



CHAPTER 13

Interoperation of MARS and Security Manager

This chapter contains the following topics:

- [FAQs about Policy Lookup from a MARS Event](#), page 13-1
- [Policy Lookup for Events Generated by Devices with Multiple Contexts](#), page 13-12
- [FAQs about MARS Events Lookup from a Security Manager Policy](#), page 13-12
- [Changing the Association of the MARS Appliance with a Device](#), page 13-18
- [Configuring Required Browser Settings for Policy and Events Lookup](#), page 13-19



Note

For more detailed information on the interoperation of MARS and Security Manager, see the “MARS Events Lookup from a Security Manager Policy” section in the [installation guide for Cisco Security Manager](#) for your release.

FAQs about Policy Lookup from a MARS Event

This section answers the following questions about Security Manager policy lookup from MARS events:

- [Q. Why do I get an error message when I click the Security Manager icon for a connection-teardown event in the MARS GUI?](#)
- [Q. Why am I asked to select a different event, when I click the Security Manager icon for an event?](#)
- [Q. Why is an error message displayed stating that the syslog is invalid even when I click the Security Manager icon for one of the syslogs supported for policy lookup?](#)
- [Q. During policy lookup, I receive an “An internal error has occurred” message. Why?](#)
- [Q. What are the possible causes for not finding a matching access rule during policy lookup from an event?](#)
- [Q. I get an error stating that the access rule on the device is not synchronized with the one in Security Manager during policy lookup. Why?](#)
- [Q. Why does an error message appear stating that an implicit permit statement in the access rule generated the selected event when I perform lookup?](#)
- [Q. Why am I seeing a discrepancy in the access rule that is shown as matched in the read-only policy query page of MARS and the Access Rules page in Security Manager?](#)
- [Q. Can I look up the signature matching an event generated by a virtual sensor?](#)

- Q. Why am I not seeing the Security Manager icon for Packet Data and Context Data events, although they are events reported by Cisco IDS 4.x and Cisco IPS 5.x devices?
- Q. What are the various ways in which I can navigate to a page in MARS in which the Security Manager icon is displayed?
- Q. When and why is the multiple events window displayed during access rule lookup?
- Q. Why is the multiple devices window displayed during policy lookup?
- Q. Why is the Save Credentials check box in the read-only policy query window disabled?
- Q. Can I start Security Manager from the read-only policy query window without having the client installed on my system?
- Q. If I did not have a Security Manager client instance open at the time of policy lookup, is it terminated when I log out of the MARS session?
- Q. What are the different authentication mechanisms for policy lookup?
- Q. Why do I get an error stating that the device is not found in Security Manager?
- Q. Why is the access rule table displayed after lookup in the read-only policy query window different from the one configured in Security Manager?
- Q. Can I test the connectivity between MARS and Security Manager before running a policy lookup query?
- Q. Can I add a Security Manager running 3.0.1, 3.0.2, or 3.1.x to a MARS appliance running 4.3.4 or 5.3.4?
- Q. Under what circumstances are the Security Manager credentials in the User Management page enabled or dimmed out?
- Q. Is it always necessary to configure the MARS user account in the Security Manager database to perform policy lookup?
- Q. Why is a new Security Manager client instance opened even though a session is currently active?
- Q. Why is the password automatically populated in the login section of the read-only policy query window after I enter the username?
- Q. What are the device types and their OS versions that are supported for policy lookup?
- Q. What is the scope of the search on the Access Rules page or Signatures page of Security Manager when a policy lookup query is run?
- Q. How is policy lookup performed if Workflow mode is enabled in Security Manager?
- Q. How is policy lookup performed if non-Workflow mode is enabled in Security Manager?
- Q. Can I perform any other task from the read-only policy query page for a signature-fired event, besides tuning of signatures?
- Q. Can I check whether Workflow mode is enabled or not and details of the activity from which the read-only policy table is retrieved?
- Q. What are the supported MARS user roles to modify the Security Manager credentials in the User Management page of MARS?
- Q. Do I need to possess administrative privileges to add a Security Manager to MARS?
- Q. Is the Security Manager icon displayed only for events that have 5-tuple data?
- Q. Why do I receive an error stating that I do not have necessary privileges to start the Security Manager client from the read-only policy query window?

- Q.What are the ACS, Common Services, and MARS roles that are supported to start the Security Manager client from the read-only policy query window?
 - Q.What are the types of MARS events for which the Security Manager icon is displayed?
 - Q.Why does policy lookup take a long time for certain events?
 - Q.Can I view the contents of objects contained in the matching access rules from the read-only policy query popup window?
 - Q.I see the Security Manager icon for “Unknown Device Event Type” events. What do these events represent?
 - Q.Are the Security Manager login credentials that I enter in the read-only policy query popup window cached until the current session is active?
 - Q.When I perform policy lookup for an event for the second time, it is faster than the previous occasion. What could be the reason for this behavior?
 - Q.During policy lookup, I get an error stating that a temporary connection problem occurred. How can I correct this problem?
 - Q.Why am I prompted for credentials to log in to Security Manager, even though I selected the option to use MARS credentials for policy lookup?
 - Q.Why is an error message displayed when I try to Start Security Manager from the read-only policy window for the matching rule or signature?
 - Q.What are the system message log IDs supported for policy lookup for events generated by security appliances and routers?
 - Q.How many Security Manager servers can I add to a MARS Local Controller to perform policy lookup?
 - Q.My MARS Local Controller is administered by a Global Controller. Can I perform policy lookup for events generated on the Local Controller from the Global Controller interface?
 - Q.There are two places in which I need to enter the Security Manager username and password. What is the difference between the credentials in the Reporting Applications tab and the one in the User Management page of MARS?
- Q.** Why do I get an error message when I click the Security Manager icon for a connection-teardown event in the MARS GUI?
- A.** 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.
- Q.** Why am I asked to select a different event, when I click the Security Manager icon for an event?
- A.** 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.



Note For more information on the list of syslog supported for policy lookup, see “Security Appliance and Router System Log Messages Supported for Policy Lookup” in the *User Guide for Cisco Security Manager 3.2*.

- Q.** Why is an error message displayed stating that the syslog is invalid even when I click the Security Manager icon for one of the syslogs supported for policy lookup?
- A.** This problem occurs if the syslog is not parsed by Security Manager and the syslog format received from MARS is incorrect. In such cases, you need to select a different syslog and perform policy lookup.
- Q.** During policy lookup, I receive an “An internal error has occurred” message. Why?
- A.** 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.
- Q.** What are the possible causes for not finding a matching access rule during policy lookup from an event?
- A.** An access rule matching the selected event might not be found in any of the following cases:
- If no access rule is configured on the lower security interface in the “in” direction of the device for inbound traffic for the selected event.
 - If the access rule specified in the syslog is not available on the device. Make sure that the device is added to Security Manager and access rules are configured on it.
 - If the event is generated by outbound traffic setup/teardown syslog with an access rule configured on the higher security interface in the “in” direction.
 - 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.
- Q.** I get an error stating that the access rule on the device is not synchronized with the one in Security Manager during policy lookup. Why?
- A.** This error can occur under any of the following circumstances:
- When an event is generated by an access rule present on the lower security interface in the “in” direction for inbound traffic and no matching rule is found in Security Manager.
 - When an event is generated by an access rule present on the higher security interface in the “in” direction for outbound traffic and no matching rule is found in Security Manager.
 - When an event is generated by an access rule present on the lower security interface in the “out” direction for outbound traffic and no matching rule is found in Security Manager.
 - 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.
- Q.** Why does an error message appear stating that an implicit permit statement in the access rule generated the selected event when I perform lookup?

- A.** This error occurs because you performed 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. 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.
- Q.** Why am I seeing a discrepancy in the access rule that is shown as matched in the read-only policy query page of MARS and the Access Rules page in Security Manager?
- A.** 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. For example, if the first row in the read-only policy query window is shown as highlighted and is TCP-based, and you change the order of the rules in the Access Rules page of Security Manager to move an ICMP-based rule to the top of the table, the ICMP-based rule (not the TCP-based rule) is highlighted when you start the Security Manager client from MARS.
- Q.** Can I look up the signature matching an event generated by a virtual sensor?
- A.** No. 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.
- Q.** Why am I not seeing the Security Manager icon for Packet Data and Context Data events, although they are events reported by Cisco IDS 4.x and Cisco IPS 5.x devices?
- A.** 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 and Context Data events in the MARS GUI for policy lookup.
- Q.** What are the various ways in which I can navigate to a page in MARS in which the Security Manager icon is displayed?
- A.** You can perform policy lookup in any one of the following ways from the MARS GUI:
- From the Query Reports page, run a query with one of the following result formats: All Matching Events, All Matching Event Raw Messages, All Matching Sessions, or All Matching Sessions, Custom Columns (when Reporting Device Set is selected as one of the custom columns).
 - 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.
- Q.** When and why is the multiple events window displayed during access rule lookup?

- A.** This window appears when you run a query for events with All Matching Sessions, or All Matching Sessions, Custom Columns as the result format and if there are two or more events in a session. From the multiple events window, click the Security Manager icon for the event that you want to examine to display the read-only policy query popup window.
- Q.** Why is the multiple devices window displayed during policy lookup?
- A.** Although MARS tries to identify a unique device by matching the host name, domain name, and reporting IP address of the device that generated the event against the corresponding details in Security Manager, the multiple devices window is displayed when there are two or more devices that match the device lookup process between MARS and Security Manager. From the multiple devices window, you can select the device for which you want to view and modify the configured access rules.
- Q.** Why is the Save Credentials check box in the read-only policy query window disabled?
- A.** This check box is available only if the Allow Users to Save Credentials check box is selected in the Device Discovery-Cisco Security Manager ANY page. 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. Otherwise, you are prompted 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.
- Q.** Can I start Security Manager from the read-only policy query window without having the client installed on my system?
- A.** Yes. 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.
- Q.** If I did not have a Security Manager client instance open at the time of policy lookup, is it terminated when I log out of the MARS session?
- A.** 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.
- Q.** What are the different authentication mechanisms for policy lookup?
- A.** You can enable MARS to either contact Security Manager using the credentials that you entered while logging in to MARS or use Security Manager credentials for MARS to authenticate with Security Manager during policy lookup. You can configure these settings under the Cross-Launch Authentication Settings section in the Reporting Applications tab of MARS. See “Adding a Security Manager Server to MARS” in the *User Guide for Cisco Security Manager 3.2* for details.
- Q.** Why do I get an error stating that the device is not found in Security Manager?
- A.** 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.
- Q.** Why is the access rule table displayed after lookup in the read-only policy query window different from the one configured in Security Manager?

- A.** This problem occurs because 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.
- Q.** Can I test the connectivity between MARS and Security Manager before running a policy lookup query?
- A.** Yes, you can test the connectivity between MARS and Security Manager any time before policy lookup, either during the process of adding Security Manager to MARS or after addition. To do this task, navigate to the Device Discovery-Cisco Security Manager ANY page, then click **Test Connectivity** to verify that the settings are correct and that the MARS Appliance can communicate with this Security Manager server.
- Q.** Can I add a Security Manager running 3.0.1, 3.0.2, or 3.1.x to a MARS appliance running 4.3.4 or 5.3.4?
- A.** Although you can 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. Make sure that the Security Manager server is running the 3.2 version if you want to lookup the policy table and also, modify matching rules or signatures.
- Q.** Under what circumstances are the Security Manager credentials in the User Management page enabled or dimmed out?
- A.** 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 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.
- Q.** Is it always necessary to configure the MARS user account in the Security Manager database to perform policy lookup?
- A.** 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 do not need to create a separate MARS user account in the Common Services 3.1 UI for authentication purposes.
- Q.** Why is a new Security Manager client instance opened even though a session is currently active?
- A.** This behavior occurs 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.

- Q.** Why is the password automatically populated in the login section of the read-only policy query window after I enter the username?
- A.** 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 [Working with Cached Passwords in Internet Explorer, page 13-19](#) for information on how cached passwords can be cleared or the caching feature can be disabled.
- Q.** What are the device types and their OS versions that are supported for policy lookup?
- A.** 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. See “Devices and OS Versions Supported by Both Security Manager and MARS” in the *User Guide for Cisco Security Manager 3.2*.
- Q.** What is the scope of the search on the Access Rules page or Signatures page of Security Manager when a policy lookup query is run?
- A.** 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).
- Q.** How is policy lookup performed if Workflow mode is enabled in Security Manager?
- A.** 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.
- Q.** How is policy lookup performed if non-Workflow mode is enabled in Security Manager?
- A.** 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.
- Q.** Can I perform any other task from the read-only policy query page for a signature-fired event, besides tuning of signatures?
- A.** Yes, you can also configure an event action filter to remove one or more actions from the read-only policy query window for a signature event.
- Q.** Can I check whether Workflow mode is enabled or not and details of the activity from which the read-only policy table is retrieved?

- A.** Yes, click the **CS Manager Details** link at the bottom of the Policy Query window 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.
- Q.** What are the supported MARS user roles to modify the Security Manager credentials in the User Management page of MARS?
- A.** 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.
- Q.** Do I need to possess administrative privileges to add a Security Manager to MARS?
- A.** Yes. 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.
- Q.** Is the Security Manager icon displayed only for events that have 5-tuple data?
- A.** No. The Security Manager policy table lookup icon in MARS is displayed for 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.
- Q.** Why do I receive an error stating that I do not have necessary privileges to start the Security Manager client from the read-only policy query window?
- A.** If you used MARS user credentials to perform policy lookup, you might be associated with the Operator or Notifications Only role, which enable to only view matching policies. If you used Security Manager credentials to perform policy lookup, you might be associated with the Help Desk role in CiscoWorks Common Services role or Cisco Secure ACS, which do not enable you to start Security Manager to modify a policy from the read-only popup window in MARS.
- Q.** What are the ACS, Common Services, and MARS roles that are supported to start the Security Manager client from the read-only policy query window?
- A.** The following are the user roles supported to perform policy lookup and modify the matching policy, depending on the authentication server that you are using:
- ACS user roles—Any predefined Cisco Secure ACS roles with the exception of the Help Desk role.
 - Common Services user roles—Approver, Network Operator, Network Administrator, or System Administrator.
 - MARS user roles—Administrator or Security Analyst.
- Q.** What are the types of MARS events for which the Security Manager icon is displayed?
- A.** The Security Manager policy table lookup icon in MARS is displayed only for traffic logs triggered by the following event types:
- 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.
 - Signatures from IPS and IOS IPS devices.

- Q.** Why does policy lookup take a long time for certain events?
- A.** 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. Also, 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.
- Q.** Can I view the contents of objects contained in the matching access rules from the read-only policy query popup window?
- A.** Yes. 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. The contents of the objects that match with the values in the syslog that generated the rule are highlighted. However, expanded object entries are highlighted only for TCP and UDP protocol in service objects, destination object names, and source object names. The Source, Destination, Service, and Interface cells are not clickable if they do not contain objects.
- Q.** I see the Security Manager icon for “Unknown Device Event Type” events. What do these events represent?
- A.** 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.
- Q.** Are the Security Manager login credentials that I enter in the read-only policy query popup window cached until the current session is active?
- A.** Yes. 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.
- Q.** When I perform policy lookup for an event for the second time, it is faster than the previous occasion. What could be the reason for this behavior?
- A.** 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.
- Q.** During policy lookup, I get an error stating that a temporary connection problem occurred. How can I correct this problem?
- A.** This error can occur if the connection between MARS and Security Manager is aborted temporarily and necessary details are not supplied by MARS and Security Manager. In such cases, retry the operation after some time.
- You can also navigate to the Device Discovery-Cisco Security Manager ANY page, then 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.
- Q.** Why am I prompted for credentials to log in to Security Manager, even though I selected the option to use MARS credentials for policy lookup?

- A.** This occurs because you logged in to MARS using an account that is not defined in the Common Services database of Security Manager. You must define the MARS user account on the Security Manager server (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 without being prompted for credentials.
- Q.** Why is an error message displayed when I try to Start Security Manager from the read-only policy window for the matching rule or signature?
- A.** This problem can occur in any one of the following scenarios:
- You did not configure the Security Manager server to use HTTPS for communication with MARS. Before MARS can query the policies defined on the Security Manager server, you must enable HTTPS on the Security Manager server. Because Security Manager runs on Common Services 3.1, you must enable browser-security from the Common Services UI to establish secure communication between Security Manager and MARS. For more information on enabling HTTPS using the Common Services UI, see *User Guide for CiscoWorks Common Services 3.1*.
 - 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 try to start the client.
 - 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.
- Q.** What are the system message log IDs supported for policy lookup for events generated by security appliances and routers?
- A.** 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
- 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`
- Q.** How many Security Manager servers can I add to a MARS Local Controller to perform policy lookup?
- A.** 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.
- Q.** My MARS Local Controller is administered by a Global Controller. Can I perform policy lookup for events generated on the Local Controller from the Global Controller interface?
- A.** No. 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.
- Q.** There are two places in which I need to enter the Security Manager username and password. What is the difference between the credentials in the Reporting Applications tab and the one in the User Management page of MARS?

- A.** 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.

Policy Lookup for Events Generated by Devices with Multiple Contexts

Problem Policy lookup fails when you click the Security Manager icon for an event generated by access rules or connection establishment/teardown on devices with multiple contexts.

Solution 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.

Problem Security Manager icon is not displayed in the Reporting Device column for events generated by devices in multiple context mode.

Solution 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. You can query events from such contexts only by running a query for “Unknown Reporting Devices” from MARS.

FAQs about MARS Events Lookup from a Security Manager Policy

This section answers the following questions about looking up MARS events from Security Manager policies:

- [Q.What are the versions of MARS and Security Manager that are supported for events lookup from policies?](#)
- [Q.Can I add multiple MARS appliances to a Security Manager server?](#)
- [Q.What are the benefits of querying for MARS events from policies?](#)
- [Q.Is there any limit to the number of keywords that are populated in the Query page of MARS when I perform events lookup from an access rule that supports hashcodes?](#)

- Q. Am I returned to the Query Criteria page or the Query Results page on successful lookup of events from a policy?
 - Q. Why does events lookup fail from policies generated by FWSM, PIX, and ASA devices in which multiple security contexts exist?
 - Q. Why do I get a “Policy not found” error message when I query for MARS events from the default signature policy?
 - Q. If my MARS session is active, the events query criteria or results are displayed in the existing MARS browser window, making me lose the data I was viewing in the MARS GUI. Is this behavior not changeable?
 - Q. Why do I get the Security Alert dialog box when I perform events lookup?
 - Q. Can I perform events lookup from a signature that is disabled for a sensor?
 - Q. Why do I receive a warning message when I try to look up events matching an access rule?
 - Q. Is it possible to view events for access rules for which logging is not enabled?
 - Q. Is there any difference in the types of syslogs that are displayed for events matching a flow and events matching a rule?
 - Q. What is the difference between the MARS user credentials entered in the New/Edit CS-MARS dialog box and in the login dialog box during events lookup?
 - Q. Is it possible to query for events generated by a signature configured on a virtual sensor?
 - Q. What are the different authentication mechanisms for events lookup?
 - Q. Why is the check box to save credentials for subsequent event lookups disabled in the Login to CS-MARS dialog box?
 - Q. Is it always necessary to configure the Security Manager user account in the MARS database to perform events lookup?
 - Q. Are the MARS login credentials that I enter in the Login to CS-MARS dialog box cached until the current Security Manager session is active?
 - Q. Can I test the connectivity between MARS and Security Manager before querying for events?
 - Q. How does the absence of hashcodes in ACEs on devices that do not support them affect the accuracy of event matches for a policy?
 - Q. Can I query events for more than one access rule or signature at the same time?
 - Q. Why do I see no events when I perform a lookup from an access rule for which object grouping or rule optimization is enabled?
 - Q. If a device is monitored by multiple MARS appliances, how can I choose the MARS appliance for which I want to view the events after lookup?
 - Q. Do I need to associate the MARS appliance with the device that it monitors before lookup, even if only one MARS monitors the device?
 - Q. Can I select the MARS appliance to associate it the device during lookup or does it need to be done before lookup?
 - Q. If I delete a MARS from Security Manager, is the association between the device and MARS automatically removed?
- Q.** What are the versions of MARS and Security Manager that are supported for events lookup from policies?

- A.** You need to use Security Manager 3.2 and MARS 4.3.4 or 5.3.4 to navigate to the events in MARS from the Security Manager policy table. You cannot add a MARS appliance running a version lower than 4.3.4 or 5.3.4 to Security Manager.
- Q.** Can I add multiple MARS appliances to a Security Manager server?
- A.** You can add multiple MARS Local Controllers to a Security Manager server, although you cannot add a MARS Global Controller to a Security Manager server.
- Q.** What are the benefits of querying for MARS events from policies?
- A.** Navigation from a Security Manager policy to a MARS event eliminates the need to run a detailed query in MARS by retrieving and populating the query criteria from the policy settings. If objects are referenced in policies, the complexity of the query criteria is increased because the components of the objects might need to be entered in the strings to be queried. However, when you select a Security Manager policy to navigate to the event generated in the MARS GUI by that policy, the contents of the objects are also expanded and prepopulated in the query fields.
- Q.** Is there any limit to the number of keywords that are populated in the Query page of MARS when I perform events lookup from an access rule that supports hashcodes?
- A.** Because Security Manager uses the hashcodes of the ACEs on devices that support them to uniquely query for syslogs generated by the ACE in MARS, large access rules might contain thousands of such hashcodes contained in them. These hashcodes are displayed as keywords in the query criteria. If the number of keywords or the sum of the number of sources, destinations, and protocols for an ACE or a signature exceeds the permissible limit of 150, an error message is displayed in the MARS GUI. The error message displays the possible cause and recommended action.
- Q.** Am I returned to the Query Criteria page or the Query Results page on successful lookup of events from a policy?
- A.** For realtime events, the query is automatically run when you lookup access rules or signatures and the results of the query are displayed in the realtime event viewer of MARS. However, for historical events, only the query criteria fields are populated from the data derived from Security Manager and the query must be submitted to view matching events. The time to be used to filter logged historical events is set to the last 10 minutes from the present time.
- Q.** Why does events lookup fail from policies generated by FWSM, PIX, and ASA devices in which multiple security contexts exist?
- A.** This problem occurs if you did not define a unique management IP address in Security Manager for each security context or if you did not configure the hostname and reporting IP address for each virtual context while adding it to MARS.
- Q.** Why do I get a “Policy not found” error message when I query for MARS events from the default signature policy?
- A.** If you add an IPS device to Security Manager and deselect the IPS check box in the Create Discovery dialog box to exclude IPS policies on the device from being discovered, the icon next to the IPS policy reverts to an empty icon to show that the policy was unassigned from the device’s configuration. For all IPS device and service policies, a default signature policy is assigned to the device when you remove the configured policies from the device. If you try to perform events lookup from the default signature, a “Policy not found” error message is displayed. However, if you edit the default signature and save it, the policy icon changes to show that a local policy is configured on the device and you can navigate to events in MARS.

- Q.** If my MARS session is active, the events query criteria or results are displayed in the existing MARS browser window, making me lose the data I was viewing in the MARS GUI. Is this behavior not changeable?
- A.** If an instance of MARS is already running, the existing browser window is reused to display the Query page of MARS because of the way in which you have set your browser to reuse windows. Set your browser to not reuse windows (such as deselecting the Reuse Windows for Launching Shortcuts check box from Tools > Internet Options > Advanced in your Internet Explorer) if you do not want the content in your current window to be replaced with whatever content is generated after events lookup.

Events lookup determines whether to reuse an existing window or open a new window based on your browser setting and does not use a predefined method. The actual setting you configure to allow reuse of browser instances varies depending on which browser you use. See your browser documentation or help system for more information on this configuration.

- Q.** Why do I get the Security Alert dialog box when I perform events lookup?
- A.** The first time you navigate to events in MARS, a Security Alert dialog box is displayed if the SSL certificate of MARS is not saved in the trusted folder of the browser. Click **Yes** to choose to trust the certificate for the current session.
- Q.** Can I perform events lookup from a signature that is disabled for a sensor?
- A.** Yes. If you right-click a signature that is disabled in the signature summary page and try to navigate to realtime or historical events in MARS, a warning message is displayed asking you to confirm whether you want to proceed with the events lookup. Click **Yes** to continue.
- Q.** Why do I receive a warning message when I try to look up events matching an access rule?
- A.** If the selected device does not support hashcodes in ACEs, a warning dialog box is displayed that query results might be inaccurate if the selected ACE conflicts or overlaps with other ACEs. Click **OK** to run the query.
- Q.** Is it possible to view events for access rules for which logging is not enabled?
- A.** If logging is not enabled for a permit ACE on ASA, PIX, and FWSM devices, or if logging is not enabled on IOS routers for ACEs, a warning message is displayed when you view events. To view syslogs associated with access rules for which logging is not enabled, you can perform a lookup for events matching a traffic flow.
- Q.** Is there any difference in the types of syslogs that are displayed for events matching a flow and events matching a rule?
- A.** When you perform a query for events matching a traffic flow, events triggered by access rules and connection setup/teardown are displayed. However, when you perform a query for events matching a rule, only events triggered by access rules and not connection setup/teardown are displayed.
- Q.** What is the difference between the MARS user credentials entered in the New/Edit CS-MARS dialog box and in the login dialog box during events lookup?
- A.** The MARS username and password values that you enter or modify in the New/Edit CS-MARS Device dialog box is used by Security Manager server to communicate with MARS and discover meta information, such as version of software running on the server and certificate details. These credentials are different from the username and password that you enter in the Login to CS-MARS *ip_address* dialog box.

The username and password pair in the Login to CS-MARS *ip_address* dialog box comprise the credentials that Security Manager uses to authenticate with MARS to look up events matching a policy rule, when you select the option to use MARS credentials during the addition of MARS to Security Manager. The MARS username and password values you enter in the events lookup login dialog box are saved in the Security Manager database until the client session times out, if you chose to allow saving of MARS login credentials during events lookup.

- Q.** Is it possible to query for events generated by a signature configured on a virtual sensor?
- A.** Yes. If a signature configured on your virtual sensor generates an event, the Keyword field displays the virtual sensor name in addition to the signature and subsignature IDs.
- Q.** What are the different authentication mechanisms for events lookup?
- A.** You can enable Security Manager to either contact MARS using the credentials that you entered while logging in to Security Manager or use MARS credentials for Security Manager to authenticate with MARS. If you select the option to be prompted for MARS credentials when the event query lookup is performed, you can also choose to save the MARS credentials in the login dialog box to avoid being prompted every time you look up MARS events in a new Security Manager client session or if the client session times out.
- Q.** Why is the check box to save credentials for subsequent event lookups disabled in the Login to CS-MARS dialog box?
- A.** This check box is available only if the Allow users to save passwords check box is selected in the CS-MARS page. When it is selected, MARS credentials are saved in the Security Manager database and reused during events lookup. The Login to CS-MARS *ip_address* dialog box is not displayed during subsequent events lookup operations if you select this check box.
- Q.** Is it always necessary to configure the Security Manager user account in the MARS database to perform events lookup?
- A.** You need to create the Security Manager user account in the MARS database only if you select the option to use Security Manager credentials for events lookup.
- Q.** Are the MARS login credentials that I enter in the Login to CS-MARS dialog box cached until the current Security Manager session is active?
- A.** Yes. If you selected the option to use the MARS login credentials for Security Manager to authenticate with MARS and did not choose to allow the login credentials to be saved in the login dialog box, these credentials are cached until you exit Security Manager or the idle session timeout period is exceeded; you are not prompted for login details until the Security Manager session is active.
- Q.** Can I test the connectivity between MARS and Security Manager before querying for events?
- A.** Yes. You can test the connectivity from Security Manager to MARS in one of the following ways:
- From the New/Edit CS-MARS dialog box, click **Retrieve from Device** next to the field to have Security Manager retrieve the certificate from MARS. When you click this button, the Retrieving certificate from *ip_address* dialog box appears for a short period to indicate the process of Security Manager contacting MARS.
 - From the General page in Device Properties, click **Discover CS-MARS** next to the Monitored By field. The Finding CS-MARS Device for *device_IP_address* dialog box appears for a brief period when Security Manager attempts to establish communication with MARS.

If the initial configuration to enable the MARS Appliance communicate with other devices on the network and prepare it to monitor data from reporting devices is not completed, an error message is displayed during connectivity test.

If the MARS appliance has been shut down or cannot be reached from the Security Manager server when you try to view events, an error message is displayed asking you to restore the connection between MARS and Security Manager.

- Q.** How does the absence of hashcodes in ACEs on devices that do not support them affect the accuracy of event matches for a policy?
- A.** When you select the option to display events matching a rule, the support of ACE hashcodes by the version of software running on a device determines the accuracy of syslog matches. Although Security Manager is able to gather the device information, the appropriate event types in MARS, 5-tuple data from the ACEs, and the ACL, these details can result in inaccurate or excessive syslog matches. To produce most accurate syslog matches for an ACE, PIX and ASA 7.0 and later support ACE hashcodes. Each ACE contains an MD5 hashcode, which is included in the syslogs generated by that ACE. For PIX and ASA devices running 7.0 or later, Security Manager includes the hashcodes of the ACEs generated by the selected rule in the query sent to MARS. ACE hashcodes are not supported on security appliances running a version of PIX or ASA software earlier than 7.0.
- Q.** Can I query events for more than one access rule or signature at the same time?
- A.** You can select only one row at a time from the Access Rules page to look up events that are generated by them. However, you can select one or more signature IDs at a time from the Signatures page and navigate to the Query page of MARS for running a query on historical and realtime events.
- Q.** Why do I see no events when I perform a lookup from an access rule for which object grouping or rule optimization is enabled?
- A.** If object grouping or rule optimization is enabled for an access rule defined in Security Manager and the associated access-list commands on the device do not match with the optimized rules, no events are displayed in MARS because of the mismatch in access rule relationship between Security Manager and the device.
- Q.** If a device is monitored by multiple MARS appliances, how can I choose the MARS appliance for which I want to view the events after lookup?
- A.** If more than one MARS monitors a device added to Security Manager, the Select CS-MARS dialog box appears, prompting you to select the MARS device that you want to associate with the device or use to view events for the selected policy rule. This dialog box appears when you try to discover the MARS device for a device from the Device Properties page or when you lookup events for a device monitored by multiple MARS devices, whichever operation is performed first. Once a MARS device is resolved to a device, you are not prompted to select from a list of available choices.
- Q.** Do I need to associate the MARS appliance with the device that it monitors before lookup, even if only one MARS monitors the device?
- A.** If only one MARS appliance monitors a device and you do not associate the MARS appliance with the device that it monitors from the Device Properties page by discovering the MARS appliance, the MARS appliance is automatically resolved to the device when you perform the events lookup for the first time.
- Q.** Can I select the MARS appliance to associate it the device during lookup or does it need to be done before lookup?

A. You can associate the MARS device with the device in inventory either before you perform events lookup or at the time of the lookup query. If you try to navigate to MARS events from the policy table of a device before associating the MARS device with it, Security Manager automatically resolves the device to the correct MARS device if only one MARS device monitors it or presents you with a list of MARS devices monitoring the device if multiple MARS devices monitor the same device. You can establish the association and continue with the lookup of events. Once you associate the MARS device with the device, the MARS hostname or IP address is populated in the Monitored By field of the Device Properties page.

Alternatively, you can discover a MARS device monitoring a device already added to Security Manager from the General pane of the Device Properties page to reduce a task in the process of looking up events.

Q. If I delete a MARS from Security Manager, is the association between the device and MARS automatically removed?

A. If you delete a MARS appliance monitoring a device from the Security Manager database, it is also removed from the Monitored By field in the Device Properties page of that device. If a device is monitored by two MARS appliances and you later delete one of them from the Security Manager database, the device is automatically associated with the remaining MARS device. You do not have to manually discover the MARS appliance for that device.

Changing the Association of the MARS Appliance with a Device

Problem A device is monitored by multiple MARS appliances that are added to Security Manager. You associated the device with a MARS appliance during events lookup. You want to select a different MARS appliance for the device and perform events lookup.

Solution Once you associate a MARS appliance with a device during events lookup, the same MARS device is used to query for events even if multiple MARS devices monitor a device. To change the MARS device to be used to look up events, you must rediscover the MARS device from the General pane of the Device Properties page.

This procedure describes how to discover a MARS device monitoring a device added to the inventory.

Before You Begin

Make sure that you added the necessary MARS appliances to Security Manager.

Procedure

-
- Step 1** Click the Device View button on the toolbar. The Devices page appears.
- Step 2** Double-click a device in the Device selector. The Device Properties page appears.
- Step 3** Click **General** from the left pane. The General page appears.
- Step 4** Under CS-MARS Monitoring, click **Discover CS-MARS** next to the Monitored By field. The Finding CS-MARS Device for *device_IP_address* dialog box appears for a brief period when Security Manager attempts to establish communication with MARS. If connectivity and discovery are successful, the Select CS-MARS dialog box is displayed.
- Step 5** Click the radio button next to the MARS appliance to be used to query events for the policy rule on the selected device.

- Step 6** Click **OK**. The selected MARS hostname or IP address is populated in the Monitored By field of the Device Properties page.



Note You do not need to click **Submit** in the General page to save your changes; the settings are automatically saved to the database.

Configuring Required Browser Settings for Policy and Events Lookup

You might have to change browser settings on the system from which you access the MARS GUI for policy and events lookup. Default browser settings might cause a number of popup warning or error messages to be displayed when you perform policy or events lookup. In some cases, navigation to the Security Manager client for policy lookup or to the MARS GUI for events lookup might be blocked due to browser settings. The topics in this section are our recommendations for managing browser settings that can affect policy and events lookup. Refer to your browser manual or online help for detailed instructions about accessing and setting the options in these procedures.

- [Working with Cached Passwords in Internet Explorer, page 13-19](#)
- [Setting Internet Explorer Security Options, page 13-20](#)
- [Setting Internet Explorer to Allow Display of Nonsecure Content, page 13-20](#)

Working with Cached Passwords in Internet Explorer

If you selected the option to be prompted for Security Manager credentials during policy lookup, it is possible that the Password field in the login section of the policy query popup window is automatically filled after you enter the username. You might notice this behavior due to a configuration in Internet Explorer, whereby passwords are cached or are remembered by the browser.

Internet Explorer can store user passwords, thereby saving you a few steps when logging in to Web applications. If you enabled the AutoComplete feature, when you visit a web page for the first time, Internet Explorer prompts you with a message whether you want to remember the password you entered. If you click Yes, the password is automatically filled on subsequent visits to this page. If you click No when asked whether you want passwords to be remembered and if the AutoComplete feature is enabled, a list of possible matches appears as you type if you have entered a similar entry before. If a suggestion in the list matches what you want to enter in that field, the browser automatically fills the entry. However, for security reasons, we recommend that you prevent the browser from remembering passwords when you log in, especially if you share your computer with others. You can either disable the feature of the browser to cache passwords or clear the cache at intervals to be not prompted with suggestions during entry.

To disable the AutoComplete feature altogether, follow these steps:

- Step 1** Select **Tools > Internet Options**.
- The Internet Options dialog box appears.
- Step 2** Click the **Advanced** tab.

- Step 3** In the Browsing pane, deselect the **Use inline auto complete** check box.
- Step 4** Click **OK** in the Internet Options dialog box.

To clear cached passwords from your browser, follow these steps:

- Step 1** Select **Tools > Internet Options**.
- The Internet Options dialog box appears.
- Step 2** Click the **Content** tab.
- Step 3** Under Personal Information, click the **AutoComplete** button.
- The AutoComplete Settings dialog box appears.
- Step 4** Click **Clear Passwords**. When you are prompted to confirm your action, click **OK**.
- Step 5** Click **OK** as many times as necessary to close the opened dialog boxes.

Setting Internet Explorer Security Options

When you try to start the Security Manager client from the read-only policy query window in MARS, the File Download dialog box might appear prompting you to confirm whether you want to save the CsmContentProvider file to your system. The option to open the file without downloading it to your local disk is not available because of security settings in Internet Explorer. To enable the Open button to be displayed in this dialog box when it appears during policy lookup, do the following:

- Step 1** Select **Tools > Internet Options**.
- Step 2** Click the **Advanced** tab.
- Step 3** Scroll to the Security area, then deselect the **Do not save encrypted Pages to Disk** check box.
- Step 4** Click **OK**.

Setting Internet Explorer to Allow Display of Nonsecure Content

When you try to open the Security Manager client from the read-only signature or access rule policy query page in the MARS GUI, the Security Information Error dialog box might be displayed if you configured your browser to prompt for confirmation whenever a web page that contains both secure and nonsecure content must be opened. You may receive the following Security Information message when you open the Security Manager client:

```
This page contains both secure and nonsecure items.
Do you want to display the nonsecure items?
```

You can configure your browser to seamlessly display nonsecure content without being prompted each time the Security Manager client is opened. To configure Internet Explorer to allow display of nonsecure content, follow these steps:

-
- Step 1** Select **Tools > Internet Options**.
- Step 2** Click the **Security** tab.
- Step 3** Click **Custom Level** on the Security tab of the Internet Options dialog box.
- Step 4** Under the Miscellaneous heading, select the **Enable** radio button for the “Display mixed content” setting. This option specifies whether Web pages can display content from both secure and non-secure servers.
- By default, the “Display mixed content” setting is set to Prompt for all security levels. If the “Display mixed content” setting is set to Enable, the message box is not displayed and nonsecure content can be displayed. If the “Display mixed content” setting is set to Disable, the message box is not displayed and nonsecure content is not downloaded for display.
- Step 5** Click **OK**.
-

