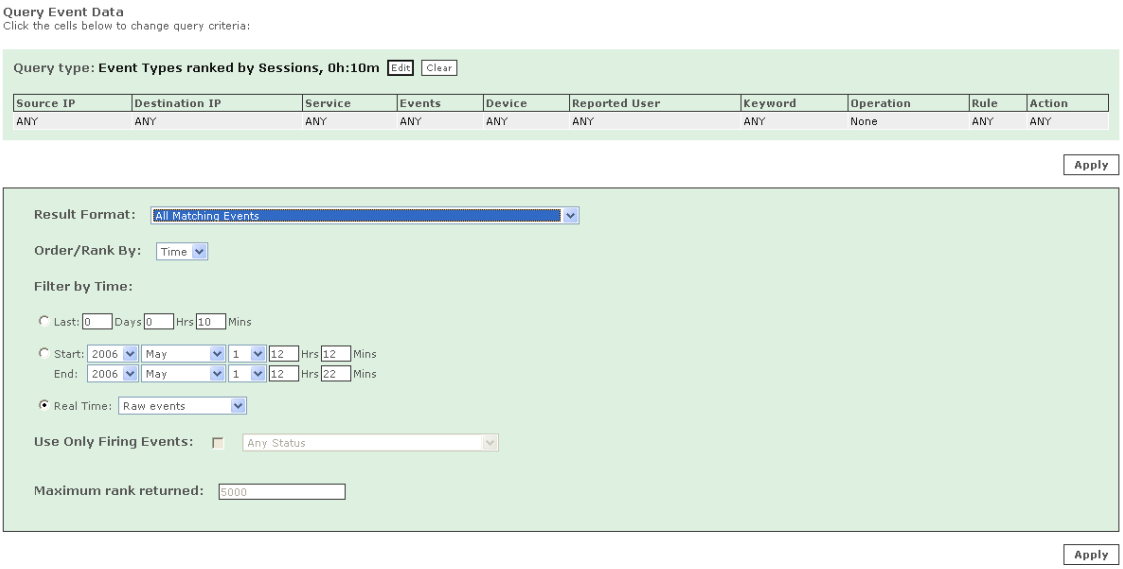
Step 1 Navigate to the **Query** home page as shown in Figure 21-13.

Figure 21-13 Query Home Page



Step 2 Click **Edit**. The Query edit dialog appears, as shown in Figure 21-14.

Figure 21-14 Configuring Real-Time Event Viewer Query



Step 3 Do the following substeps:

a. From the **Result Format** dropdown list, select a format that can be ranked by time.

The formerly grayed-out **Real Time** radio button becomes clickable.

b. Click the **Real Time** radio button, and select **Raw events** or **Sessionized Events** from the dropdown list.

Only **All Marching Events**, and **All Matching Events Raw Messages** have the **Raw events** option.

All Matching Events with **Raw events** displays Event ID, Event Type, Source IP/Port, Destination IP/Port, Protocol Time, and Reporting Device fields.

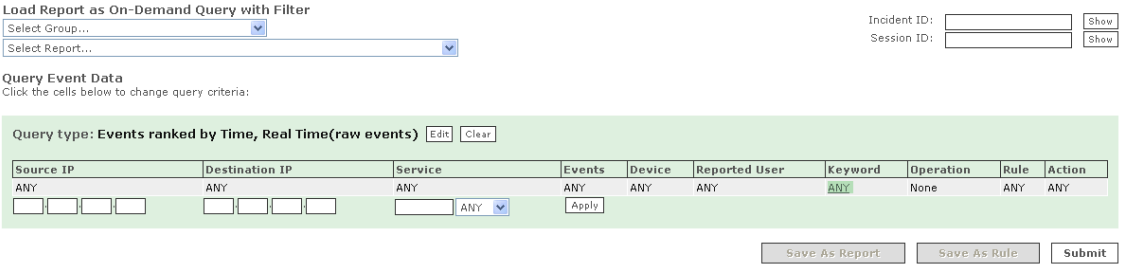
All Matching Events Raw Messages with **Raw events** displays Event ID, Event Type, Time, Reporting Device, and Raw Message fields.

A Result Format with the **Sessionized Events** option displays Event/Session/Incident ID, Event Type, Source IP/Port, Destination IP/Port, Protocol, Time, Reporting Device, Path/Mitigation, and Tune fields.

c. Click **Apply**.

The Query Event Data screen appears with the **Save as Report** and **Save as Rule** buttons gray and inactive, as shown in Figure 21-15.

Figure 21-15 Real-Time Event Query to Submit



Step 4 Modify the parameters of the Query Event Data filter as you require and click **Submit**.

Note The Operation, Rule, and Action parameters of the Query Event Data filter do not function for the real-time event viewer.

Real-time results begin to scroll up from the bottom of the page within 5 seconds, as shown in Figure 21-16. Real-time raw events are shown in this example.

Figure 21-16 View of Events in Real-Time

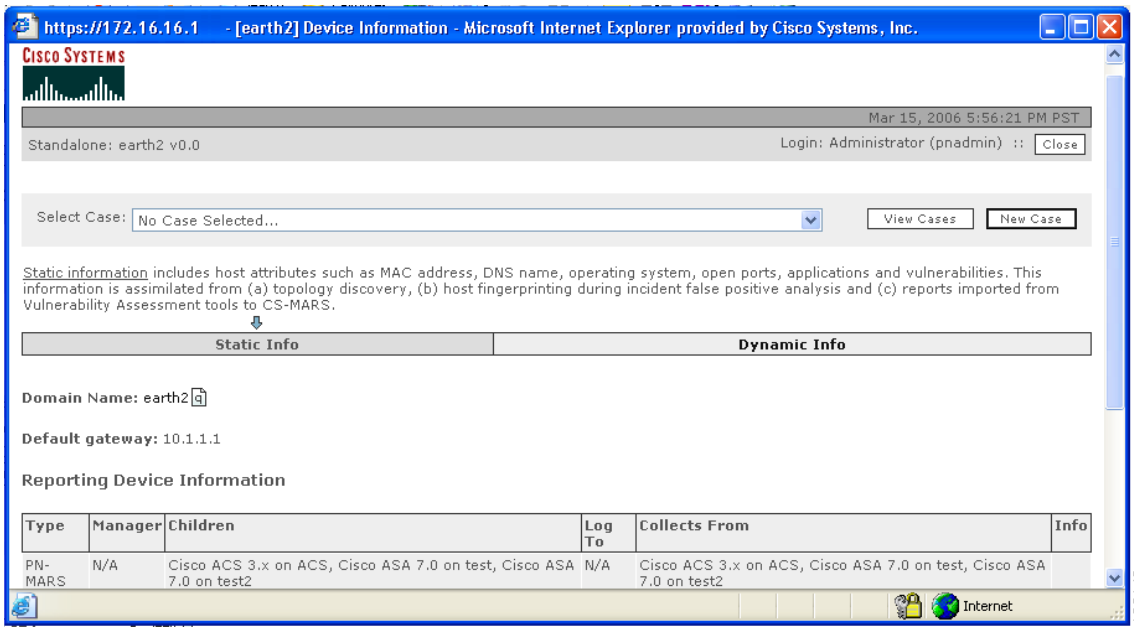
The Real-time event viewer display is governed by the following controls:

- **Scroll Speed**—Select one of four scrolling rates.
- **Pause** button—Suspends the scrolling display.
- **Restart** button—Restarts the display from the current time. This button appears when you pause the scrolling display.
- **Resume** button**—**Restarts the display from the time when paused. This button appears when you pause the scrolling display.
- **Clear**—Terminates the real-time query.

Note Clicking Pause, Resume or setting Scroll Speed are GUI actions that do not reset the MARS GUI timeout interval. These actions will not prevent the GUI from timing out.

Step 5 Click the active links within a real-time event record to view the related pop-up windows. For example, the Reporting Device Information pop-up window is shown in Figure 21-17.

Figure 21-17 Reporting Device Information Pop-up Window



Should errors occur during the display of events, a message box appears, as shown in Figure 21-18.

Figure 21-18 Real-time Event Viewer Error Message

Click **OK** to clear the message box, and restart the Real-time event viewer by clicking **Submit**.

Tip To view the most recent real-time events, you can click **Submit** at any time, or **Pause** and **Restart** to reinitialize the Real-Time Event Viewer. The most recent events are always at the bottom of the output queue, and their freshness when you view them is limited by the number of events in the queue and the scroll speed of the display.

This ends the Procedure for Invoking the Real-Time Event Viewer.

Perform a Long-Duration Query Using a Report

This section explains how to create and view a long-duration query on the MARS. There are two ways to perform a long-duration query on the MARS:

1. **Modifying an existing report.**

Advantages:

- The report is compiled relatively quickly.
- You can compile data gathered over a longer time period

Disadvantage.

This type of query can only be used without any changes to query criteria other than time range, and can only be used with the following reports:

- Activity: All - Top Destination Ports
- Activity: All - Top Destinations
- Activity: All - Top Event Types
- Activity: All - Top Reporting Devices
- Activity: All - Top Sources
- Activity: Attacks Seen - Top Reporting Devices
- Activity: Denies - Top Destination Ports
- Activity: P2P Filesharing/Chat - Top Event Types
- Activity: Scans - Top Destination Ports
- Activity: Scans - Top Destinations
- Activity: Unknown Events - All Events
- Activity: Web Usage - Top Destinations by Sessions
- Activity: Web Usage - Top Sources
- Attacks: All - Top Rules Fired
- Attacks: All - Top Sources

2. **Performing a batch query.**

Advantages:

- You can modify any of the query criteria.
- Best suited for data that spans a short time period.

Disadvantages

- This type of query can be slow and may take a substantial amount of time to complete.
- Only Admin users can perform a batch query.

If you want to observe activity on your MARS over a long period, you can change the duration of time over an existing report that runs on a regular basis, such as hourly or daily, whether they are shipped with the MARS or created by you.

Note Trying to run a long-duration query using a report that only runs “on demand” has the same effect as running a query; it can take just as long because it has to compile data, whereas data from the regularly-run reports has been precompiled on an ongoing basis.

To query using a report, follow these steps:

Step 1 In the **QUERY / REPORTS** tab, click the **Reports** tab to obtain the Main Report window.

Figure 21-19 Main Report Window

Report Selection

	Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
○	Activity: All - NAT Connections	Run on demand only	Normal	None	Query Type: NAT connections ranked by Time Time: May 1, 2004 8:21:50 PM PDT - Jun 6, 2004 8:31:50 PM PDT	This report lists Network Address Translations performed on non-denied sessions as reported to MARS.	Finished: Jun 16, 2004 4:40:36 AM PDT	Jun 15, 2004 8:32:09 PM PDT	May 1, 2004 8:21:50 PM PDT - Jun 6, 2004 8:31:50 PM PDT
○	Activity: All - Top Destination Ports	Run on demand only	Trend	None	Query Type: Destination Ports ranked by Sessions Time: 1hh:0mm:0ss	This report ranks the UDP and TCP destination ports of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.	Finished: Jun 10, 2004 4:17:02 PM PDT	Jun 10, 2004 4:16:58 PM PDT	Jun 10, 2004 3:16:58 PM PDT - Jun 10, 2004 4:16:58 PM PDT
◉	Activity: All - Top Destinations	Every hour	Normal	None	Query Type: Destination IPs ranked by Sessions Time: 28ww:4dd:0hh:10mm:0ss	This report ranks the session destinations of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.	Finished: Jun 17, 2004 2:15:52 PM PDT	Jun 17, 2004 2:15:52 PM PDT	Nov 30, 2003 1:05:52 PM PST - Jun 17, 2004 2:15:52 PM PDT

143798

Step 2 Navigate to and then click the radio button next to the regularly-scheduled report you want to modify (in this example, we use **Activity: All - Top Destinations**). Click the **Query** column to edit the report. The Build Report window appears.

Figure 21-20 Build Report window

Build Report
Click the cells below to define the report:

Name	Schedule	Format	Recipients	Query	Description	Status	Submitted	Time Range
Activity: All - Top Destinations	Every hour	Normal	None	Query Type: Destination IPs ranked by Sessions Time: 28ww:4dd:0hh:10mm:0ss	This report ranks the session destinations of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.	Finished: Jun 16, 2004 7:15:42 PM PDT	Jun 16, 2004 7:15:42 PM PDT	Nov 29, 2003 6:05:42 PM PST - Jun 16, 2004 7:15:42 PM PDT

Submit Previous Next

Time Range:

◉ Last: 200 Days 0 Hrs 10 Mins

○ Start: 2004 June 16 19 Hrs 42 Mins
End: 2004 June 16 19 Hrs 52 Mins

Submit Previous Next

143686

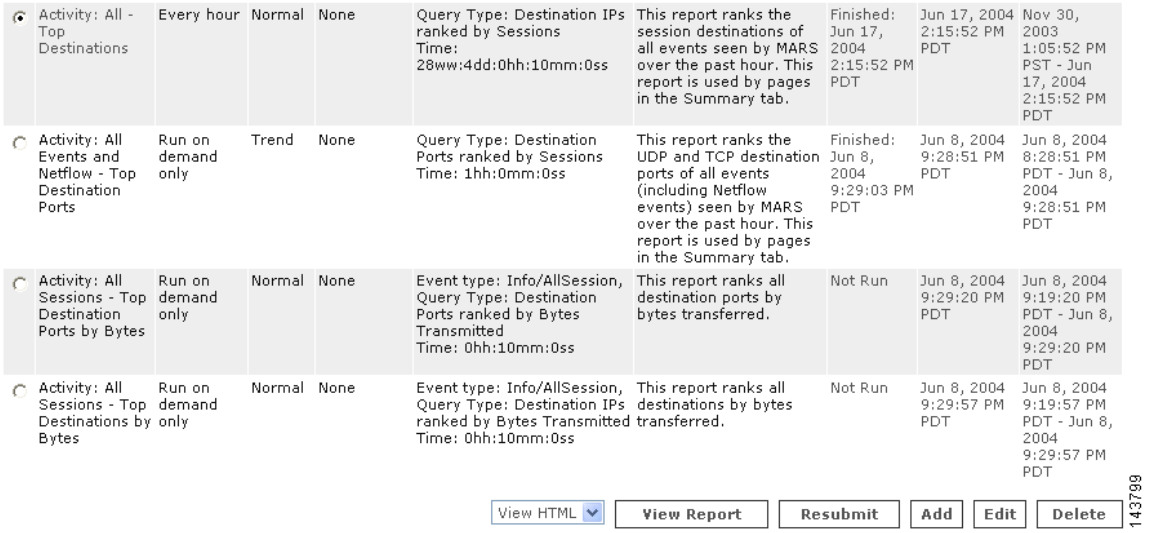
Step 3 In the lower portion of the Build Report window, change the **Time Range** the report (**Activity: All - Top Destinations**) covers to the duration you want it to cover.

Step 4 Click the **Submit** button to run the report and return to the Main Report window.

View a Query Result in the Report Tab

To view a query in the Report tab, follow these steps:

Figure 21-21 Main Report window (bottom)



Activity: All - Top Destinations	Every hour	Normal	None	Query Type: Destination IPs ranked by Sessions Time: 28ww:4dd:0hh:10mm:0ss	This report ranks the session destinations of all events seen by MARS over the past hour. This report is used by pages in the Summary tab.	Finished: Jun 17, 2004 2:15:52 PM PDT	Jun 17, 2004 2:15:52 PM PDT	Nov 30, 2003 1:05:52 PM PST - Jun 17, 2004 2:15:52 PM PDT
Activity: All Events and Netflow - Top Destination Ports	Run on demand only	Trend	None	Query Type: Destination Ports ranked by Sessions Time: 1hh:0mm:0ss	This report ranks the UDP and TCP destination ports of all events (including Netflow events) seen by MARS over the past hour. This report is used by pages in the Summary tab.	Finished: Jun 8, 2004 9:29:03 PM PDT	Jun 8, 2004 9:28:51 PM PDT	Jun 8, 2004 8:28:51 PM PDT - Jun 8, 2004 9:28:51 PM PDT
Activity: All Sessions - Top Destination Ports by Bytes	Run on demand only	Normal	None	Event type: Info/AllSession, Query Type: Destination Ports ranked by Bytes Transmitted Time: 0hh:10mm:0ss	This report ranks all destination ports by bytes transferred.	Not Run	Jun 8, 2004 9:29:20 PM PDT	Jun 8, 2004 9:19:20 PM PDT - Jun 8, 2004 9:29:20 PM PDT
Activity: All Sessions - Top Destinations by Bytes	Run on demand only	Normal	None	Event type: Info/AllSession, Query Type: Destination IPs ranked by Bytes Transmitted Time: 0hh:10mm:0ss	This report ranks all destinations by bytes transferred.	Not Run	Jun 8, 2004 9:29:57 PM PDT	Jun 8, 2004 9:19:57 PM PDT - Jun 8, 2004 9:29:57 PM PDT

Step 1 At the bottom of the Main Report window, click the radio button next to the report (**Activity: All - Top Destinations**).

Step 2 From the drop-down list on the bottom of the Reports page, select either:

- **View HTML**: to view the report as an HTML file.
- **View CSV**: to view the report as a CSV (comma-separated values) file.

Step 3 Click the **View Report** button.

Note The **Status** column shows the percent completion of the report. You can view a partially-completed report, but it might not contain the data you require. The **Status** column updates when the page refreshes per the **Page Refresh Rate** setting on the **Query/Reports > Batch Query** page.

Note In general, do not use the browser refresh or other browser navigation buttons with the MARS Appliance GUI.

Perform a Batch Query

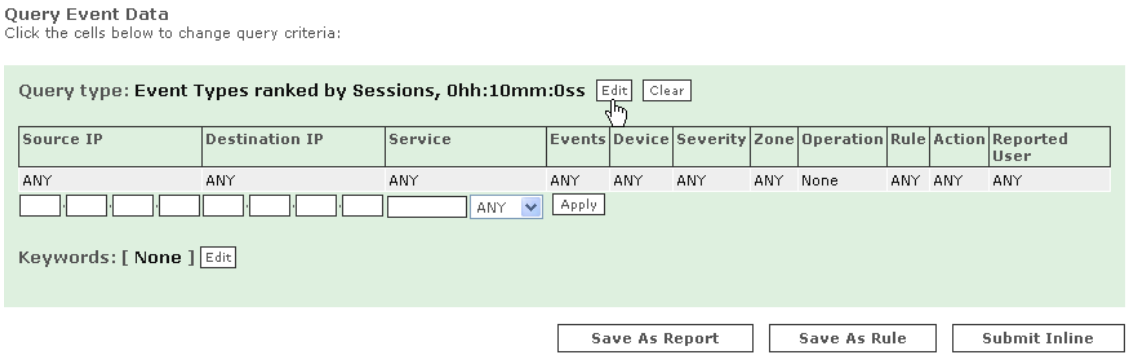
This type of long-duration query can take a long time to perform and is more suitable for a shorter duration of time.

Note Only Admin users can perform a batch query.

To perform a batch query, follow these steps:

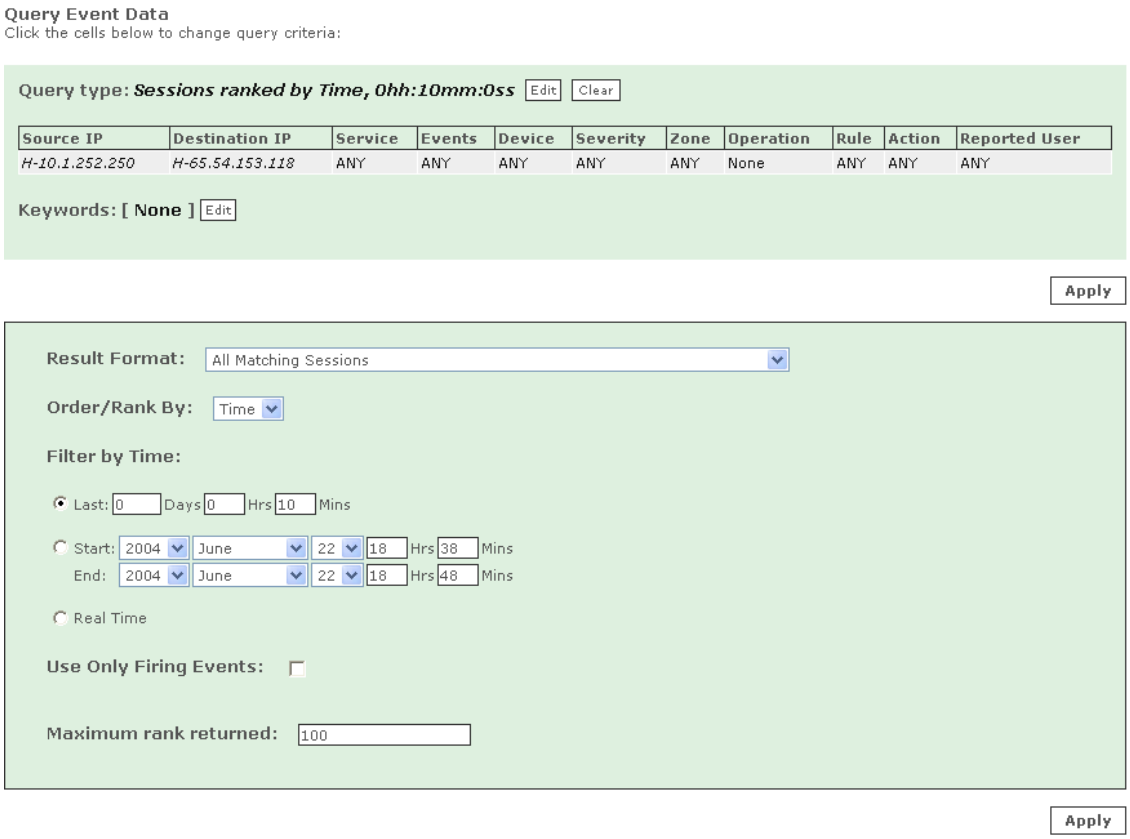
Step 1 Click the **QUERY / REPORTS > Query** tab. The Query window appears.

Figure 21-22 Query window



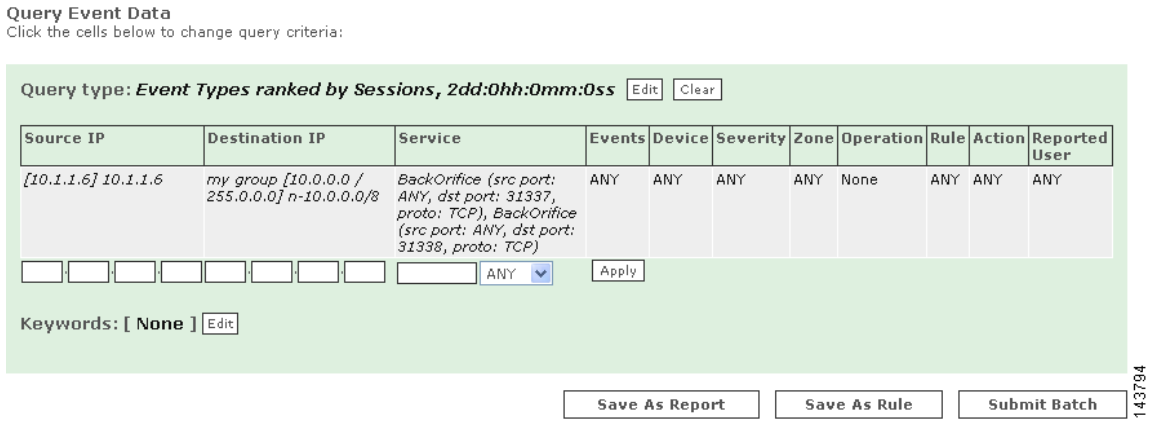
Step 2 In the Query window, click the **Edit** button to change the query criteria. The Query Event Data window appears.

Figure 21-23 Query Event Data window



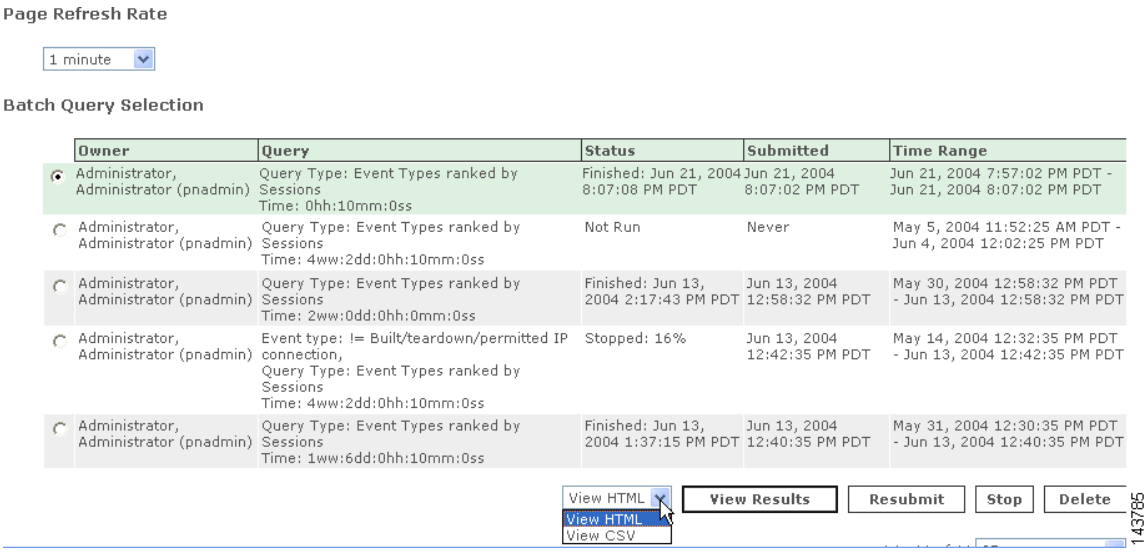
Step 3 In the Query Event Data window, you can change the query criteria. (For more information on query criteria, see Query Criteria, page 21-10). By clicking on various parameters you can change the nature of the query. In this case we are specifying a Source IP address of **10.1.1.6**, a Destination IP address range previously saved as **mygroup**, and setting the duration of the query to the past **2** days.Click either **Apply** button to apply your changes to the query. The Query Save/Submit window appears.

Figure 21-24 Query Save/Submit window



Step 4 The Query Save/Submit window asks you to choose from the options of **Save as Rule**, **Save as Report**, or **Submit Batch**. To submit your query as a batch query, click **Submit Batch**. Your query is submitted, and you are automatically taken to the Batch Query tab.

Figure 21-25 Batch Query Tab



Step 5 To watch the status of the query in real-time, you can use the Batch Query tab drop-down list to change the **Page Refresh Rate** from **Never** (the default) to 1 minute, 3 minutes, 5 minutes, 10 minutes, 15 minutes, or 30 minutes.

Note In general, do not use the browser refresh or other browser navigation buttons with the MARS Appliance GUI.

Step 6 To view the results of the batch query as it is running, click the radio button next to your query (here it's highlighted in green) and click **View Results**. This can be done while the query is in progress.

If the email address in your user profile on the MARS is valid, the results of your batch query are emailed to you when the query has completed. You can also view the results of your batch query by clicking **QUERY / REPORTS > Batch Query > View Results**.

Note When you click **View Results** while the query is in progress, the results compiled up to that moment are recomputed. This can make the display take longer to appear than after the results are compiled.

Reports

Using the Reports page, you can build repeatable queries, edit and delete current reports, run reports, and view reports in either HTML or CSV (comma separated value) formats.

Predefined System Reports are treated as global reports. Global Controller receives report data once its connected to the Local Controller. Previous report results (prior to managing the Local Controller) will not be pushed up to Global Controller. Thus viewing of reports will not include the information before the Local Controller becomes active.

When you view a report, you are viewing the last instance that ran. If you want to view an up-to-the-minute report, resubmit the report before viewing it.

Report results are purged from the database after a purge interval, as tabulated in Table 21-1.

Table 21-1 Maximum Database Retention Limits for Report Results

Cisco Security MARS Model	Maximum Number of Stored Reports[1]	Database Purge Interval[2]
CS-MARS-20-K9	1,000 ranking reports 5,000 event/session reports	3 months
CS-MARS-50-K9	1,000 ranking reports 5,000 event/session reports	3 months
CS-MARS-100-K9	1,000 ranking reports 5,000 event/session reports	6 months
CS-MARS-100E-K9	1,000 ranking reports 5,000 event/session reports	6 months
CS-MARS-200-K9	1,000 ranking reports 5,000 event/session reports	6 months
CS-MARS-GC-K9	1,000 ranking reports 5,000 event/session reports	12 months
CS-MARS-GCM-K9	1,000 ranking reports 5,000 event/session reports	12 months

1. Table values are for Cisco Security MARS Release 4.1.5. In Release 4.1.4 and prior, the maximum number of ranking reports is 100, maximum number of event/session reports is 1,000.
2. As of Cisco Security MARS Release 4.1.5. In Release 4.1.3, and 4.1.4, report results are retained for one year in the MARS database before they are automatically purged. In Releases prior to Release 4.1.3, report results are retained indefinitely. The purge interval cannot be changed.

Report Type Views: Total vs. Peak vs. Recent

Where alerts provide up-to-the-minute views of high-priority incidents, reports aggregate sessions into different views. Reports correlate based on the three data points:

- Period of time
- Query criteria
- View type

The *period of time* defines boundaries around the analyzed session data based on when it was recorded. *Query criteria* restrict the set of sessions that will be aggregated to that which matches your criteria. Criteria can include source address, destination address, network service, event, reported user, and reporting device. The *view type* defines how to aggregate the matched data into a meaningful report view—one that matches the type of study in which you are interested.

Note In each view type, you can refine the report criteria to filter out expected activity—the data you know about. You can filter this activity by refining the query criteria. These criteria should be tuned to a specific network. Reports can be valuable in detecting behaviors beyond the normal traffic flows of your network. You can determine the expected activities using reports that are not filtered and vetting those results against normal network use.

MARS provides three view types, each of which restricts the matched sessions to a user-defined limit of *N*. The following view types exist:

- **Total View**. For each result type matching the query criteria, this view counts the occurrences of that result type that transpire during the specified time period. It presents the total count of the top *N* matched result types, ranked by number of sessions, as determined by which ones occurred most frequently over the period of time. You can use these reports to determine your network's condition relative to the studied sessions. For example, you can use this view to identify attacks that launched at frequent intervals. This view does not present spikes in network activity; it simply presents the top occurring result types.
- **Peak View**. Within MARS, all report result data is stored in 10-minute time slices. The Peak View studies each of the 10-minute time slices within the specified time period to which one contained the highest number of matched sessions for a specific result type. It also determines an additional nine peaks within the time period, where each peak identifies a unique result type relative to the other peaks.

Each peak value is charted relative to the other nine peaks. For each time slice containing a peak value, the Peak View lists the top *N* matched result types that occurred. It is possible to have multiple peaks within the same time slice, as it is the result type, not the time slice, that must be unique across peaks.

Note To be detected within this view, the result type must peak above normal traffic. Therefore, you must tune the query data to filter out expected traffic.

Unlike the Total View, the Peak View does not focus on the overall top occurring results, instead it identifies a high volume of traffic over a short time period. Its purpose is to detect temporary bursts of traffic on your network that overshadow normal traffic usage. These bursts identify possible issues, such as worm outbreaks.

- **Recent View**. This view is similar to Total View; however, it identifies the top *N* result types that occurred within the past hour. It then plots all occurrences of those result types over the selected time period.
- **CSV**. Generates the Total View but presents the report in the CSV format for processing by another tool or script. This option is intended for use with e-mail notifications where post-processing is required.

Creating a Report

You can create a report through the **Query** page, or you can create a report from scratch on the **Reports** page. These instructions detail creating a report from the **Reports** page, but are applicable to editing reports and to creating reports from the **Query** page.

To Create a New Report

Step 1 On the Reports page, click the **Add** button.

Step 2 In the **Report Name** and **Report Description** fields, enter a report name and description. Click the **Next** button.

Step 3 Select the schedule parameters for the report.

Step 4 Select a View Type for the report. You can receive these reports in your email or view them in the UI. Your choices are: **Total View**, **Peak View**, **Recent View**, and **CSV** (see Report Type Views: Total vs. Peak vs. Recent, page 21-24). Click the **Next** button.

Step 5 Select users in the Recipients Available field by expanding the user groups, clicking users or user groups, and clicking the **Add** button. See User Management, page 24-8 for more information.

Step 6 Repeat Step 5 for other users. Click the **Next** button.

Step 7 Build or modify the query. To edit the query time range, either click the Report type link or click the **Edit** button. See Result Format, page 21-5 for information on query parameters; see Query Criteria, page 21-10 for more information on building queries. Click **Apply** to save your changes; click **Next** when the query is complete.

Step 8 Click **Submit** to save your report.

Working With Existing Reports

To View a Report

Step 1 Click the radio button next to the report.

Step 2 From the drop-down list on the bottom of the page, select either:

- **View HTML**: to view the report as an HTML file.
- **View CSV**: to view the report as a CSV file.

Step 3 Click the **View Report** button.

Note If you chose to view the report as a CSV file, you need to save the file to your computer and open the CSV file in a third-party application.

To Run a Report

Step 1 Click the radio button next to the report.

Step 2 Click the **Run Now** button.

Note Due to caching issues, reports with a time range of less than one hour are not recommended.

See Table 21-1, "Maximum Database Retention Limits for Report Results" for information on how long report results are retained in the database per MARS model number.

To Delete a Report

Step 1 Click the radio button next to the report.

Step 2 Click the **Delete** button to delete the report.

Step 3 On the Delete Confirmation page, click **Delete**.

To Edit a Report

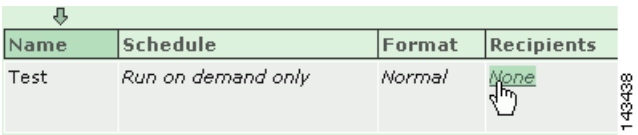
You can not edit system generated reports. Editing report criteria is meant for minor tweaking to previously generated report.

Step 1 Click the radio button next to the report.

Step 2 Click the **Edit** button to edit the report.

Step 3 Navigate using the **Previous** and **Next** buttons, or clicking on the report criteria.

Figure 21-26 Navigating to the Recipients column by clicking its criteria



Step 4 Edit the report, and click the **Apply** button to apply changes to the report.

Step 5 Click the **Submit** button to finalize the report.

Note Changing the report's query criteria will not re-generate a new result. New edited criteria is based on the previously generated report. In some situation such as filtering out specific IP source, user should create a new report.

Note Email notification of a global generated report will be sent from the Global Controller and not the Local Controller.