CHAPTER 17

Security Manager Policy Table Lookup from a MARS Event

This chapter describes how to configure and use Security Manager and MARS so as to enable bi-directional lookup between events recieved by MARS and access rule and signature policy found in Security Manager.

While Security Manager enables you to centrally manage security policies and device settings in large scale networks, Cisco Security MARS identifies, isolates, and recommends precise removal of compromised network elements. Cisco Security MARS does this task by transforming raw security data into an easily-readable format to subvert valid security incidents and maintain compliance. MARS integrates with Security Manager to map traffic-related syslog messages to the firewall or signature policy in Security Manager that triggered the event. Policy lookup enables rapid, round-trip analysis for troubleshooting firewall configuration-related network issues and policy configuration errors, and for fine-tuning defined policies. Following suggestions from MARS on access rule and signature changes to block the traffic, you can use Security Manager to manually mitigate using the access rule and signature recommendations provided by MARS, thereby, ensuring that the configuration management solution stays abreast of the mitigation responses. Security Manager can also publish the same change to all like devices that it manages, providing a more robust containment.

In Security Manager 3.1.1 through 3.0.1 and Cisco Security MARS 5.3.3 through 5.2.x and 4.3.3 through 4.2.1, although you can look up the Security Manager policy table that generated a MARS event or incident from within the MARS UI in read-only mode, you cannot alter the access rule that generated the event without logging in to Security Manager in a separate session. With Security Manager 3.2 and MARS 4.3.4 and 5.3.4, you can modify access rules generating the MARS event seamlessly from the read-only policy table popup window, which displays all rules associated with an event, by clicking the highlighted access rule number without starting Security Manager separately. Similarly, you can navigate to the signature summary table in Security Manager from MARS events associated with IPS sensors and IOS IPS devices and alter the signature properties. This feature enables you to map a syslog message to the policy that triggered that message and modify it simultaneously, thereby reducing time spent configuring and troubleshooting access rules in large or complex networks.

For example, consider the following case where a user cannot connect to *destination X* from *source Y*. To troubleshoot this issue, an administrator can do the following:

1. Log in to the MARS web interface and use an on-demand query to determine whether any recieved events indicate that traffic was blocked between *source Y* and *destination X*.
2. If such events are found, the administrator can cor[illegible] by determining which access rule blocks the traffic. To do so, the click the policy query icon ( ) in the row of one of the selected events. MARS then queries Security Manager to retrieve the list of access rules that match that traffic flow. Assuming that Security Manager manages the routers and firewalls between *source Y* and *destination X*, a list of matching access rules are returned.

3. Next, the administrator clicks the access rule number to log in to Security Manager and edit the identified policy, or access rule, to allow traffic between *source Y* and *destination X*. MARS reuses the already running Security Manager session, if one exists, or starts a new session using the Security Manager login credentials defined in MARS.

This chapter contains the following topics:

Taskflow for Policy Table Query from MARS Events

The Security Manager Policy Table Lookup icon appears in the Reporting Device column of the MARS session display when MARS receives a syslog triggered by the following:

- Matches against access rules from a Cisco PIX Firewall, Cisco Adaptive Security Appliance (Cisco ASA), Cisco Firewall Services Module (Cisco FWSM), or Cisco IOS, and the five tuple information required to establish an event (source IP, destination IP, source port, destination port, and protocol) can be derived.
- Connection establishment and tear-down using TCP, UDP, and ICMP on security appliances and FWSM blades.
- Firing of signatures from IPS and IOS IPS devices.

Clicking the icon queries Security Manager, the result of which is to identify the access rule in the policy table of the device that created the traffic incident or event. The following steps depict the policy query process between MARS and Security Manager:

1. From the Summary, Incidents, or Query page, navigate to the Incident Details page or the Query Results page for a particular incident ID and click the Security Manager Policy Query icon in the Reporting Device field to invoke the policy table lookup.
2. MARS establishes an HTTPS connection in one of two ways, depending on the authentication mechanism chosen while adding Security Manager to MARS: by using the MARS credentials or prompting the user for login credentials, or by using the Security Manager username and password saved in the MARS database.
3. If authentication fails, MARS displays an error message in a popup window. On successful authentication, MARS requests the device ID from Security Manager by providing the hostname and IP address.

4. If more than one device matches the MARS query criteria, all matching reporting devices are displayed in a popup window from which you can select the device for which you need to modify the access rule. If only one device matches the MARS query criteria, step 5 is performed. If no device matches the query criteria, an error message is displayed. For more information, see Understanding Security Manager Device Lookup, page 17-4.
5. MARS performs one of the following actions, depending on the type of syslog that generated the event:
   - If an access rule triggered the syslog on ASA devices, PIX security appliances, IOS routers, or FWSM blades, MARS sends the syslog message to Security Manager. Security Manager then looks up the policy table for all access rules that match the device ID and five-tuple data. MARS also provides the action, direction, interface, and ACL name information.
   - If a TCP, UDP, or ICMP connection establishment or teardown resulted in the syslog on ASA, PIX, or FWSM devices, MARS sends the raw syslog message to Security Manager for processing. Security Manager looks for all access rules that match the device ID, five-tuple data, direction of traffic flow, and mapped (NATed) IP addresses in the message.
   - If the signature on an IPS or IOS IPS device triggered the syslog, MARS requests all signature policies that match the device, signature, and subsignature IDs. MARS displays an error message if you attempt to view the Security Manager signature summary table for a virtual sensor, because the virtual sensor ID is not available in the MARS event data to query Security Manager for a matching signature.

   For more information on how Security Manager analyzes the syslogs from MARS and retrieves matching policies from the Access Rules page, see Understanding Access Rule Table Lookup, page 17-4. For more information on how the signature associated with an IPS event is retrieved from the signature policy table, see Understanding Signature Table Lookup, page 17-7.
6. The policy table lookup query is done in one of the following three ways, depending on whether Workflow or non-Workflow mode is enabled and Security Manager client is running or not.
   - If an instance of the Security Manager client is not running and either Workflow or non-Workflow mode is enabled in Security Manager, the lookup query is performed on the policies committed to the Security Manager database.
   - If Workflow mode is enabled and an instance of the Security Manager client is active, the lookup query is performed on all policies within the context of the current activity (in an editable state, namely, Edit, Edit Open, Submit, or Submit Open) as well as references found in data committed to the Security Manager database.
   - If non-Workflow mode is enabled and a Security Manager client session is open, the lookup operation is performed on all policies in the current login session (within the context of the automatically created activity in non-Workflow mode).
7. For events generated by access rules and connection establishment and tear-down syslogs, MARS displays the read-only access rule policy lookup table with matching rules highlighted from which you can navigate to the Access rules page of Security Manager and fine-tune the policy. For IPS events, MARS displays the read-only signature details page from which you can click Edit Signature to navigate to the Signatures policy page in Security Manager and modify the highlighted IPS signature that generated the event.
8. For access rule and connection-related syslogs, click the hyperlinked rule number from the read-only access rule table window to start the Security Manager client and modify the highlighted rule. For syslogs triggered by IPS signatures, click Edit Signature from the read-only popup window to start the Security Manager client and modify the highlighted signature. You can also configure an event action filter to remove one or more actions from a signature event.

   The Security Manager client is started from MARS in one of the following three ways:

- If the Security Manager client is not installed on the system to which the policy lookup query was made, you are prompted to install the Security Manager client and the page for downloading the application is opened.
- If an instance of the Security Manager client is already running, the existing session is reused.
- If the Security Manager client session has timed out or an instance is not active, a new instance of the Security Manager client is started.

Understanding Security Manager Device Lookup

MARS requests the access rule and signature policy table of a device that Security Manager administers by supplying the following criteria to Security Manager:

- Device Name—Derived from the Device Name field in the Security and Monitoring Information page of MARS.

Note For devices that support the discovery operation, such as routers and firewalls, MARS renames this field's value to match the name discovered in the device configuration, which typically uses the hostname.domain format. For devices that cannot be discovered, such as Windows and Linux hosts and host applications, MARS uses the provided value.

When you add FWSM and ASA devices with multiple security contexts to Security Manager, the context name is set as the hostname in the Device Properties page and policy lookup from MARS events for these contexts works properly. If the hostname is not the same as the context name, policy lookup from events fails. In such cases, make sure that the hostname defined for that context in the Device Name field of the MARS GUI matches with the hostname configured in the Device Properties page of Security Manager for policy lookup to work correctly.

- IP Address—Derived from the Reporting IP field in the Security and Monitoring Information page of MARS.
- Domain Name—If available, derived from the device name in MARS (for example, c3550-225-125.clab.cisco.com).

The Device Lookup query takes the following actions between MARS and Security Manager:

1. Security Manager matches the MARS Device Name to the Security Manager host names. If only one matching hostname is discovered, the process for Policy Table Lookup is invoked.
2. If there are multiple matches on hostname and no unique display name matches, the domain name (if available) is used to narrow the choices.
3. If the domain name is not available, MARS Reporting IP is used to narrow the choices.
4. If a unique device cannot be identified, MARS displays a list of possible devices in a popup window that shows the IP address, host name, display name, and domain name for all possible device matches. The user manually selects the device and the process for the policy table lookup is invoked.

Understanding Access Rule Table Lookup

The device lookup information is combined with the event information to perform the Security Manager access rule table lookup.

In the policy table lookup that was implemented in Security Manager 3.1.1 through 3.0.1 and MARS 5.3.1 through 4.2.1, the Security Manager policy query icon was displayed for all MARS events that had the 5-tuple data available. This method of lookup resulted in incorrect and inaccurate access rule matches from MARS events. For example, in earlier releases of Security Manager and MARS, the policy query icon was displayed for events generated by the connection establishment and teardown of management traffic from a firewall even though this traffic flow was not subjected to access rule check. Also, the incomplete parsing of connection-related syslogs was compounded by the absence of connection direction and post-NAT addresses in the teardown syslogs.

Security Manager 3.2 integration with MARS 4.3.4 and 5.3.4 for access rule table lookup supports more accurate mapping of MARS syslogs (events) to Security Manager access rules and reduces the number of irrelevant matches, thereby enabling faster and improved troubleshooting of access rules. This improved behavior is accomplished because MARS sends Security Manager the raw syslog message and not just the parsed event information, such as the event 5-tuple, action, ACL name, interface, and direction of flow. Using the raw event sent by MARS, Security Manager extracts critical data about the direction of traffic flow and other details, such as pre-NAT and post-NAT addresses. After the most accurately matching policy is found, Security Manager passes the information to MARS, which is translated in a readable format.

TCP and UDP connection setup/teardown syslogs represent the traffic flow through the firewall. A connection setup syslog is generated when a session is established through the device, when traffic flows to the device, or when traffic flows from the device. Each connection setup syslog has an associated teardown syslog, which is generated when the session is terminated. Although both the setup and teardown syslogs share a common connection ID, the teardown syslog does not contain the pre-NATed address and direction information. For teardown syslogs, MARS also transmits the corresponding setup syslog for that connection because it contains the necessary information for an accurate match. For sessionized events, MARS also sends the session object, which contains NATed details, to Security Manager for lookup. Security Manager parses the details from the syslog in raw format and performs two queries, instead of one, on the policy database to find a matching permit ACE in the inbound and outbound interfaces in the “in” and “out” directions, respectively. As a result, each policy query for a connection setup/teardown syslog yields zero, one, or two matches, depending on the configuration of a permit ACE on that interface in the specified direction. A maximum of two matching rules is displayed in the read-only access rule table popup window after the lookup.

ICMP connection setup and teardown syslogs do not contain the ICMP code, type, interface names, direction keyword, and a connection ID. Therefore, lookup of access rules for ICMP setup/teardown syslogs is not as accurate as their TCP and UDP counterparts owing to the absence of necessary details to locate an exact match. However, the ICMP setup/teardown syslogs associated with management traffic to and from a device are handled slightly differently. For management traffic triggered by TCP and UDP connection-related messages, Security Manager checks for the presence of the “NP Identity Ifc” keyword as the second interface in the syslog format for these protocols to obtain the most accurate matches for the lookup query. Although the Security Manager icon is displayed for events generated by ICMP connection teardown syslogs, an error message is displayed when you perform policy lookup from these events. The error message states that the corresponding connection setup syslog for the teardown syslog could not be found and asks you to try this operation after a few seconds. However, the same error is displayed even if you perform lookup at a later time.

Each syslog generated by an access rule or connection setup/teardown is associated with a unique ID. You can navigate to the policy rules that trigger syslogs in MARS from the Incident Details page by clicking the Security Manager icon. You can query policies only from those syslog IDs that are supported by MARS and Security Manager. For details on the syslog IDs supported by MARS and Security Manager for policy lookup from events, see Security Appliance and Router System Log Messages Supported for Policy Lookup, page 17-6.

MARS displays the policy table in a popup window. The matching access rule is displayed in highlight. If MARS was unable to provide the interface, direction, and action information, multiple matched access rules may be highlighted.

Sample TCP Connection Setup/Teardown Syslog Messages for an ASA Device

```
Mar 19 2007 21:05:59 2.168.154.2 : %ASA-2-302013: Built outbound TCP connection 42210

Mar 19 2007 21:06:27 2.168.154.2 : %ASA-2-302014: Teardown TCP connection 42210
```

Sample ICMP Connection Setup/Teardown Syslog Messages for an ASA Device

```
Mar 19 2007 21:03:44 2.168.154.2 : %ASA-2-302021: Teardown ICMP connection

Mar 19 2007 21:03:44 2.168.154.2 : %ASA-2-302020: Built ICMP connection
```

Sample UDP Connection Setup/Teardown Syslog Messages for an ASA Device

```
Mar 19 2007 21:08:53 2.168.154.2 : %ASA-2-302015: Built outbound UDP connection 42214

Mar 19 2007 21:10:55 2.168.154.2 : %ASA-2-302016: Teardown UDP connection 42214
```

Sample Cisco PIX Firewall Syslog Messages with Access Group Name Information

```
10.33.10.2 <142>%PIX-4-106023: Deny tcp src inside:10.1.5.234/3010 dst outside:5.6.7.8/21
```

Sample Cisco IOS 12.2 Syslog Messages with ACL Name Information

```
100.1.20.2 Mon Jun 9 14:46:31 2003 <46>485232: Jun 9 14:46:29 PDT: %SEC-6-IPACCESSLOGP:
list

10.34.1.1 <46>146570: Dec 19 21:01:57 PST: %SEC-6-IPACCESSLOGP: list
```

Security Appliance and Router System Log Messages Supported for Policy Lookup

You can configure logging options on security appliances when a deny ACE matches a packet for network access (an access list applied with the access-group command). If you enter the **log** keyword without any arguments, you enable system log message 106100 at the default level (6) and for the default interval (300 seconds). If you do not enter the **log** keyword, the default logging occurs, using system log message 106023. In devices with multiple contexts, each security context includes its own logging configuration and generates its own messages.

System log messages begin with a percent sign (%) and are structured as follows:

```
%{ASA | PIX | FWSM}-Level-Message_number: Message_text
```

A unique 6-digit number identifies each message. The following syslog message IDs are supported for looking up policies in Security Manager from incidents generated in MARS. If you change the logging level of the firewall, ensure that the following messages IDs are generated at the new level so the MARS Appliance receives them.

106100, 106023, 302013, 302014, 302015, 302016, 302020, 302021

The default level for many of the events that are studied by MARS is the debug level, which can generate a high volume of additional events that are not used by MARS. If you are experiencing an influx of these other events, you can use the **logging message** command to either turn off events or change the severity level of the event to a level that generates required messages but not as many as debug. For details on the message, explanation, and recommended action for each of these message IDs, see the System Message Guide of the relevant product documentation.

On Cisco IOS routers, system log messages are generated for access lists configured with the **log** or **log-input** keywords. Use the **log** keyword to get access list logging messages, including violations. Use the **log-input** keyword to include input interface, source MAC address, or virtual circuit in the logging output. The first packet that triggers the access list causes an immediate logging message, and subsequent packets are collected over 5-minute intervals before they are displayed or logged. The logging message includes the access list number, whether the packet was permitted or denied, the source IP address of the packet, and the number of packets from that source permitted or denied in the prior 5-minute interval. You can look up access rules that generate these log messages by clicking the Security Manager policy query icon in the Incident Details page or the Query Results page of MARS.

For IOS routers, system log messages with the following identifiers support policy lookup and the Security Manager icon is displayed beside them in the MARS GUI:

%SEC-6-IPACCESSLOGDP, %SEC-6-IPACCESSLOGNP, %SEC-6-IPACCESSLOGS, %SEC-6-IPACCESSLOGP

For IOS system log messages with IDs other than the ones listed above and that are not generated by access rules, the Security Manager icon is not displayed in the MARS GUI.

Understanding Signature Table Lookup

Security Manager 3.2 and MARS 4.3.4 and 5.3.4 support signature summary table lookup for events generated by IPS devices (Cisco IPS sensors and Cisco IOS IPS devices) and IDS sensors. Sensors that use a signature-based technology can detect network intrusions. A signature is a set of rules that your sensor uses to detect typical intrusive activity, such as DoS attacks. As sensors scan network packets, they use signatures to detect known attacks and respond with actions that you define. The sensor compares the list of signatures with network activity. When a match is found, the sensor takes an action, such as logging the event or sending an alert. Signature-based intrusion detection can produce false positives that you can minimize by tuning your signatures. Some signatures have subsignatures, that is, the signature is divided into subcategories. When you configure a subsignature, changes made to the parameters of one subsignature apply only to that subsignature.

Security Manager looks for the following criteria from the raw event message that MARS sends for IPS events:

- Signature ID—Identifies the unique numerical value assigned to this signature. This value lets the sensor identify a particular signature.
- SubSignature ID—Identifies the unique numerical value assigned to this subsignature. A subsignature ID is used to identify a more granular version of a broad signature.

Note Signature policy lookup is not supported for virtual sensors because the sensor ID is not contained in the raw syslog message that is logged in MARS to enable Security Manager to perform a lookup.

Packet Data events that identify the data that was being transmitted on the network the instant an alarm was detected on IPS and IDS sensors can cause the size of the raw message associated with this event to become very huge. Also, these events are not triggered by signature rules on sensors. As a result, the

Security Manager icon is not displayed for Packet Data events in the MARS GUI for policy lookup.

Events triggered by custom signature configured on a sensor are categorized as "Unknown Device Event Type" in the MARS GUI and the Security Manager icon is displayed for these events to enable policy lookup.

After a match is found, Security Manager transmits the signature details to MARS and the matching signature parameters are displayed in a read-only popup window in MARS. You can click Edit Signature to navigate to the signature summary table of Security Manager with the matching signature selected. You can also click Event Action Filter from the read-only popup window to configure a filter on the basis of signature categories to remove one or more actions from the signature event. The filter is applied in the order specified in the summary table. The authentication mechanism that you entered while adding Security Manager to MARS is used to open the signature summary table and a new instance of Security Manager is started if one is not running or the existing session times out.

Guidelines for Working with Policy Table Lookup from MARS

Remember the following points when you query the Security Manager policy table from MARS syslog messages:

- You need to use Security Manager 3.2 and MARS 4.3.4 or 5.3.4 to navigate to the policy table in Security Manager from MARS and modify the matching rule. If you add a Security Manager server running 3.0.x or 3.1.x to a MARS appliance running 4.3.2 through 4.3.4 or 5.3.2 through 5.3.4, you can perform the policy table lookup in view mode only.

  Support for read-only policy table lookup from a MARS appliance running 4.3.4 or 5.3.4 is solely to provide backward compatibility with a Security Manager server running 3.0.1, 3.0.2, or 3.1.x.
- The Security Manager policy table lookup icon is not displayed for NetFlow events received by MARS from NetFlow-enabled reporting devices that are positioned within your network because they are not triggered by an access rule.
- The Security Manager policy table lookup icon is not displayed for events of type, Packet Data and Context Data, because they are not generated by signatures configured on Cisco IDS 4.x and Cisco IPS 5.x devices, whether they are sensor appliances or modules.
- For PIX and ASA devices or FWSM blades with multiple security contexts, you must enter the reporting IP address for each context while configuring the device in MARS. Otherwise, the Security Manager icon is not displayed beside events received from the contexts for which the reporting IP address is not defined in MARS and you can query events from such contexts only by running a query for "Unknown Reporting Devices" from MARS.
- A Local Controller can be configured to retrieve the policy tables from only one Security Manager server at a time. An error message is displayed when you attempt to add more than Security Manager server to a Local Controller.
- If you add a Local Controller, to which Security Manager server has been added, to a Global Controller, you can view the Security Manager server in the Security and Monitoring Information list of the Local Controller from the Global Controller interface. However, the Security Manager policy query icon is not displayed beside events or incidents displayed on a Global Controller.
- All users associated with any of the CiscoWorks Common Services roles except the Help Desk role or any of the predefined Cisco Secure ACS roles have permission to modify the matching policy by clicking the Security Manager icon from the read-only policy lookup table.

- While adding a Security Manager to MARS, only users with Admin role can be configured to enable MARS contact and discover Security Manager server configuration. Otherwise, an error message is displayed when you submit your changes.
- All users associated with any of the MARS roles with the exception of the Operator and Notifications Only roles can modify the Security Manager authentication credentials while editing an existing user account in MARS.
- If the Security Manager server cannot be reached from MARS when you perform a policy lookup, an error message is displayed asking you to restore the connection between MARS and Security Manager.
- If HTTPS is not enabled on Security Manager for secure access between the Security Manager server and MARS, an error message is displayed when you try to start Security Manager. Ensure HTTPS is enabled on the Security Manager server so that communication between the Security Manager and MARS is encrypted.
- If the Daemon Manager on the Security Manager server is not running, an error message is displayed prompting you to restart the service when you perform the policy table lookup.
- The MARS Appliance compares the certificate presented by Security Manager with a previously stored instance of the certificate while establishing a secure connection with Security Manager. If a conflict is detected, MARS accepts and stores the replacement certificate, either automatically or after prompting for manual acceptance, depending on the options configured in MARS. For more information on how MARS responds during attempts to establish a secure connection, see *User Guide for Cisco Security MARS Local Controller 4.3.x and 5.3.x*.
- The Security Manager username and password values that you enter or modify in the Reporting Applications tab is used by MARS to communicate with Security Manager server and discover meta information, such as version of software running on the server and configuration details. These credentials are different from the username and password in the Cisco Security Manager section of the User Configuration page.

  The username and password pair in the User Configuration page comprise the credentials that MARS uses to authenticate with Security Manager to look up the policy table, when you select the option to use Security Manager credentials for policy lookup. The Security Manager username and password fields in the User Configuration page are populated with the values you enter in the policy query login dialog box if you chose to allow saving of Security Manager login credentials during policy lookup.
- If you did not specify the username and password for logging in to Security Manager or entered incorrect credentials while adding Security Manager, the connectivity test fails and an error message is displayed. Similarly, if you changed the login credentials in Security Manager but failed to update them in the MARS GUI, an error message is displayed during policy lookup.
- If a Security Manager client session is not open at the time you perform policy lookup, you are not logged out from the Security Manager instance (opened for the purpose of policy lookup) when the idle timeout period is exceeded or when you log out of the MARS session. The Security Manager session closes only when you log out from it or when the idle timeout configured for it is exceeded.
- If you selected the option to use the Security Manager login credentials for MARS to authenticate with Security Manager and did not choose to allow the login credentials to be saved in the login dialog box, these credentials are cached until you exit MARS or the idle session timeout period is exceeded; you are not prompted for login details until the MARS session is active. If the Security Manager session times out after MARS has successfully authenticated with Security Manager and you selected the option to be prompted for login credentials for policy table lookup, the login dialog box is displayed when you click the Security Manager icon from a MARS syslog.

- If you selected the option to be prompted for Security Manager login credentials to authenticate MARS during policy table lookup and deleted the Security Manager server from the MARS database, the username and password fields under the Cisco Security Manager section of the User Configuration Page (Management > User Management tab > Add) in the MARS GUI are dimmed. These fields are also dimmed if you chose not to allow saving of Security Manager login credentials while MARS authenticates with Security Manager.
- If you selected the option to use the Security Manager login credentials for MARS to authenticate with Security Manager and chose to allow the login credentials to be saved in the login dialog box, the username and password fields under the Cisco Security Manager section of the User Configuration Page are activated and can be edited by MARS users with Admin or Security Analyst roles.
- If you saved Security Manager login credentials in the Cisco Security Manager section of the User Configuration page and later logged in to MARS using an account with full read/write privileges to modify the cross-launch authentication settings by deselecting the Allow Users to Save Credentials check box in the Reporting Applications tab, the username and password entries in the Cisco Security Manager section of the User Configuration page are deleted. However, if you perform the same task using an Operator or Notifications Only user role, the Security Manager username and password details are not deleted from the User Configuration page, but can only be viewed.
- If you logged in to Security Manager using a user account that is different from the one that is being used to start Security Manager from MARS for the policy table lookup and you selected the option to use Security Manager credentials, a new instance of the Security Manager client is started even if a client session is active.
- If you log in to MARS using an account that is not defined in the Common Services 3.1 UI and selects the option to use MARS credentials in the Reporting Applications tab, you are prompted to enter the user credentials that is configured in Common Services during policy table lookup.
- If the Security Manager client is not installed on the system from which you are accessing the MARS web interface, you are prompted to install the Security Manager client during policy lookup and the page to download the client software is opened.
- If an instance of the Security Manager client is already running, the existing session is reused by MARS to display the policy lookup table for editing access rules or signatures.
- If the Security Manager client session has timed out or an instance is not active, a new instance of the Security Manager client is started to query the policy table for matching rules and signatures.
- If an instance of the Security Manager client is not running and either Workflow or non-Workflow mode is enabled in Security Manager, MARS performs the lookup query on the policies committed to the Security Manager database.
- If Workflow mode is enabled and an instance of the Security Manager client is active, the lookup query is performed on all policies within the context of the current activity (in an editable state, namely, Edit, Edit Open, Submit, or Submit Open) as well as references found in the data committed to the Security Manager database.
- If non-Workflow mode is enabled and an instance of the Security Manager client is active, the lookup query is performed on all policies in the current login session.
- If a modal window or dialog box is open in Security Manager or the modal window is overlaid with any other application window, an error message is displayed when the policy lookup query is performed. Close the modal dialog box in Security Manager and retry the task.
- If a new instance of the Security Manager client is started during policy table lookup, the time taken to display the matching rules might be slightly greater than the time consumed when a Security Manager client session is active.

- The time taken to display the policy table lookup query results is proportional to the number of rules in the policy table of Security Manager. Increased number of rules might impact the performance of MARS and Security Manager.
- The policy rules retrieved from the Security Manager policy table and displayed in the read-only policy query window in MARS are cached to enhance performance. Caching reduces the time taken to display query results on subsequent lookups as the query results are reused when a request is made to query policies for the same event.
- The Security Manager policy table lookup icon in MARS is displayed only for traffic logs triggered by the following event types:
  - Matching of Access rules from a PIX firewall, ASA device, IOS router, or an FWSM blade, regardless of whether the 5-tuple information is available or not. If the 5-tuple data cannot be derived from the syslog, the most accurate match is displayed after policy table lookup.
  - Connection establishment and tear-down using TCP, UDP, and ICMP on PIX, ASA, and FWSM devices.
  - Firing of signatures from IPS and IOS IPS devices.

  Note The versions of software running on the devices that report syslogs to MARS and for which policies are defined in Security Manager must be supported by both Security Manager and MARS. See Devices and OS Versions Supported by Both Security Manager and MARS, page 17-15 for a list of devices supported by both Security Manager and MARS.

- The same events received by MARS can display the Security Manager policy table lookup icon inconsistently between the low-latency, realtime event query and standard queries, such as sessions ranked by time. Specifically, the icon will not appear in the low-latency, realtime query, but it may appear in queries against sessionized events.

  This behavior is expected. When MARS receives events, they are parsed, sessionized, written to an event shared buffer, and then written to the database. Because sessionization takes time, sometimes keeping an event in cache for 2 minutes, the low-latency event query displays events right after parsing, but before sessionization. Displaying the event at this point allows the low-latency query to achieve a close to realtime effect. For some events, parsing cannot determine some part of the 5-tuple data, such as a destination address. Later, sessionization later fills in such missing data using configuration data. As a result, the 5-tuple data displayed by the low-latency event query can be different from values stored in the database, which are used to populate the standard queries.
- MARS displays the Security Manager security policy committed views, not the deployed views. If you change the access rule in Security Manager and do not deploy the changes to the device, the syslog is generated by the older access rule on the device because the changes are not synchronized and policy lookup is performed on the access rule saved on the device and not on the most recently saved changes in Security Manager.
- When you run a query for realtime or historical events and try to perform policy lookup from an incident in the query results, occasionally, an error message is displayed in the Policy Query popup window stating that an internal error has occurred. This error is temporary and disappears if you retry this operation after a while. You are prompted to log in again to Security Manager and policy lookup should be successful from then on. An error of this type also occurs when RPC connection fails or when policy changes to the device are not submitted to the Security Manager server.

- Although the Security Manager icon is displayed for events generated by ICMP connection teardown syslogs, an error message is displayed when you perform policy lookup from these events. The error message states that the corresponding connection setup syslog for the teardown syslog could not be found and asks you to try this operation after a few seconds. However, the same error is displayed even if you perform lookup at a later time.
- If the access rule associated with a device is empty in Security Manager, an error message is displayed when you perform the policy lookup query from MARS for a syslog generated by an access rule on that device.
- If you perform the policy table lookup for a device added to MARS only and not to Security Manager, an error message is displayed in the read-only policy table window. Make sure that you add the device to Security Manager and discover the policies so that the configuration on the device is synchronized with Security Manager.
- If you attempt to view the Security Manager signature summary table for a virtual sensor, an error message is displayed when you click the Security Manager icon for a syslog message from a virtual sensor because the virtual sensor ID is not available in the MARS event data to perform the policy lookup query.
- An error can occur with the policy query if a device configuration is discovered using Security Manager but it is not submitted in Security Manager. The following error message is an example of this issue:

```
<190>2312080: *May 9 23:50:02.199: %SEC-6-IPACCESSLOGDP: list permit-all permitted
icmp 10.2.3.8 ->
10.4.21.2 (0/0), 1 packet
An error occurred while querying policies from Cisco Security Manager. Reason: Failed
to retrieve policy
information from CSM. Reason: Cisco Security Manager Internal error: Failed to get
interfaces in the device!
```

  Before you perform policy queries, verify that all discovered devices have been submitted in Security Manager.
- If an access rule policy contains network/host and service objects, the definitions of the elements contained in these objects are displayed in the read-only policy lookup table. For the matching policy, the definitions of the network and service objects are expanded and displayed.
- If no access rule is configured on the lower security interface in the “in” direction of the device for inbound traffic or if the access rule specified in the syslog is not available on the device, an error message is displayed during policy lookup. When you click the Security Manager icon for syslogs associated with such access rules, a message states that a matching rule cannot be found. You are prompted to make sure that the device is added to Security Manager and access rules are configured on it.
- When you click the Security Manager icon for an event triggered by management traffic, an error message is displayed stating that the selected event was not subjected to access rule matches. You are prompted to select another event and retry policy lookup.
- If an event is generated by a connection teardown syslog and the setup and teardown of the connection occur in two different sessions (with a gap of 2 minutes in-between), the corresponding connection establishment syslog is not sent by MARS to Security Manager when you perform policy lookup for such events. As a result, an error message is displayed stating that the connection setup syslog is not available to display the matching rules for that event. An identical error message is also displayed if you attempt to query access rules for a connection teardown event from the realtime event viewer of MARS.

- When you click the Security Manager icon for an event that contains a syslog ID that is not supported for policy lookup, you are prompted to select another supported event. Although the Security Manager icon is displayed in the MARS GUI only for those events that support policy lookup, you might see this error message while looking up policies for events generated by management traffic or connection teardown syslogs without a corresponding setup syslog.
- An error message is displayed stating that the syslog is invalid even when you click the Security Manager icon for one of the syslogs supported for policy lookup. This problem occurs if the syslog is not parsed by Security Manager and the syslog format received from MARS is incorrect.
- When you perform lookup for an event generated by outbound traffic setup/teardown syslog with an access rule configured on the higher security interface in the “in” direction, an error message is displayed stating that an implicit permit statement is present in the access rule. Also, this error message occurs if a firewall device is added to Security Manager and the changes are not submitted to the database at the time of performing policy lookup from MARS.
- If the device for which you perform access rule lookup has been added to Security Manager without submitting the configuration to the database or if the access rule that generated the syslog is not available on the device, an error message is displayed stating that the access rules on the device is not in synchronization with the one configured in Security Manager.
- For inbound traffic, when an event is generated by an access rule present on the lower security interface in the “in” direction and no matching rule found in Security Manager during policy lookup, an error message is displayed stating that the access rules on the device and in Security Manager are not synchronized. This error is also displayed when a matching policy cannot be found for access rules present on the higher security interface in the “in” direction or on the lower security interface in the “out” direction for outbound traffic.
- If you modify the access rule in Security Manager after the read-only policy query window is displayed with highlighted rules that generated the event and start the Security Manager client, the rule table in the read-only policy page is used as the basis for displaying the matched rule in Security Manager and the modified rule table in Security Manager is not considered.
- When you try to lookup a signature policy from an IPS event in MARS, an error message is displayed if invalid event details are passed from MARS to Security Manager.
- If the signature that generated an event in MARS is deleted or modified on the device, an error is displayed stating that the signature is not found when you perform policy lookup for such an event.

Checklist for Policy Table Lookup from MARS

You can use the following checklist to track the tasks required to integrate MARS with a Security Manager server and the reporting and mitigation devices managed by that Security Manager server. Each step might contain several substeps; the steps and substeps should be performed in order. The checklist contains references to the specific procedures used to perform each task.

Step 1 Identify devices that need to be managed by both Security Manager and MARS.

The first step in integrating MARS and Security Manager involves identifying those devices for which Security Manager is used to define policy rules. You must ensure that devices are running a software version supported by both MARS and Security Manager.

For more information, see Devices and OS Versions Supported by Both Security Manager and MARS, page 17-15

Step 2 Identify and enable all required traffic flows between the devices and MARS.

After you identify the devices to be managed by the Security Manager server and monitored by MARS, you must verify that the network services they use for management, reporting, and notification are permitted along the required traffic flows. Ensure that the management, logging, and notification traffic between the MARS Appliance and each monitored device is allowed by intermediate gateways.

Tip It is a recommended security practice to have all devices, including MARS Appliances, synchronized to the same time.

For more information, see See the section "Required Traffic Flows" in of the "Deployment Planning Guidelines" chapter of the *Install and Setup Guide for Cisco Security MARS, Release 5.3.x*or *Install and Setup Guide for Cisco Security MARS, Release 4.3.x*.

Step 3 Prepare the devices to be managed by Security Manager.

Before you can manage devices using Security Manager, you must set up the devices with a minimum configuration that provides basic connectivity. To enable communication between Security Manager and devices, you must configure transport settings on the devices, before you add them to the inventory. Bootstrapping involves getting the device up and running on the network, assigning it an IP address, and connecting it to the physical media.

For more information, see “Preparing Devices for Management”

Step 4 Add the devices to Security Manager.

For more information, see “Managing the Device Inventory”

Step 5 Bootstrap the devices managed by MARS.

After you identify the devices managed by the Security Manager server and to be monitored by MARS, you must prepare, or bootstrap, that device to ensure that the MARS Appliance can receive or pull any necessary logs from those devices. After you identify and bootstrap the devices and enable the required traffic flows, you must represent those devices in MARS, which uses this information to communicate with the devices.

For more information, see For more information on adding and activating devices, see *User Guide for Cisco Security MARS Local Controller 4.3.x and 5.3.x*.

Step 6 Add the devices to MARS.

For more information, see For more information, see *User Guide for Cisco Security MARS Local Controller 4.3.x and 5.3.x*.

Step 7 Bootstrap each Security Manager server and add it to the correct MARS Local Controller.

For more information, see Bootstrapping Security Manager Server to Communicate with MARS, page 17-15

Step 8 Perform policy lookups as required.

Once an event generated by one of the Security Manager-managed devices is received by MARS, you can perform a policy lookup operation and modify the possible policies that could have affected the generation of that event from the Security Manager server. For more information on how to perform policy table lookup for events generated by access rules and signatures, see the following sections:

For more information, see the following references:

1. Navigating to Access Rule Policy in Security Manager from MARS, page 17-19
2. Navigating to IPS Signature Policy in Security Manager from MARS, page 17-24

Devices and OS Versions Supported by Both Security Manager and MARS

You must ensure that devices that need to be monitored by MARS and managed by Security Manager are running a software versions supported by both MARS and Security Manager to perform the policy table lookup from MARS syslogs and events lookup from Security Manager policies.

Table 17-1 on page 17-15 lists the software versions for each device platform supported by both Security Manager and MARS.

Table 17-1 Supported Devices and OS Versions for Security Manager and MARS Integration

Device Platform	Device OS Version
Cisco IOS Routers	12.x and later
PIX Security Appliances	6.0, 6.1, 6.2, 6.3, 7.0, 7.2, 7.2.1
Adaptive Security Appliances (ASA)	7.0.1, 7.2, 7.2.1
Cisco Intrusion Prevention System (IPS), IDSM-2 module	5.1, 6.0, 6.0.1, 6.0.2, 6.0.3
Cisco IOS Intrusion Prevention System (IOS IPS) sensors	Cisco IOS 12.3(14)T4, 12.4M, 12.4(2)T, 12.4(4)T, 12.4(11)T2
Cisco Catalyst 6500 Series Switches	Cisco IOS 12.2 and later
Firewall Services Module (FWSM)	1.1, 1.2, 2.3, 3.1, 3.1.3, 3.1.5[1]

1. FWSM support is available only in Security Manager Enterprise Edition (Professional-50) and higher. The professional version includes support for the management of Cisco Catalyst 6500 Series switches and associated service modules. The Standard versions do not include this support.

Note For a complete list of devices and OS versions supported by Security Manager and MARS separately, see the Supported Devices and Software Versions document of the respective applications.

Bootstrapping Security Manager Server to Communicate with MARS

To prepare the Security Manager server to be queried by MARS, you must configure the following settings:

- If you are using AAA authentication, such as Cisco Secure ACS, on the Common Services 3.1 server, you must update the administrative access settings to ensure that the MARS Appliance has the necessary access to the Security Manager server.
- Define a user account in Security Manager that MARS can use to perform queries. A separate account is recommended to provide a cleaner audit trail on the Security Manager server. You must create a user account with one of the following roles defined in Common Services 3.1 to be able to perform the policy table lookup query and modify the highlighted policy by starting Security Manager from the read-only popup window:
  - Approver

- Network Operator
- Network Administrator
- System Administrator

Note Any of the predefined Cisco Secure ACS roles with the exception of the Help Desk role can modify matching policies by starting Security Manager from the read-only policy lookup table. Users with the Help Desk security level can only view the read-only policy lookup table. An error message is displayed when a user with a Help Desk role attempts to start Security Manager to modify a policy from the read-only popup window in MARS.

When you add a Security Manager server to MARS, if you choose to use the option to prompt users for Security Manager credentials for the policy table lookup, you might not need to create a separate MARS user account in the Common Services 3.1 UI for authentication purposes.

For more information on adding users and associating roles with them from the Common Services 3.1 UI, see *User Guide for CiscoWorks Common Services 3.1*.

Adding a Security Manager Server to MARS

The Security Manager server is represented in MARS by defining a host with a software application residing on that host. The Security Manager server that you add to the Local Controller can be used to perform policy lookup only for those devices that it manages and that publish their events to MARS.

Each Local Controller can query one Security Manager server only; you cannot define more than one Security Manager server per Local Controller. You can define the same Security Manager server on multiple Local Controllers. When planning the zones for Global Controller/multi-Local Controller deployments, ensure that each Local Controller maps to the Security Manager server that manages the reporting devices monitored by that Local Controller.

If a Security Manager server is not added to MARS, the username and password fields in the Cisco Security Manager section of the User Configuration page are disabled. A message appears in the User Configuration page that the Security Manager credentials for policy table cross-launch cannot be saved in the MARS database because a Security Manager server is not yet added to MARS.

Before You Begin

- Make sure that the Security Manager server is running version 3.2 if you want to look up the policy table and modify matching rules or signatures. If you add a Security Manager server running 3.0.1, 3.0.2, or 3.1.x to a MARS appliance running 4.3.2 through 4.3.4 or 5.3.2 through 5.3.4, you can query for policies in view mode only; you must open a Security Manager client instance separately to modify the policies.

  Adding a Security Manager server running 3.0.1, 3.0.2, or 3.1.x to a MARS appliance provides the same behavior that existed in versions of MARS earlier than 4.3.4 and 5.3.4 to perform policy lookup.

- You must be logged in to the MARS Local Controller as a user with an Admin role.

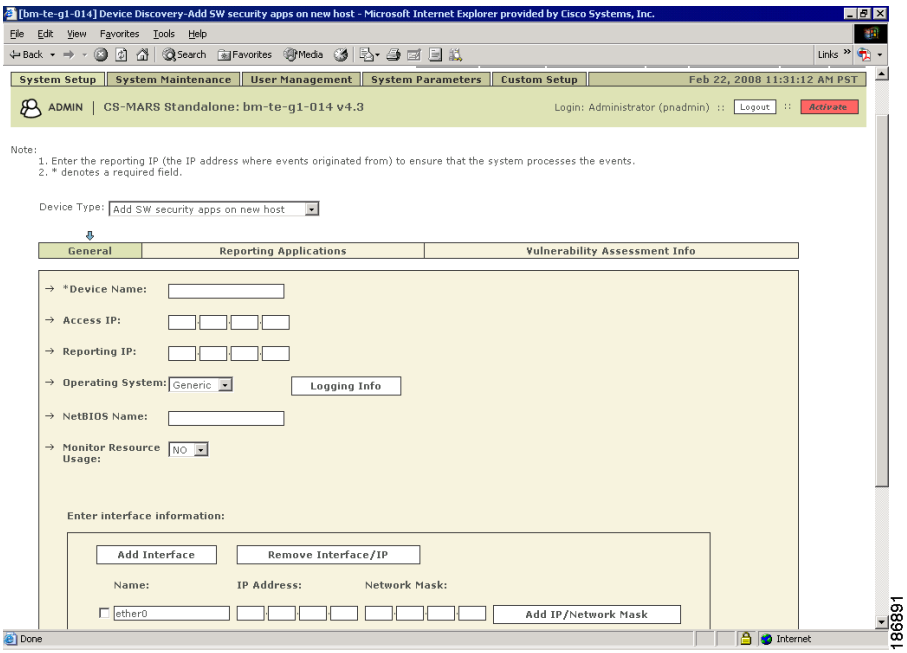
To identify a Security Manager server to use for policy lookups from within the web interface of MARS, follow these steps:

Step 1 Select **Admin > System Setup > Security and Monitor Devices > Add**.

Step 2 Do one of the following:

- Select **Add SW Security apps on a new host** from the Device Type list, and continue with Step 3. See Figure 17-1.
- Select **Add SW security apps on existing host** from the Device Type list. Select the device to which you want to add the software application and click **Add**. Continue with Step 6.

Figure 17-1 Device Discovery-Add SW security apps on new host



You can select the Add SW Security apps on an existing host option if you have already defined the host within MARS, perhaps as part of the Management > IP Management settings or if you are running another application on the host, such as Microsoft Internet Information Services.

Step 3 Specify values for the following fields:

- **Device Name**—Enter the name of the host (Security Manager server). This name is used for display purposes only in the MARS GUI and you can assign any meaningful name.
- **Access IP**—This address is used to discover settings and pull query data from a Security Manager server using HTTPS. This address represents the physical IP address of the Security Manager server.
- **Reporting IP**—(Optional) Enter the same IP address of the Security Manager server interface as the one entered in the Access IP field. This address also represents the physical IP address of the Security Manager server.
- **Operating System**—(Optional) Specify the operating system type by selecting **Windows** or **Generic** from the drop-down list.

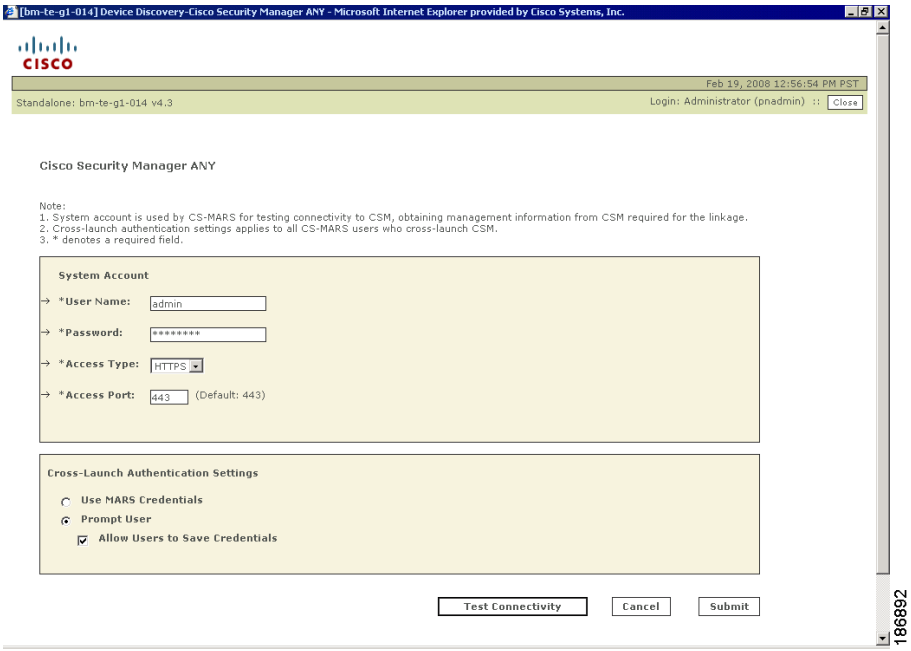
Step 4 Under Enter interface information, enter the interface name, IP address, and netmask value of each interface in the Security Manager server from which configuration information will be queried.

Step 5 Click **Apply** to save these settings.

Step 6 Click **Next** to access the Reporting Applications tab.

Step 7 Select the **Cisco Security Manager ANY** from the Select Application list, and click **Add**. See Figure 17-2.

Figure 17-2 Device Discovery-Cisco Security Manager ANY Page



Step 8 If you entered an address in the Access IP field on the host that represents this Security Manager server, specify values for the following fields:

- **User Name**—Identifies the Cisco Security Manager administrative account to be used to discover configuration settings.
- **Password**—Identifies the password associated with the username account.
- **Access Type**—Identifies the protocol used to discover configuration information. Select HTTPS from the drop-down list.
- **Access Port**—Identifies the port that MARS uses to communicate with Security Manager. The default access port for HTTPS is port 443.

Step 9 Under Cross-Launch Authentication Settings, do one of the following:

- Click the **Use MARS Credentials** radio button if you want to use the MARS login credentials to contact Security Manager for the policy table lookup. The MARS user account must have been previously added to the Local User Setup page in the Common Services UI with a role other than Help Desk to navigate successfully to the Security Manager policy table and modify the matching rules. This option is useful when MARS and Security Manager use a common, external server for authentication and authorization such as Cisco Secure ACS.
- Click the **Prompt User** radio button if you want to prompt the user to enter the credentials to log in to Security Manager to cross-launch the policy lookup table from MARS. The Security Manager login dialog box is displayed when you click the Security Manager icon to view the read-only policy lookup table. When you select the Prompt User option, you can choose to allow the Security Manager credentials to be saved or not.

  When you click this radio button, the **Allow Users to Save Credentials** check box, beneath it, is enabled. Select this check box if you want the Save Credentials check box in the Security Manager login dialog box to be enabled when you cross-launch the policy lookup table. Selecting the Save Credentials check box causes the Security Manager credentials to be saved in the MARS database and you are not prompted for access details during subsequent lookups.

If you deselect the **Allow Users to Save Credentials** check box, the Save Credentials check box is disabled in the login dialog box, prompting you to enter the login details each time you start the Security Manager policy table from MARS in a new session or after the timeout period. When the Allow Users to Save Credentials check box is deselected, the Security Manager credentials saved in the MARS database are deleted.

Note Login credentials are cached by MARS when you successfully log in to Security Manager. These credentials are discarded when you exit MARS or the idle session timeout period is exceeded.

If the Allow Users to Save Credentials check box is deselected, the username and password fields in the Cisco Security Manager section of the User Configuration page are disabled. A message appears in the User Configuration page that the Security Manager credentials to perform policy lookup cannot be saved in the MARS database because the Allow Users to Save Credentials check box is deselected. The message appears in the User Configuration page even when you choose to use MARS credentials for policy table lookup.

Step 10 (Optional) Click **Test Connectivity** to verify that the settings are correct and that the MARS Appliance can communicate with this Security Manager server.

If the username and password are correct and the MARS Appliance is configured as an administrative host for the device, a popup window appears with a "Connectivity successful." message when the discovery operation is successfully completed. Otherwise, an error message appears asking you to click the View Error link for more information about the probable cause and its possible solution.

Step 11 To add this device to the MARS database, click **Submit**.

The submit operation records the changes in the database tables. However, it does not load the changes into working memory of the MARS Appliance. The activate operation loads submitted changes into working memory.

Step 12 Click **Activate**.

After the MARS Appliance is activated, it can query the Security Manager server to perform policy lookups.

Navigating to Access Rule Policy in Security Manager from MARS

Access rules filter network traffic by controlling whether routed packets are forwarded or blocked at the firewall's interfaces. Rules are processed by a device from first to last, or first-match basis, against each received packet. After you configure and deploy access rules from Security Manager to a device and enable logging on the device monitored by MARS, a log entry is created when an access rule matches the network traffic that the device is processing and the action defined in the rule is used to decide if traffic needs to be permitted. An incident is generated in MARS after the log associated with an access rule is received from the device.

In MARS, an incident is a chain of events that are correlated by a rule to signal an attack upon your network. MARS simplifies and expedites the detection, mitigation, reporting, and analysis of the incident. The Network Summary dashboard, the Query Results pages, and the Incident pages help to detect recent incidents and show the rules and the events that compose them.

Using MARS, you can also navigate from messages that are generated during the establishment or tearing down of a TCP, UDP, or ICMP connection to the permit ACE in Security Manager for that specific syslog. You can then edit the access rule generating the MARS event or incident to update the action the device must take in response to a receiving packet.

Before You Begin

- Make sure you have performed all the tasks in the Checklist for Policy Table Lookup from MARS, page 17-13.
- Make sure that Security Manager can be reached from MARS.
- In the Query Reports page, the following result formats are supported for access rule lookup:
  - All Matching Events.
  - All Matching Event Raw Messages.
  - All Matching Sessions.
  - All Matching Sessions, Custom Columns (when Reporting Device Set is selected as one of the custom columns).

To look up and modify the access rule in the policy table of Security Manager from an incident in MARS, follow these steps:

Step 1 Log in to the MARS Local Controller. The Dashboard page is displayed with the Summary tab selected.

If you selected the authentication option to use MARS credentials for policy lookup, log in as an Administrator or Security Analyst to be able to modify the matched access rules. If you selected the option to use Security Manager credentials for policy lookup, the MARS login user role does not matter.

Step 2 Identify the incident or event to investigate from the Query Results page or the Incident Details page.

- To navigate to the Query Results page, run a query to return events matching the specified query criteria. For example, if you run a query to return events ranked by time with the most current first from the Query/Reports tab, the Query Results page appears as shown in Figure 17-6. Click the Security Manager icon in the Reporting Device column from the query results.
- To navigate to the Incident Details page (see Figure 17-7), do one of the following:
  - From the Query/Reports tab, run a query to return incidents ranked by either number of sessions or bytes transmitted that contain events that meet the query criteria. Click the link in the Incident ID column from the query results.
  - From the Recent Incidents section of the Dashboard (see Figure 17-8), click the link in the Incident ID column.
  - Click the Incidents tab to navigate to the Incidents page (see Figure 17-9), which displays recent incidents, and click the link in the Incident ID column.
  - Search for the Incident ID by entering the ID in the appropriate field and clicking Show beside it.

Step 3 Click the Security Manager icon in the Reporting Device field to invoke the Security Manager policy table lookup.

If you selected the option to be prompted for credentials to log in to Security Manager for policy table lookup, a login dialog box is displayed. Otherwise, one of three popup windows is displayed.

Step 4 Enter the Security Manager login credentials and click **OK**.

You are prompted for credentials the first time you start a new MARS session. These credentials are cached until the session expires or you open a fresh session.

Note This dialog box is not displayed if you chose to use MARS credentials for logging in to Security Manager, or selected the check box to save Security Manager credentials when you performed the policy table lookup earlier.

If you access the MARS GUI using Internet Explorer, it is possible that the password is automatically entered in the login dialog box after you enter the username. This behavior occurs if you configured your browser to remember passwords. See the "Interoperation of MARS and Security Manager" chapter in the *FAQ and Troubleshooting Guide for Cisco Security Manager 3.2* for information on how cached passwords can be cleared or the caching feature can be disabled.

One of the following three popup windows may appear:

- Multiple Events window— Lists all reporting device events in the session, this window appears in this step when there are two or more events in the session. See Figure 17-3. Go to Step 5.
- Multiple Devices window—Lists all matching reporting devices that meet criteria available to MARS. This window appears when there are two or more matching devices. See Figure 17-4. Go to Step 6.
- Policy Table window—Lists the policy table of the reporting device. Access rules that match the MARS criteria are highlighted, this window appears in this step when there is one event and a unique reporting device identified. See Figure 17-5. For a detailed description of how to work with the policy table popup window, see Examining and Editing Highlighted Rules. For a description of the elements in the Policy Query window, see Read-Only Security Manager Policy Lookup Page for Access Rules, page 17-30.

Figure 17-3 MARS Multiple Events Pop-up Window

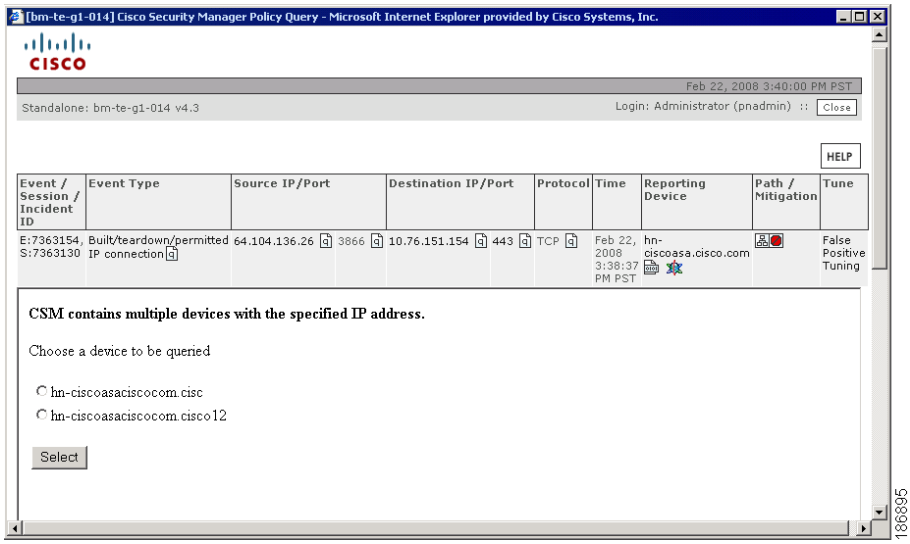


Figure 17-4 MARS Multiple Devices Pop-up Window

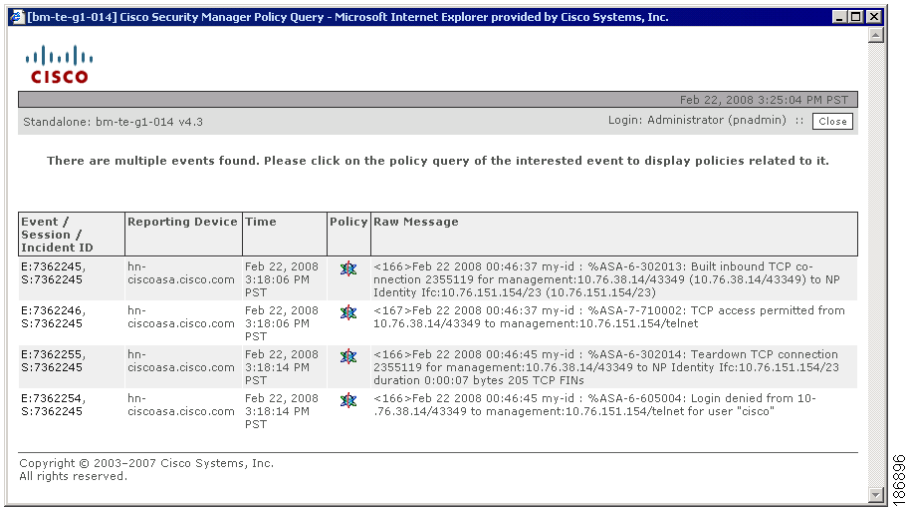
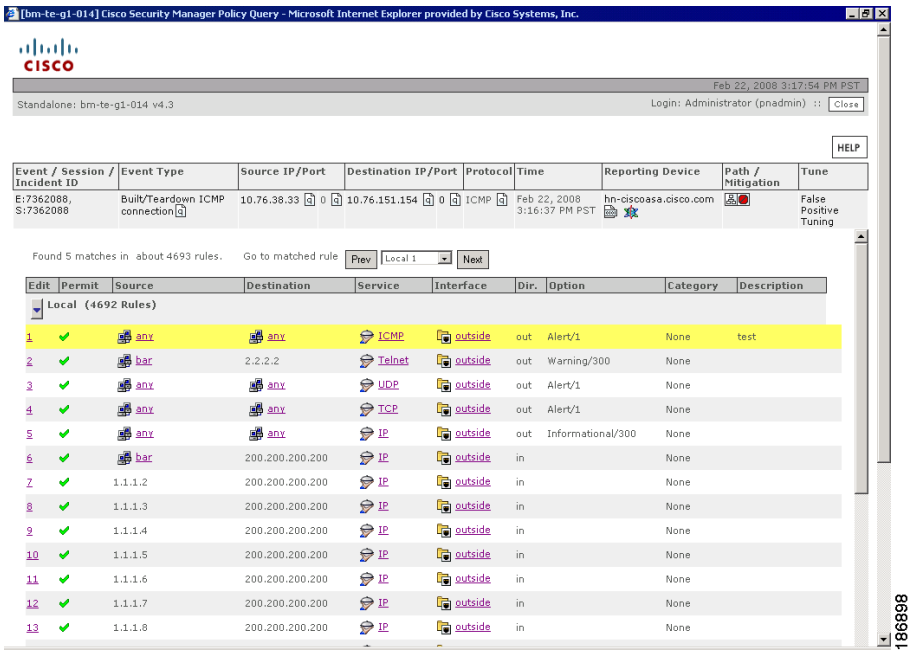


Figure 17-5 Read-Only Access Rule Table Pop-up Window



Step 5 (Optional) If the Multiple Events window is displayed, click the Security Manager icon in the Policy field of the appropriate event. One of the following two popup windows may appear:

- Multiple Devices window. Go to Step 6.
- Policy Table window. For a detailed description of how to work with the policy table popup window, see Examining and Editing Highlighted Rules. For a description of the elements in the Policy Query window, see Read-Only Security Manager Policy Lookup Page for Access Rules, page 17-30.

Step 6 (Optional) If the Multiple Devices popup window is displayed, click the radio button next to the appropriate reporting device. Click **Select**. The read-only access rule table popup window appears for the selected device.

The access rules that match the MARS query criteria are highlighted. The access rules displayed in the read-only policy table window depend on whether an instance of the Security Manager client is running and whether Workflow or non-Workflow mode is enabled. For more information, see Task 6 in the Taskflow for Policy Table Query from MARS Events, page 17-2.

If there are more rules in the access rule table than can displayed in a single page, they are displayed across several pages and you can navigate back and forth. Pagination allows you to display a maximum number of items per page. Additional items carry over to the next page. You choose the number of items to display per page from the Rows per page drop-down list. Select a value from the Go to page drop-down list to navigate to the page number you desire, and click **Prev** or **Next** to navigate between pages.

To switch between matched rules, click **Prev** or **Next**, as required, beside the Go to matched policy drop-down list for each highlighted access rule. Select the first or last rule number from the Go to matched policy list to navigate to the first or last highlighted access rule. If multiple access rules match the query criteria, the first matching rule is highlighted, regardless of whether the page in which the match is found is the first page of the access rule table or not.

If an access rule contains network/host, interface, or service objects, you can click the object in the read-only policy lookup table to view the definitions of these objects in a popup window.

Step 7 Click the hyperlink in the rule number under the No. column for a highlighted access rule.

Note If an instance of the Security Manager client is running, the same instance is reused for the policy table lookup. If the Security Manager client session has timed out or is not open, a new client session is started. If the Security Manager client is not installed on the system, you are prompted to install the Security Manager client and the page to download the client software is opened.

Note When you try to start the Security Manager client from the read-only policy query window in MARS, the File Download dialog box appears prompting you to confirm whether you want to download the CsmContentProvider file to your system. This dialog box appears because of security settings in Internet Explorer. To cause the Open button to be displayed in this dialog box during policy lookup, see the "Interoperation of MARS and Security Manager" chapter in the *FAQ and Troubleshooting Guide for Cisco Security Manager 3.2*.

The Security Manager client window is activated and the Access Rules page appears with the access rule that generated the event highlighted in the policy table. You can modify the access rule to control the flow of network packets and deploy the updated policy to the device to refine network protection.

If the highlighted access rule contains network/host, service, or interface objects, right-click the appropriate table cell of the rule in the Access Rules page and select **Show <object> Contents** from the shortcut menu to view the list of flattened values of the object.

Step 8 Click **Transcript Details** at the bottom of the read-only access rule table to open a popup window that displays information about the raw syslog for the event that you selected in MARS and the parsed format of the syslog after it is processed by Security Manager to find access rules that generated the syslog. These details enable you to understand the taskflow of the access rule lookup query and are informational messages, which can used to troubleshoot errors.

Step 9 Click the **CS Manager Details** link at the bottom of the page to open a dialog box displaying the server name, username used to log in to Security Manager, whether Workflow mode is enabled, and the activity from which the signature details are retrieved. Click the Close icon to close the dialog box.

Navigating to IPS Signature Policy in Security Manager from MARS

Sensors scan network packets using signatures to detect attacks or other misuses of network resources. When the sensor finds a match for an incoming packet with the signature, it takes some action, such as logging the event. If the signatures are configured on the sensor using Security Manager and the sensor is monitored by MARS, the sensor publishes the logs to MARS. From the Query page, you can define the query parameters and run a query to return events or incidents generated by signatures configured on the sensor. You can click the Security Manager icon from the returned events or raw messages associated with events. Alternatively, you can select a particular incident ID from the returned query results and view the details associated with the incident. From the Incident Details page, you can click the Security Manager icon in the Reporting Device column for the event that you want to examine.

Note In the Query Reports page, the following result formats are supported for access rule lookup:

All Matching Events.

All Matching Event Raw Messages.

All Matching Sessions.

All Matching Sessions, Custom Columns (when Reporting Device Set is selected as one of the custom columns).

A collection of events generated by sensors are also displayed in the Incidents page from which you can select an incident ID and navigate to the signature policy in Security Manager. You can then edit their parameters (tune them) to achieve optimal performance on your network, and particularly to minimize false positives and false negatives.

Before You Begin

- Make sure you have performed all the tasks in the Checklist for Policy Table Lookup from MARS, page 17-13.
- Make sure that Security Manager can be reached from MARS.

To look up and modify an IPS signature in the signature summary table of Security Manager from an incident in MARS, follow these steps:

Step 1 Log in to the MARS Local Controller. The Dashboard page is displayed with the Summary tab selected.

If you selected the authentication option to use MARS credentials for policy lookup, log in as an Administrator or Security Analyst to be able to modify the matched access rules. If you selected the option to use Security Manager credentials for policy lookup, the MARS login user role does not matter.

Step 2 Identify the incident or event to investigate from the Query Results page or the Incident Details page in one of the following ways:

- To navigate to the Query Results page, run a query to return events matching the specified query criteria. For example, if you run a query to return events ranked by time with the most current first from the Query/Reports tab, the Query Results page appears as shown in Figure 17-6. Click the Security Manager icon in the Reporting Device column from the query results.
- To navigate to the Incident Details page (see Figure 17-7), do one of the following:
  - From the Query/Reports tab, run a query to return incidents ranked by either number of sessions or bytes transmitted that contain events that meet the query criteria. Click the link in the Incident ID column from the query results.
  - From the Recent Incidents section of the Dashboard (see Figure 17-8), click the link in the Incident ID column.
  - Click the Incidents tab to navigate to the Incidents page (see Figure 17-9), which displays recent incidents, and click the link in the Incident ID column.
  - Search for the Incident ID by entering the ID in the appropriate field and clicking Show beside it.

Figure 17-6 Query Results Page with Matching Events

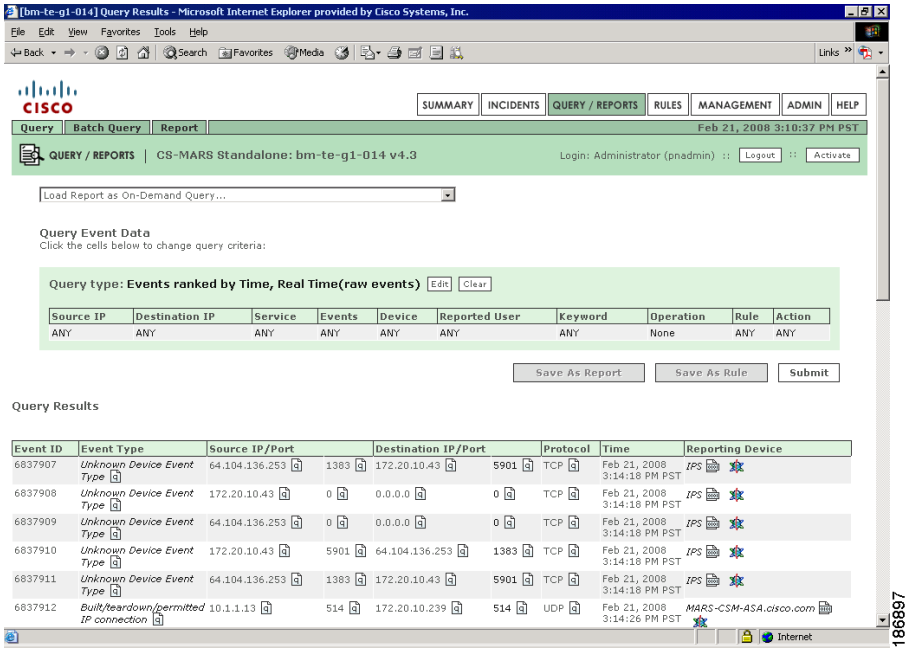


Figure 17-7 Incident Details Page

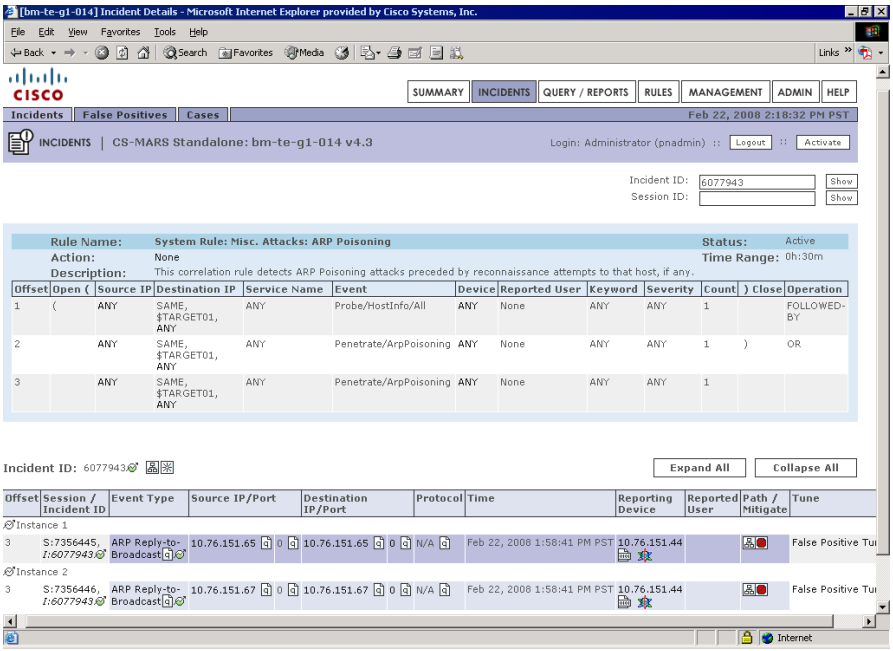


Figure 17-8 Recent Incidents on MARS Summary Page

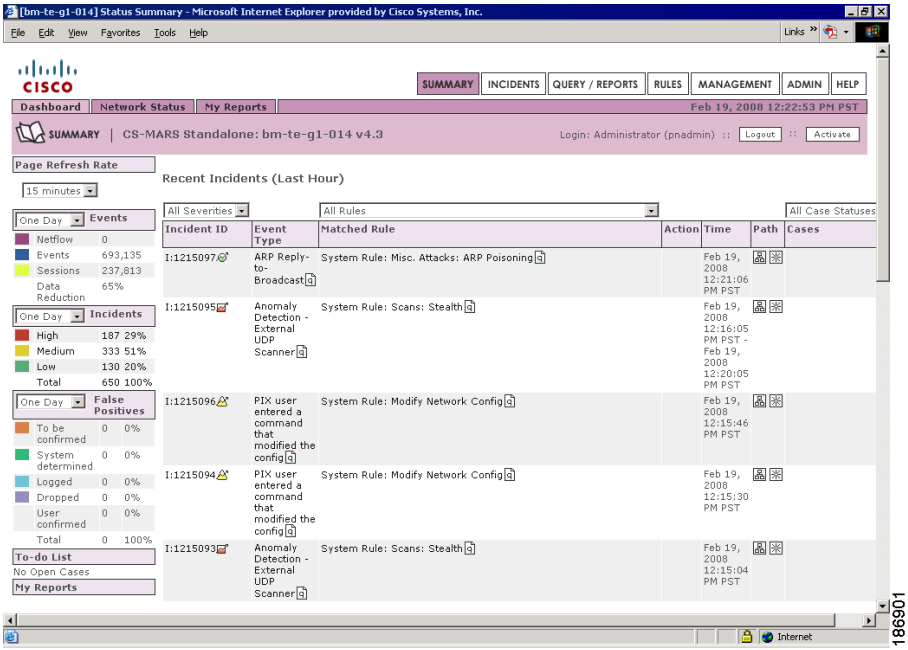
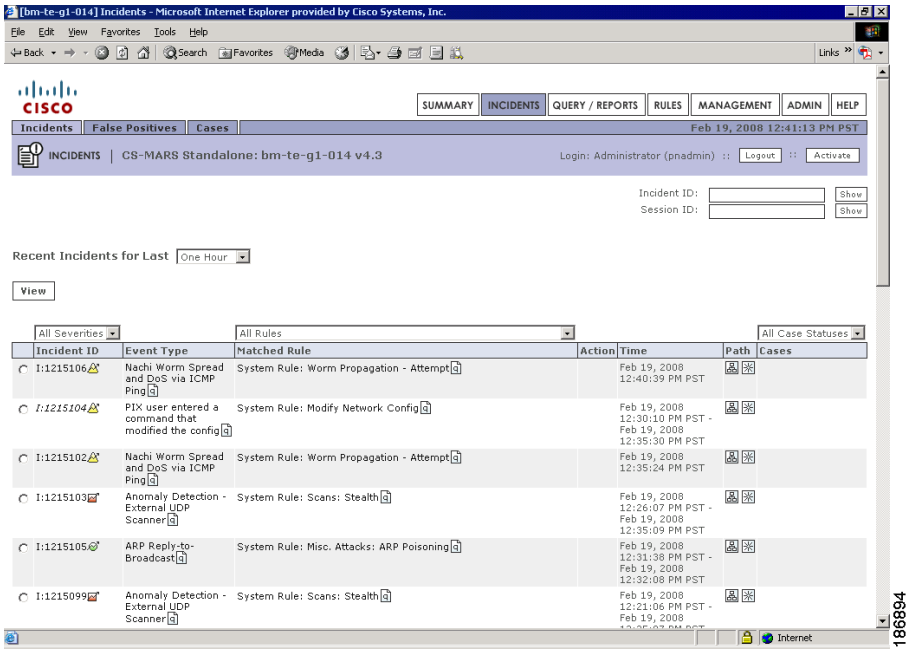


Figure 17-9 MARS Incidents Page



Step 3 Click the Security Manager icon in the Reporting Device field to invoke the Security Manager policy table lookup. If you selected the option to be prompted for credentials to log in to Security Manager for policy table lookup, a login section is displayed in the Policy Query popup window. See Figure 17-10Go to Step 4.

Otherwise, the Cisco Security Manager Policy Query popup window is displayed with the signature parameters in read-only mode. See Figure 17-11Go to Step 5. For a description of the elements in the Policy Query window, see Read-Only Security Manager Policy Lookup Page for an IPS Signature, page 17-33.

Note Events triggered by custom signature configured on a sensor are categorized as “Unknown Device Event Type” in the MARS GUI and the Security Manager icon is displayed for these events to enable policy lookup.

Figure 17-10 Read-Only Signature Policy Pop-up Window with Login Section

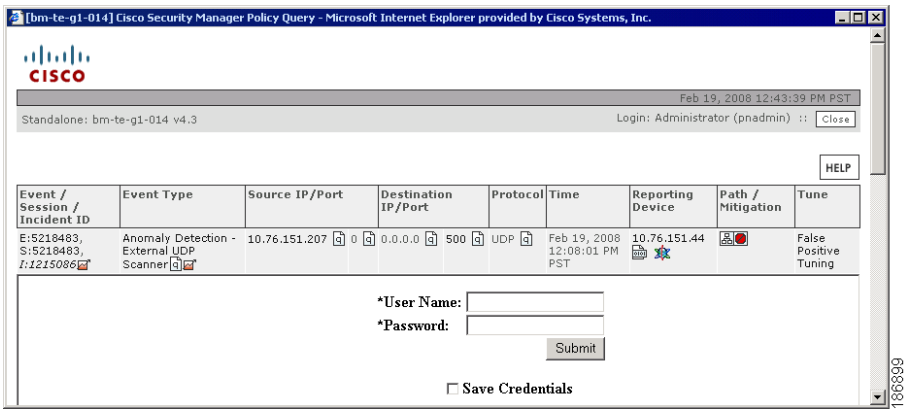
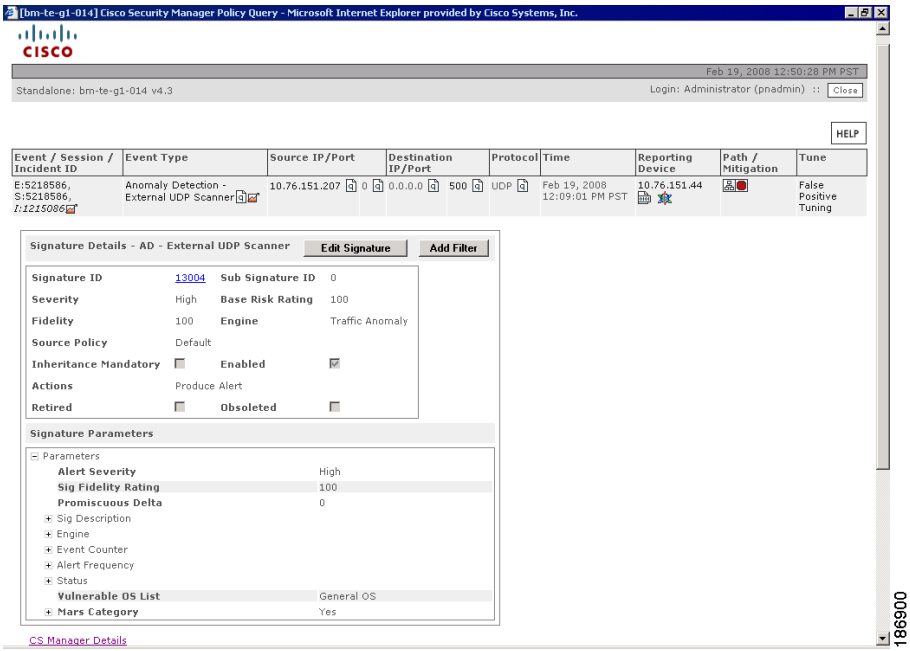


Figure 17-11 Read-Only Signature Policy Pop-up Window with Matching Signature Parameters



Step 4 Enter the Security Manager login credentials and click **OK**. The Cisco Security Manager Policy Query popup window is displayed with the signature parameters in read-only mode. For a description of the elements in the Policy Query window, see Read-Only Security Manager Policy Lookup Page for an IPS Signature, page 17-33.

You are prompted for credentials the first time you start a new MARS session. These credentials are cached until the session expires or you open a fresh session.

Note This dialog box is not displayed if you chose to use MARS credentials for logging in to Security Manager, or selected the check box to save Security Manager credentials when you performed the policy table lookup earlier.

If you access the MARS GUI using Internet Explorer, it is possible that the password is automatically entered in the login dialog box after you enter the username. This behavior occurs if you configured your browser to remember passwords. See the "Interoperation of MARS and Security Manager" chapter in the *FAQ and Troubleshooting Guide for Cisco Security Manager 3.2* for information on how cached passwords can be cleared or the caching feature can be disabled.

Step 5 Do one of the following:

- Click **Edit Signature** to open the Signatures page in Security Manager. The IPS signature that generated the event is highlighted in the policy table. You can tune the signature parameters to detect network intrusions.

  Note If an instance of the Security Manager client is running, the same instance is reused for the policy table lookup. If the Security Manager client session has timed out or is not open, a new client session is started. If the Security Manager client is not installed on the system, you are prompted to install the Security Manager client and the page to download the client software is opened.

- Click **Add Filter** to open the Add Event Action Filter dialog box in Security Manager to remove specific actions from an event or to discard an entire event and prevent further processing by the sensor. The fields that specify the actions that should be removed from the event, the percentage of packets to deny for deny attacker features, and the port and IP address used by the attacker host are populated with values derived from the event logged in MARS. The remaining fields in the Add Event Action Filter dialog box are displayed with default values. When you save the event action filter, it is stored as a local policy filter for that specific device.
- Click the **CS Manager Details** link at the bottom of the page to open a dialog box displaying the server name, username used to log in to Security Manager, whether Workflow mode is enabled, and the activity from which the signature details are retrieved. Click the Close icon to close the dialog box.

Note When you try to start the Security Manager client from the read-only policy query window in MARS, the File Download dialog box appears prompting you to confirm whether you want to download the CsmContentProvider file to your system. This dialog box appears because of security settings in Internet Explorer. To cause the Open button to be displayed in this dialog box during policy lookup, see the "Interoperation of MARS and Security Manager" chapter in the *FAQ and Troubleshooting Guide for Cisco Security Manager 3.2*.

Read-Only Security Manager Policy Lookup Page for Access Rules

Use the Cisco Security Manager Policy Query page in the MARS GUI to view the access rule that triggered the incident that you want to examine. This page takes one of the following forms, depending on the number of events and devices that match the incident you are investigating.

- A list of all reporting device events in the session when there are two or more events in the session. Click the Security Manager icon in the Reporting Device field for the event whose access rules you want to lookup. If multiple devices match the MARS query criteria, the page refreshes to display the information as described in the next bullet. If a unique device can be identified for the event, the page assumes the form as described in the third bullet.
- A list all matching reporting devices that meet criteria available to MARS when there are two or more matching devices. A radio button is displayed next to each device to select the device for which you want to lookup access rules. Selecting a device causes the page to display the information as described in the next bullet.
- Access rule table of the reporting device. Access rules that match the MARS criteria are highlighted, this window appears in this step when there is one event and a unique Security Manager device identified.
- An error message if no device matches the MARS query criteria.

Navigation Path

To access the read-only policy lookup page for access rules, do one of the following:

1. From the Query/Reports tab, run a query to return events or raw messages associated with events that meet the query criteria to display the Query Results page. Click the Security Manager icon in the Reporting Device column from the query results.
2. In the MARS GUI, navigate to the Incident Details page in one of the following ways:
   - From the Query/Reports tab, run a query to return incidents ranked by either number of sessions or bytes transmitted that contain events that meet the query criteria. Click the link in the Incident ID column from the query results.
   - From the Recent Incidents section of the Dashboard, click the link in the Incident ID column.
   - Click the Incidents tab to navigate to the Incidents page, which displays recent incidents, and click the link in the Incident ID column.
   - Search for the Incident ID by entering the ID in the appropriate field and clicking Show beside it.

   Click the Security Manager icon in the Reporting Device field of the Incident Details page for incidents generated by access rules.

Note Although this page contains elements other than those listed in the field reference table, these elements are read-only or are used to navigate to other pages in MARS. Only the elements with which you can perform actions specific to access rule table lookup are listed in the table.

Note Even though the Security Manager icon in the event displayed at the top of the page can be clicked, it only refreshes the page with the same contents. You need to click the hyperlink in the rule number of the read-only policy table to navigate to the Access Rules page in the Security Manager client; clicking this icon does not start the Security Manager client.

Field Reference

Table 17-2 Read-Only Access Rule Policy Lookup Page

Element	Description
Cisco Security Manager Login	Available only if you selected the option to prompt the user for Security Manager login credentials for access rule lookup and the Security Manager credentials are neither cached nor saved in the MARS database.
User Name	The username for logging in to Security Manager. **Note** The user must have administrative privileges to open the Security Manager client from the read-only access rule table. Otherwise, an error message is displayed when you click the hyperlinked rule number from the No. column of the access rule table.
Password	The password for logging in to Security Manager.
Submit	Sends the entered credentials to Security Manager and displays the read-only access table in the same page, if authentication is successful.
Save Credentials	Available only if the Allow Users to Save Credentials check box is selected in the Reporting Applications tab of MARS. When selected, Security Manager credentials are saved in the MARS database and reused during policy lookup. You are not prompted for credentials during subsequent policy lookup operations if you select this check box.
Access rule policy table	If the Security Manager Login section is displayed, this table appears after MARS is successfully authenticated with Security Manager. Also, if a unique device and a single event cannot be identified for an incident, this table is displayed after you select the required device and event from the list of multiple devices and multiple events.
Go to matched policy	Select the rule number to which you want to navigate in the table.
Prev	Click to move to the matching access rule previous to the one currently highlighted in the table.

Table 17-2 Read-Only Access Rule Policy Lookup Page (continued)

Next	Click to move to the matching access rule next to the one currently highlighted in the table.
No.	Identifies the ordered rule number in the table. Click the hyperlink in the rule number to start the Security Manager client with the current row highlighted the access rule table and modify its settings. Hold your cursor over the rule number to view a tooltip. **Note** If an instance of the Security Manager client is already open, the same instance is activated.
Source	Identifies the source network object names or addresses of hosts and networks, for example, 10.1.1.1, 10.1.1.1/32, 10.1.1.1/255.255.255.255 and net10. Clickable only if it represents a network object. Clicking the object displays the contents of the object in a popup window. The source IP address or hostname contained in the object is highlighted in the popup window if it matches with the source IP address in the syslog that generated this rule.
Destination	Identifies the destination network/host object names or addresses of hosts or networks. Clickable only if it represents a network object. Clicking the object displays the contents of the object in a popup window. The destination IP address or hostname contained in the object is highlighted in the popup window if it matches with the destination IP address in the syslog that generated this rule.
Service	Identifies service objects that specify protocol and port information. Clickable only if it represents a service object. Clicking the object displays the contents of the object in a popup window. The protocol and port contained in the interface object are highlighted in the popup window if they match with the protocol in the syslog that generated this rule. However, this feature of highlighted entries is supported only for TCP-based and UDP-based rules.

Table 17-2 Read-Only Access Rule Policy Lookup Page (continued)

Interface	Identifies the logical name of the interface (interface role) or physical interface to which a rule is assigned. Clickable only if it represents an interface object. Clicking the object displays the contents of the object in a popup window. Unlike network/host and service objects, the flattened-out interface objects that match with the interface value in the syslog that generated this rule are not highlighted in the popup window.
Go to page	Select the page number to which you want to navigate. Click **Prev**and **Next** on either side of the drop-down list to navigate between pages.
Rows per page	Select the number of rows that you want to be displayed in each page of the access rule table.
Transcript Details	Click to open a dialog box displaying information about the raw syslog for the event that you selected in MARS and the parsed format of the syslog after it is processed by Security Manager to find access rules that generated the syslog. These details enable you to understand the taskflow of the access rule lookup query and are informational messages, which can be used to troubleshoot errors.
CS Manager Details	Click open a dialog box displaying the server name, username used to log in to Security Manager, whether Workflow mode is enabled, and the activity from which the signature details are retrieved.

Read-Only Security Manager Policy Lookup Page for an IPS Signature

Use the Cisco Security Manager Policy Query page in the MARS GUI to view the signature that triggered the incident that you want to examine. From this page, you can open the Security Manager client to edit the signature parameters or define an event action filter to remove specific actions from an event.

Navigation Path

To access the read-only policy lookup page for IPS signatures, do one of the following:

1. From the Query/Reports tab, run a query to return events or raw messages associated with events that meet the query criteria to display the Query Results page. Click the Security Manager icon in the Reporting Device column from the query results.
2. In the MARS GUI, navigate to the Incident Details page in one of the following ways:

- From the Query/Reports tab, run a query to return incidents ranked by either number of sessions or bytes transmitted that contain events that meet the query criteria. Click the link in the Incident ID column from the query results.
- From the Recent Incidents section of the Dashboard, click the link in the Incident ID column.
- Click the **Incidents** tab to navigate to the Incidents page, which displays recent incidents, and click the link in the Incident ID column.
- Search for the Incident ID by entering the ID in the appropriate field and clicking Show beside it.

Click the Security Manager icon in the Reporting Device field of the Incident Details page for incidents generated by signatures.

Note Although this page contains elements other than those listed in the field reference table, these elements are either read-only or are used to navigate to other pages in MARS. Only the elements with which you can perform actions specific to signature policy lookup are listed in the table.

Even though the Security Manager icon in the event displayed at the top of the page can be clicked, it only refreshes the page with the same contents. You need to click Edit Signature to navigate to the Signatures page in the Security Manager client; clicking this icon does not start the Security Manager client.

Field Reference

Table 17-3 Read-Only Signature Policy Lookup Page

Element	Description
Cisco Security Manager Login	Available only if you selected the option to prompt the user for Security Manager login credentials for signature rule lookup in the Reporting Applications tab and the Security Manager credentials are neither cached nor saved in the MARS database.
User Name	The username for logging in to Security Manager. **Note** The user must have administrative privileges to open the Security Manager client from the read-only signature details page. Otherwise, an error message is displayed when you click Edit Signature or Add Filter.
Password	The password for logging in to Security Manager.
Submit	Sends the entered credentials to Security Manager and displays the read-only signature parameters in the same page, if authentication is successful.

Table 17-3 Read-Only Signature Policy Lookup Page (continued)

Save Credentials	Available only if the Allow Users to Save Credentials check box is selected in the Reporting Applications tab of MARS. When selected, Security Manager credentials are saved in the MARS database and reused during policy lookup. You are not prompted for credentials during subsequent policy lookup operations if you select this check box.
Signature Details	If the Cisco Security Manager Login section is displayed, this section appears after MARS is successfully authenticated with Security Manager. Otherwise, these details are displayed immediately after the policy query lookup page is opened.
Edit Signature	Click to open the Signatures page in Security Manager. The IPS signature that generated the event is highlighted in the policy table. If an instance of the Security Manager client is already open, the same instance is activated. If the Security Manager client is not installed on the system, you are prompted to install the Security Manager client and the page to download the client software is opened.
Add Filter	Opens the Add Event Action Filter dialog box in Security Manager with the Actions to Subtract, % to Deny, Attacker Address, and Attacker Port fields populated with values derived from the MARS event. The remaining fields are displayed with default values.
Signature ID	Identifies the unique numerical value assigned to this signature. The signature ID contains hyperlinks to the Cisco Network Security Database (NSDB). Clicking on the link in the ID column will trigger the opening of an external browser window that opens to the entry in Security Center (MySDN) for that signature.

Table 17-3 Read-Only Signature Policy Lookup Page (continued)

Signature Parameters	Displays the built-in micro-engine parameters for a particular signature. These parameters determine how the signature is configured and applied to an incoming packet. Click the + icon beside the Parameters option to expand the tree and display the available signature parameters. If a + icon appears beside any of the items in the expanded list, it indicates that more options are available for this parameter.
CS Manager Details	Click open a dialog box displaying the server name, username used to log in to Security Manager, whether Workflow mode is enabled, and the activity from which the signature details are retrieved.