



Configuring Inbound Email

ScienceLogic version 8.9.0

Table of Contents

Introduction to Inbound Email	1
Overview	1
Infrastructure Requirements	1
General Inbound Email Settings	2
Overview	2
Configuring System Email Settings	2
System Settings that Affect Inbound Email	4
Events from Email	6
Overview	6
System Settings that Affect Events from Email	7
Viewing the List of Event From Email Policies	8
Filtering the List of Event From Email Policies	10
Configuring an Event from Email Policy	11
Creating an Event Policy of Type "Email"	13
Formatting Inbound Email	16
How the ScienceLogic Platform Processes Events from Email Policies	17
Tickets from Email	18
Overview	18
Viewing the List of Ticket From Email Policies	19
Filtering the List of Ticket From Email Policies	19
Creating a Ticket From Email Policy	21
Sending an Email to Create a Ticket	23
Using Email to Add a Note to a Ticket	23
Email Round-Trip Monitoring Policies	24
Overview	24
Viewing the Email Round-Trip Monitoring Policies	24
Filtering the List of Email Round-Trip Monitoring Policies	25
Creating an Email Round-Trip Monitoring Policy	26
Configuring the Monitored Device	28

Introduction to Inbound Email

Overview

This manual is intended for system administrators responsible for configuring SL1. SL1 can receive email messages from external sources and process those messages to trigger events, create tickets, and monitor the speed of email servers. This manual describes how to configure SL1 to process inbound email. You must configure the general inbound email settings before configuring events from email, tickets from email, or email round-trip monitoring policies.

Infrastructure Requirements

To use the inbound email functions of SL1, you must configure your IT infrastructure so that at least one DNS MX record maps to the IP address of the Database Server or All-In-One Appliance. If a DNS MX record does not exist for the IP address of your Database Server or All-In-One Appliance, no email will be delivered to SL1. If you are not responsible for DNS records, ask your system administrator for help with this step.

Typically, the DNS MX record that maps to the IP address of the system will be a sub-domain of your primary domain. If you want email to be sent from outside your corporate network to your SL1 system, you might need to configure an externally accessible email address that forwards to the appropriate email address for the SL1 system. The general steps to do this in your email system are:

1. Configure a new mailbox for an address that uses your primary domain. For example, "support@company.com".
2. Create a mail contact for the address used by your SL1 system. For example, "ticket@monitoring.company.com".
3. Configure the mailbox you created in step 1 to automatically forward all mail to the contact you created in step 2.

General Inbound Email Settings

Overview

This chapter describes the global settings in SL1 that allow SL1 to receive inbound email messages. You must configure SL1 as described in this chapter before defining policies for events from email, tickets from email, or email round-trip policies.

Configuring System Email Settings

Perform the following steps to configure the system settings for email:

1. Go to the **Email Settings** page (System > Settings > Email):

The screenshot shows the 'Email Settings' configuration page. The page has a blue header with 'Email Settings' on the left and 'Refresh' and 'Guide' buttons on the right. Below the header, there are several input fields for configuration:

- Authorized Email Domains: your-domain-goes-here.com
- System From Email Address: root@your-domain-goes-here.com
- Email Formal Name: EM7 Event Notifier
- Email Gateway: 192.168.0.1
- Email Gateway Alt: 192.168.0.2
- Escalation Notify Subject: TICKET ESCALATED: #%d | %M | %T | %F

A 'Save' button is located at the bottom center of the form area.

2. To define settings for inbound email, provide the following values in the following fields:
 - **Authorized Email Domains.** Enter the fully qualified name of the Database Server or All-In-One Appliance. This name must match the previously configured DNS MX record that maps to the IP address of the Database Server or All-In-One Appliance. If there are multiple DNS MX records for the Database Server or All-In-One Appliance, you can enter multiple domains in this field by separating entries with a comma.
3. The other fields on this page pertain to outbound email and are not required to configure inbound email. However, if you want to configure outbound email now, enter the following information:
 - **System From Email Address.** Enter the default email address that SL1 should use to send outbound emails.
 - **Email Formal Name.** Enter the name that will appear in the **from** field in email messages sent from SL1.
 - **Email Gateway.** Enter the IP address or fully qualified name of the SMTP relay server used by SL1. To use the email server built in to SL1, enter the IP address or fully qualified name of the Database Server or All-In-One Appliance.
 - **Email Gateway Alt.** Enter the IP address or fully qualified name of the SMTP relay server SL1 should use if the primary email gateway is unavailable.
 - **Escalation Notify Subject.** Enter the subject line that SL1 will use when sending ticket escalation notification emails.
4. Click the **[Save]** button. If the settings were saved successfully, the message "Email Settings Saved" is displayed at the top of the page.

System Settings that Affect Inbound Email

To define global settings that affect all inbound email, perform the following steps:

1. Go to the **Behavior Settings** page (System > Settings > Behavior):

The screenshot shows the 'Behavior Settings' configuration page. The 'Strip FQDN From Inbound Email Device Name' dropdown menu is highlighted with a red box and is currently set to 'Enabled'. Other visible settings include 'Single Instance Login (Admins)' set to 'Disabled', 'Account Lockout Duration' set to '1 hour', and 'SNMP Poll Timeout (Msec)' set to '1000'. The right column contains various system settings such as 'Port Scan Alerts' (Enabled), 'Port Scan Timeout' (120000 Msec), and 'DNS Hostnames' (Strip Domain Name (Hostname)).

2. To define settings for inbound email, provide the following values in the following field:

- **Strip FQDN From Inbound Email Device Name.** In Events from Email policies, specifies how SL1 will match the regular expression for device name. Choices are:
 - *Enabled.* SL1 will search the text string in the incoming email and match all characters up to the first period that appears in the text string. If multiple devices in SL1 match the characters up to the first period (for example, `my_device.1` and `my_device.2`), SL1 will align the event with the matching device with the highest Device ID.
 - *Disabled.* SL1 will search the text string in the incoming email for a match for the device name. The text string must include an exact match to the regular expression (defined in the Events from Email policy), including any text following a period in the device name. If SL1 does not find an exact match in the incoming email, SL1 creates an entry in the system log.

- **Inbound Email Alert Message.** In each event policy, the **First Match String** and **Second Match String** fields specify the string or regular expression used to correlate the event with a log message. To trigger an event, the text of a log message must match the value in the **First Match String** and **Second Match String** fields in that event's policy. For Events from Email policies, this field specifies whether only the email message body will be written to the device log or whether both the email message subject and email message body will be written to the device log. Choices are:
 - *Email Message Body Only.* Only the email message body is written to the device log. The **First Match String** and **Second Match String** fields can examine and match only the email message body.
 - *Email Message Subject and Body.* Both the email message body and the email message subject are written to the device log. The **First Match String** and **Second Match String** fields can examine and match against both the email message body.

NOTE: The global setting **Inbound Email Alert Message** affects how events are triggered. This field does not affect the **Regex Pattern** field in the Event from Email policy. The **Regex Pattern** field in an Event from Email policy specifies the device log to which the alert should be written.

3. Click the **[Save]** button.

Chapter

3

Events from Email

3

Overview

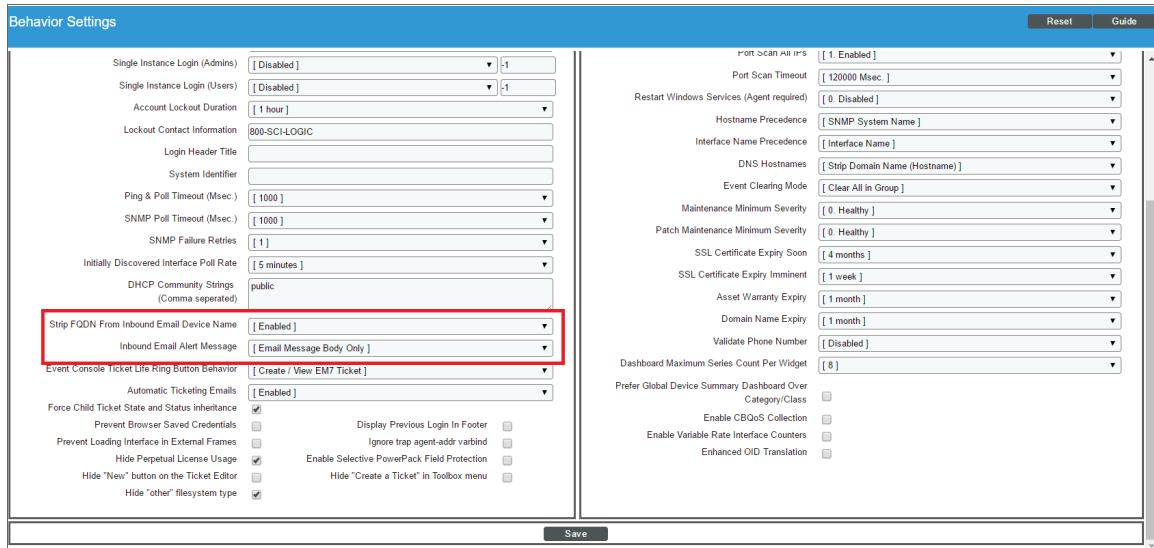
SL1 can generate events based on emails that the system receives from external devices. Before configuring SL1 to generate events from email, you must follow the steps listed in the [General Inbound Email Settings](#) chapter.

This chapter describes how to perform the following configuration tasks that are required before SL1 can generate events from email:

- [An email originator](#). An email originator is a policy that defines how an inbound email should be processed to generate a log message for a device in the system.
- [An email event policy](#). An email event policy defines how log messages generated from emails should generate events.
- [Correctly formatted inbound emails](#).

System Settings that Affect Events from Email

The **Behavior Settings** page (System > Settings > Behavior) allows you to define global parameters. The following parameter affects Event from Email policies:



- **Strip FQDN From Inbound Email Device Name.** This field in the **Behavior Settings** page specifies how SL1 will match the regular expression for the device name in an Event from Email policy. Choices are:
 - *Enabled.* SL1 will search the text string in the incoming email and match all characters up to the first period that appears in the text string. If multiple devices in SL1 match the characters up to the first period (for example, *my_device.1* and *my_device.2*), SL1 will align the event with the matching device with the highest Device ID.
 - *Disabled.* SL1 will search the text string in the incoming email for a match for the device name. The text string must include an exact match to the regular expression (defined in the Events from Email policy), including any text following a period in the device name. If SL1 does not find an exact match in the incoming email, SL1 creates an entry in the system log.
- **Inbound Email Alert Message.** In each event policy, the **First Match String** and **Second Match String** fields specify the string or regular expression used to correlate the event with a log message. To trigger an event, the text of a log message must match the value in the **First Match String** and **Second Match String** fields in that event's policy. For Events from Email policies, this field specifies whether only the email message body will be written to the device log or whether both the email message subject and email message body will be written to the device log. Choices are:
 - *Email Message Body Only.* Only the email message body is written to the device log. The **First Match String** and **Second Match String** fields can examine and match only the email message body.

- *Email Message Subject and Body*. Both the email message body and the email message subject are written to the device log. The **First Match String** and **Second Match String** fields can examine and match against both the email message body.

NOTE: The global setting **Inbound Email Alert Message** affects how events are triggered. This field does not affect the **Regex Pattern** field in the Event from Email policy. The **Regex Pattern** field in an Event from Email policy specifies the device log to which the alert should be written.

Viewing the List of Event From Email Policies

TIP: To sort the list of policies, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again. The **Edit Date** column sorts by descending order on the first click; to sort by ascending order, click the column heading again.

The **Mailer Redirection** page (Registry > Events > Inbound Email) displays the following information about each Event from Email policy:

Originator Address	Alignment Type	Regex Type	Regex Pattern	Default Element	ID	Edit User	Edit Date
em7@ghr.decs.com	Override Device Search	--	--	ACME - Printer [HP] 1		mjohnson	2015-04-17 04:00:33
ggibson@sciencelogic.com	Align Unmatched	Subject	*critical file system	StarHubEMS Microsc 2		ggibson	2013-09-24 01:09:51

- **Originator Address**. Fully-qualified email address from which SL1 will accept event messages. If an incoming email message comes from the same email address as specified in this field, SL1 will process that email message as an event. The originator address is usually the address of another monitoring system that is escalating events through SL1. When used in this way, SL1 becomes a "manager of managers."

- **Alignment Type.** Specifies how SL1 should handle inbound email messages that do not include a match with the **Regex Pattern**. The **Regex Pattern** tells SL1 which element to align with the resulting event. Choices are:
 - *If device not found, discard unmatched email.* If the inbound email does not include text that matches the **Regex Pattern**, discard the email. No event will be created from this instance of the inbound email.
 - *If device not found, align unmatched email with default element.* If the inbound email does not include text that matches the **Regex Pattern**, align the email with the element specified in the **Default Element** field. The resulting event will be aligned with the **Default Element**.
 - *Override device search, align email with default element.* Do not try to match the email with the **Regex Pattern**. Instead, automatically align the email with the element specified in the **Default Element** field. The resulting event will be aligned with the **Default Element**.
- **Regex Type.** Part of the email message where the **Regex Pattern** will appear. Choices are:
 - Subject
 - Body
- **Regex Pattern.** A specific string that appears directly before the name or IP address of the device to associate with the event message. SL1 will then find the device name or IP address in the email message and associate the message with the appropriate device. If the **Regex Type** is *Body*, and the email body is in HTML format, SL1 will strip out the HTML constructs before searching for the regex pattern.

NOTE: This string does not trigger the event; this string only informs SL1 which device to associate with the event message. SL1 will search all event definitions with a source of **Email** and then compare the entire email message to the **Match String** field in each event definition.

- **Default Element.** If in the **Alignment Type** field, one of the following options is selected:
 - *If device not found, align unmatched email with default element.*
 - *Override device search, align email with default element.*

then the **Default Element** field specifies the default element to use. The default element can be an Organization, Device, Asset, Interface, Vendor, User Account, or Virtual interface.

NOTE: If the **Default Element** is not associated with the current user's organization, this field will display the value *Restricted*.

- **ID.** Unique, numeric ID associated with the Event from Email policy. SL1 automatically assigns this ID to the policy.
- **Edit User.** The user who created or last edited the Event from Email policy.
- **Edit Date.** Date the Event from Email policy was created or last edited.

Filtering the List of Event From Email Policies

The **Mailer Redirection** page includes six filters, in the top row in the list of policies. You can specify one or more parameters to filter the display of Event from Email policies. Only Event from Email policies that meet all the filter criteria will be displayed in the **Mailer Redirection** page.

You can filter by one or more of the following parameters. The list of Event from Email policies is dynamically updated as you select each filter.

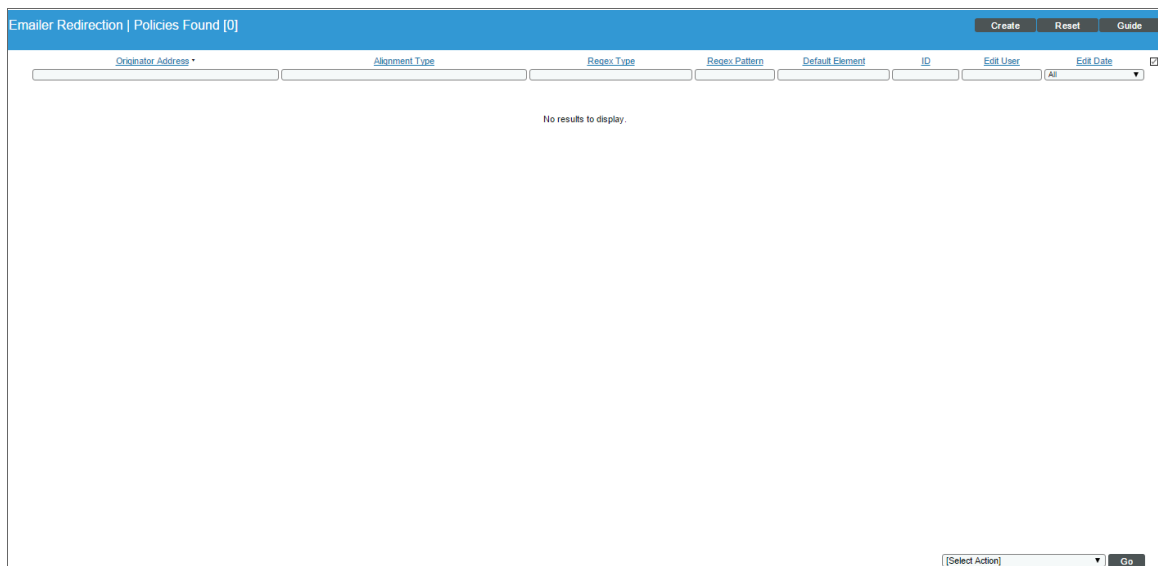
- For each filter except **Edit Date**, you must enter text to match against. SL1 will search for Event from Email policies that match the text, including partial matches. Text matches are not case-sensitive. You can use the following special characters in each filter:
 - , (comma). Specifies an "or" operation. For example:
"dell, micro" would match all values that contain the string "dell" OR the string "micro".
 - & (ampersand). Specifies an "and" operation. For example:
"dell & micro" would match all values that contain the string "dell" AND the string "micro".
 - ! (exclamation mark). Specifies a "not" operation. For example:
"!dell" would match all values that do not contain the string "dell".
- **Originator Address**. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Mailer Redirection** page will display only Event from Email policies that have a matching originator email address.
- **Alignment Type**. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Mailer Redirection** page will display only Event from Email policies that have a matching alignment type.
- **Regex Type**. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Mailer Redirection** page will display only Event from Email policies that are associated with a matching regex type (either Body or Subject).
- **Regex Pattern**. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Mailer Redirection** page will display only Event from Email policies that include a matching regex pattern.
- **Default Element**. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Mailer Redirection** page will display only Event from Email policies that include a matching default element.
- **ID**. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Mailer Redirection** page will display only Event from Email policies that include a matching ID.
- **Edit User**. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Mailer Redirection** page will display only Event from Email policies that have a matching "created by" or "edited by" value.

- **Edit Date.** You can select from a list of time periods. The **Emailer Redirection** page will display only Event from Email policies that have been created or edited within that time period. Choices are:
 - *All.* Display all policies that match the other filters.
 - *Last Minute.* Display only policies that have been created within the last minute.
 - *Last Hour.* Display only policies that have been created within the last hour.
 - *Last Day.* Display only policies that have been created within the last day.
 - *Last Week.* Display only policies that have been created within the last week.
 - *Last Month.* Display only policies that have been created within the last month.
 - *Last Year.* Display only policies that have been created within the last year.

Configuring an Event from Email Policy

SL1 uses each Event from Email policy to determine whether an incoming email comes from a source that is authorized to trigger events. Perform the following steps to configure an email originator:

1. Go to the **Emailer Redirection** page (Registry > Events > Inbound Email):



2. In the **Emailer Redirection** page, click the **[Create]** button. The **Add Policy** modal page appears.

The screenshot shows a web browser window with the address bar displaying "10.64.171.130/em7/index.em7?exec=admin_events_from_email_editor&height=665&width=615&ra...". The main content area is a modal titled "Add Policy | Create New" with a "Reset" button in the top right. The form contains the following fields:

- Originator Address:** A text input field.
- Alignment Type:** A dropdown menu with the selected option "[If device not found, discard unmatched email]".
- Regex Pattern:** A text input field.
- Regex Pattern Type:** A dropdown menu with the selected option "[Classic]".
- Regex Type:** A dropdown menu with the selected option "[Subject]".


A "Save" button is located at the bottom center of the modal.

3. To define the Event from Email policy, supply values in the following fields:

- **Originator Address.** Enter the fully-qualified email address from which SL1 will accept event messages. If an incoming email message comes from the same email address as specified in this field, SL1 will process that email message as an event. The originator address is usually the address of another monitoring system that is escalating events through SL1. When used in this way, SL1 becomes a "manager of managers."
- **Alignment Type.** Specifies how SL1 should handle inbound email messages that do not include a match with the **Regex Pattern**. The **Regex Pattern** tells SL1 which element to align with the resulting event. Choices are:
 - *If device not found, discard unmatched email.* If the inbound email does not include text that matches the **Regex Pattern**, discard the email. No event will be created from this instance of the inbound email.
 - *If device not found, align unmatched email with default element.* If the inbound email does not include text that matches the **Regex Pattern**, align the email with the element specified in the **Default Element** field. The resulting event will be aligned with the **Default Element**.
 - *Override device search, align email with default element.* Do not try to match the email with the **Regex Pattern**. Instead, automatically align the email with the element specified in the **Default Element** field. The resulting event will be aligned with the **Default Element**.

- **Regex Pattern.** Enter a specific string that appears directly before the name or IP address of the device to associate with the event message. SL1 will then find the device name or IP address in the email message and associate the message with the appropriate device. See the [Formatting Inbound Emails](#) section in this chapter for more information.
- **Regex Pattern Type** Specify if you want advanced control over the regex behavior. Choices are:
 - *Classic.* Select this option if you want the SL1 to use simple text matching to search for the **Regex Pattern**.
 - *Advanced.* Select this option if you want the SL1 to search for the **Regex Pattern** using advanced regex. Advanced regex patterns can be up to 255 character in length and support all of the special characters supported by Python regex.

NOTE: The **Regex Pattern** string does not trigger the event; this string only informs SL1 which device to associate with the event message. To trigger an event, SL1 will search all event definitions with a source of **Email** and then compare the entire email message to the **Match String** field in each event definition.

- **Regex Type.** Select either *Body* or *Subject* from the drop-down list. This is the part of the email message where the **Regex Pattern** will appear.
- **Default Element.** If you selected *If device not found, align unmatched email with default element* or *Override device search, align email with default element* in the **Alignment Type** field, then the **Default Element** field specifies the default element to use. Clicking on the binoculars icon () opens the **Element Alignment** modal page, where you can search for and select a default element. The default element can be an Organization, Device, Asset, Interface, Vendor, User Account, or Virtual Interface.

NOTE: If the **Default Element** is not associated with the current user's organization, this field will display the value *Restricted*.

4. Click the **[Save]** button.
5. An email originator must be created for each address/regex combination that you will use to create events from email.

Creating an Event Policy of Type "Email"

When SL1 receives an inbound email message that is authorized to trigger events and successfully matches the email to a device, SL1 compares the email message against all event policies with a source of **Email**. If the email message does not match one or more event policies, SL1 will not generate an event but will add the email message to the device logs of the matched device.

This section will describe how to create an event policy of type "email" and how to define matching criteria based on the contents of the email. For information on additional event options, such as occurrence count/time, detection weight, identifier patterns/formatting, auto-clearing, and expiry delays, see the **Events** manual.

To create an event policy of type "email", perform the following steps:

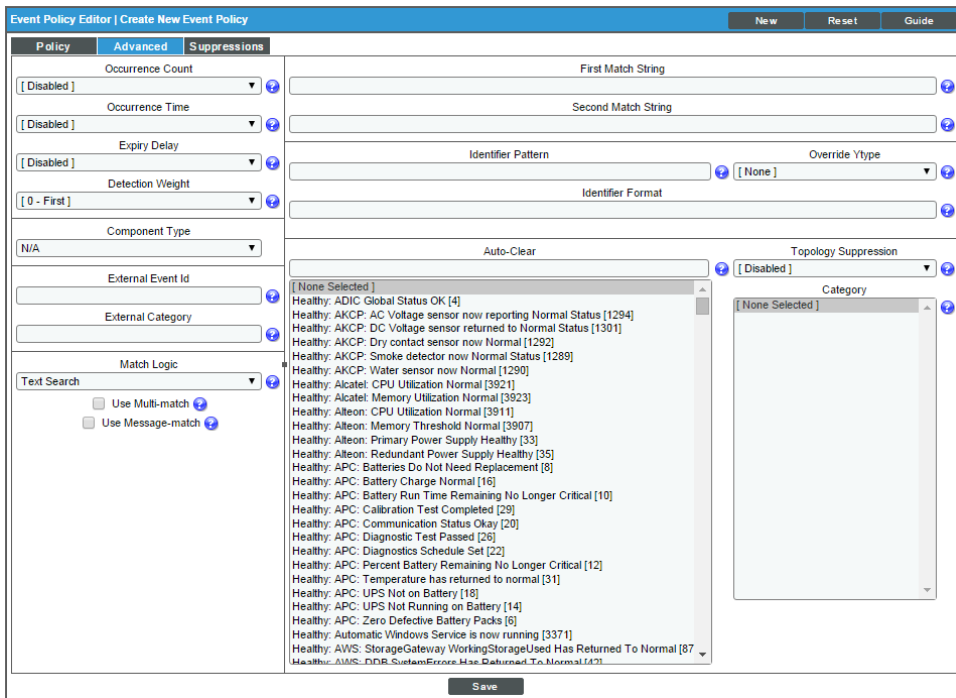
1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager):

Event Policy Name	Type	State	P-Pack	Severity	Weight	ID	Expiry	Time	Thresh	Edited By	Last Edited	External ID	Category
1. Test Trap Redirection	Trap	Enabled	No	Major	0	3949	0 Min.	0 Min.	0	em7admin	2015-12-01 16:08:48	--	--
2. ADIC Global Status Failed	Dynamic	Enabled	Yes	Major	0	2	90 Min.	0 Min.	0	em7admin	2015-05-14 11:24:53	--	--
3. ADIC Global Status OK	Dynamic	Enabled	Yes	Healthy	0	4	15 Min.	0 Min.	0	em7admin	2015-05-14 11:24:53	--	--
4. ADIC Global Status Unknown	Dynamic	Enabled	Yes	Notice	0	3	30 Min.	0 Min.	0	em7admin	2015-05-14 11:24:53	--	--
5. ADIC Tape Library Degraded	Dynamic	Enabled	Yes	Minor	0	1	60 Min.	0 Min.	0	em7admin	2015-05-14 11:24:53	--	--

3

2. Click the **[Create]** button. The **Event Policy Editor** page appears:

3. To define an event policy based on an incoming email message, supply values in the following fields:
 - **Event Source.** Select *Email* from the drop-down list.
 - **Policy Name.** Enter a name for the policy.
 - **Event Message.** Enter the message associated with this event. To use the body of the email as the event message, leave the default value of "%M" in this field. For more information on Event Message formatting, see the **Events** manual.
 - **Event Severity.** Select a severity for this event from the drop-down list.
 - **Policy Description.** Enter a description of the event. This field is optional.
4. Click the **[Save]** button.
5. The event policy will now match every valid email message received from authorized external devices. To configure the event policy to match only against emails containing specific text, perform the following steps.
6. Click the **[Advanced]** tab:



7. Provide values in each of the following fields:

- **Match Logic.** Select either *Text Search* or *Regex Match* from the drop-down list. If you select *Text Search*, the SL1 system will use simple text matching to compare strings. If you select *Regex Match*, the SL1 system will use regular expressions to compare strings.
- **First Match String.** Enter the text string or regular expression that SL1 will compare to the text in the email subject or body.
- **Second Match String.** Optionally, enter a second text string or regular expression. If you enter a value in this field, the email must match both the contents of the **First Match String** field and the **Second Match String** field for the event to trigger.

NOTE: Match Strings are compared to the subject and body of received emails.

8. Click the **[Save]** button.

Formatting Inbound Email

For SL1 to process events from inbound emails, you must configure your external devices to send email using certain formatting rules. Inbound emails must meet the following requirements to be processed as events by SL1:

- The email must be sent to the following address:
`notify@domain-name-of-ScienceLogic-platform`

Where "domain-name-of-ScienceLogic-platform" is one of the fully qualified domain names of the Database Server or All-In-One Appliance, i.e., one of the domain names you entered in the **Authorized Email Domains** field in the **Email Settings** page.
- The "from" address used by the external device must match an address defined in the **Originator Address** field in an email originator policy.
- The email message must contain a string that matches the regular expression defined in the **Regex Pattern** field in the email originator policy. If the email originator has the **Regex Type** set to *Body*, the string must be included in the email body. If the email originator has the **Regex Type** set to *Subject*, the string must be included in the email subject.
- The **Regex Pattern** string must be followed by the IP address, hostname, or device ID of a device monitored by the SL1 system. If an event is created, it will be associated with the specified device. For example, if the email originator has the **Regex Pattern** field set as "Event," the **Regex Type** set to *Subject*, and a device with an IP address of 192.168.1.1 is monitored in the system, a valid email subject would be:

Event 192.168.1.1

NOTE: There must be a space between the regex pattern and the IP address, hostname, or device ID.

- If you are using the "%M" substitution in your email event policies, ensure the message you wish to substitute is contained within the body of the email.
- If you are using Match Strings in your email event policies, ensure that matching text is contained within the body of the email.

NOTE: You can specify how an Event from Email policy will match a regular expression to a device name in the **Behavior Settings** page (System > Settings > Behavior).

How the ScienceLogic Platform Processes Events from Email Policies

When SL1 receives an email from an Events from Email policy, SL1 examines all the Events from Email policies and executes the first policy that matches the incoming email.

SL1 will log debug messages for each policy that did not match the incoming email message. After SL1 finds the first matching policy, SL1 does not examine any other policies and does not generate any more debug messages.

If SL1 does not find any Events from Email policies that match the incoming email, SL1 generates the error message "E701 Could not match device to email...".

Chapter

4

Tickets from Email

Overview

SL1 can create tickets based upon email messages sent to SL1. Before configuring SL1 to create tickets from email, you must follow the steps listed in the [General Inbound Email Settings](#) chapter.

This chapter will describe how to configure a Tickets From Email policy, which allows SL1 to generate tickets from email, and how to send an email message to trigger an automatic ticket.

Viewing the List of Ticket From Email Policies

TIP: To sort the list of policies, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again.

The **Tickets From Emails** page (Registry > Ticketing > Email Tickets) displays the following about each Ticket from Email policy:

	Policy Name	Destination Email	Template	Template ID	Edit User	Edit Date
1	Availability_Tickets_to_MoM	hrd@em73.sciencelogic.com	Device Failed Availability Check	7	kgibson	2015-04-17 03:43:54
2	NoResponse_Ticket_to_MoM	jack@em73.sciencelogic.com	No Response When Monitoring %X (%a)	1	kgibson	2015-04-17 03:44:49

- **Policy Name.** Name of the Ticket from Email policy.
- **Destination Email.** Fully qualified email address associated with the policy. SL1 will process all email messages received in this mailbox as tickets.
- **Template.** Name of the ticket template the SL1 will use to create the ticket.
- **Template ID.** Numeric ID for the ticket template SL1 will use to create the ticket.
- **Edit User.** SL1 user who created or last edited the Ticket from Email policy.
- **Edit Date.** Date the Ticket from Email policy was created or last edited.

Filtering the List of Ticket From Email Policies

The **Tickets From Emails** page (Registry > Ticketing > Email Tickets) includes filters in the top row in the list of policies. You can specify one or more parameters to filter the display of Ticket from Email policies. Only Ticket from Email policies that meet all the filter criteria will be displayed in the **Tickets From Emails** page.

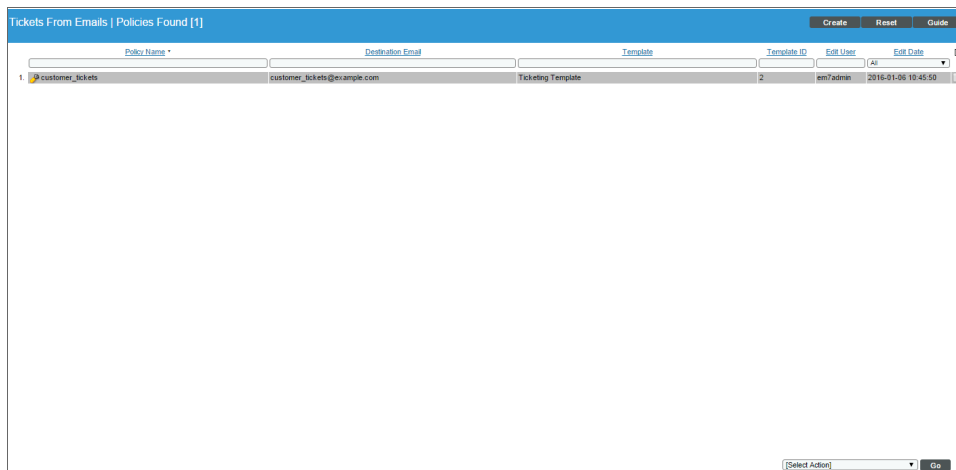
You can filter by one or more of the following parameters. The list of Ticket from Email policies is dynamically updated as you select each filter.

- For each filter except **Edit Date**, you must enter text to match against. SL1 will search for Ticket from Email policies that match the text, including partial matches. Text matches are not case-sensitive. You can use the following special characters in each filter:
 - , (comma). Specifies an "or" operation. For example:
 - "dell, micro" would match all values that contain the string "dell" OR the string "micro".
 - & (ampersand). Specifies an "and" operation. For example:
 - "dell & micro" would match all values that contain the string "dell" AND the string "micro".
 - ! (exclamation mark). Specifies a "not" operation. For example:
 - "!dell" would match all values that do not contain the string "dell".
- **Policy Name**. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Tickets From Emails** page will display only Ticket from Email policies that have a matching name.
- **Destination Email**. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Tickets From Emails** page will display only Ticket from Email policies that are associated with a matching destination email.
- **Template**. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Tickets From Emails** page will display only Ticket from Email policies that include a matching template name.
- **Template ID**. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Tickets From Emails** page will display only Ticket from Email policies that include a matching template ID.
- **Edit User**. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Tickets From Emails** page will display only Ticket from Email policies that have a matching "created by" or "edited by" value.
- **Edit Date**. You can select from a list of time periods. The **Tickets From Emails** page will display only Ticket from Email policies that have been created or edited within that time period.
 - *All*. Display all policies that match the other filters.
 - *Last Minute*. Display only policies that have been created within the last minute.
 - *Last Hour*. Display only policies that have been created within the last hour.
 - *Last Day*. Display only policies that have been created within the last day.
 - *Last Week*. Display only policies that have been created within the last week.
 - *Last Month*. Display only policies that have been created within the last month.
 - *Last Year*. Display only policies that have been created within the last year.

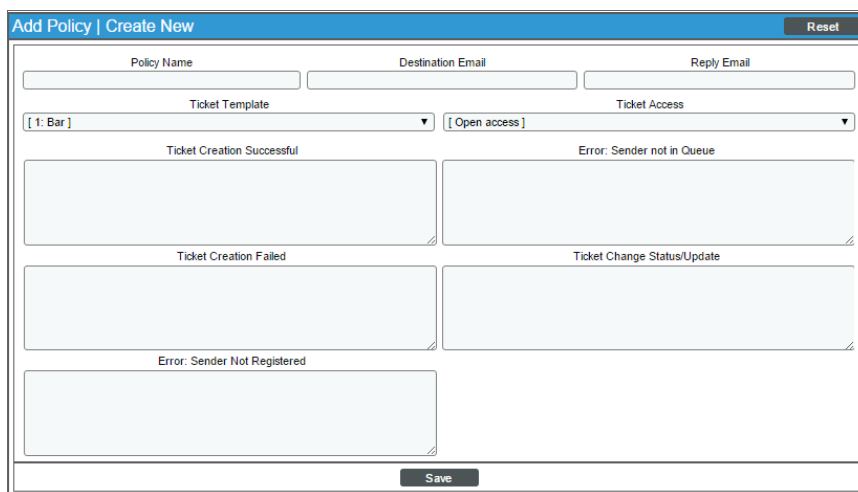
Creating a Ticket From Email Policy

Perform the following steps to create a Ticket From Email policy:

1. Go to the **Tickets From Emails** page (Registry > Ticketing > Email Tickets):



2. In the **Tickets From Emails** page, click the **[Create]** button. The **Add Policy** page appears.



3. In the **Add Policy** page, provide a value in each of the following fields:
 - **Policy Name.** Enter a name for the policy.
 - **Destination Email.** Enter the email address to which ticket emails will be sent. The email address you enter in this field must use one of the fully qualified domain names of the Database Server or All-In-One Appliance, i.e., one of the domain names you entered in the **Authorized Email Domains** field

in the **Email Settings** page. Each Ticket from Email policy should have a unique email address.

- **Reply Email.** Enter the email address from which SL1 will send notification emails. Users will reply to this email address to add notes to tickets created from email.
- **Ticket Template.** Select a ticket template from the drop-down list. For more information on creating a ticket template, see the **Ticketing** manual. The ticket template used will define the ticket queue and other attributes of tickets created by this Ticket from Email policy.
- **Ticket Access.** Select a security level from the drop-down list. The following options are available:
 - **Open Access.** Any email sent to the **Destination Email** address will create a ticket.
 - **Any Registered Users.** Email sent to the **Destination Email** address from an email address associated with a user account in the SL1 system will create a ticket.
 - **Registered Users in Queue.** Email sent to the **Destination Email** address will create a ticket if:
 - The "from" email address is associated with a user account in the SL1 system.
 - The user account also has access to the ticket queue defined in the ticket template.
- **Ticket Creation Successful.** Message that indicates that a ticket has been created successfully from the email.
 - If included in this field, the characters "%!" (without quotation marks) will be replaced with the ticket ID of the newly created ticket.
 - If included in this field, the characters "%W" (without quotation marks) will be replaced with a link to the newly created ticket.
- **Error: Sender not in Queue.** Message that indicates that the ticket could not be created because the **Registered Users in Queue** option has been set, and the sender's email address does not match a user account that has access to the ticket queue defined in the selected ticket template.
- **Ticket Creation Failed.** Message that indicates that the ticket could not be created.
- **Ticket Change Status/Update.** Message that indicates that a note added by email successfully updated a ticket.
 - If included in this field, the characters "%!" (without quotation marks) will be replaced with the ticket ID of the newly created ticket.
 - If included in this field, the characters "%W" (without quotation marks) will be replaced with a link to the newly created ticket.
- **Error: Sender not Registered.** Message that indicates that the ticket could not be created because the **Any Registered Users** option has been set, and the sender's email address does not match a user account.

4. Click the **[Save]** button.

Sending an Email to Create a Ticket

To create a ticket, an inbound email must meet the following requirements:

- The email is sent to an address defined in the **Destination Email** field in a Tickets from Email Policy.
- The email is sent from an address that meets the criteria for the **Ticket Access** setting in the Tickets from Email Policy

If an inbound email meets both these criteria, a ticket will be created. The body of the email will be inserted as the first note in the ticket.

If the "%" character is included in the **Ticket Description** field in the ticket template, the subject of the email will be substituted in for the "%" character.

All other attributes of the ticket, such as queue and severity, are defined by the ticket template associated with the Tickets From Email policy.

Using Email to Add a Note to a Ticket

SL1 automatically sends a notice email (to the original sender of the email) if a ticket is created successfully from an email or if the ticket is updated with an email.

The user who receives the automatic notice email can add a note to the ticket by replying back to SL1. To add a note to the ticket, the user who receives the automatic notice from SL1 should:

- reply to the automatic notice
- not change the subject of the email
- in the body of the email, include the text to attach to the ticket

Email Round-Trip Monitoring Policies

Overview

Email Round-Trip Monitoring Policies monitor round-trip email delivery. Each policy generates performance data for the time between SL1 sending an email to a device and SL1 receiving a reply email from the device. To configure an Email Round-Trip Monitoring Policy, you must create the policy in SL1 and then configure the external device to reply to the emails from the SL1.

Viewing the Email Round-Trip Monitoring Policies

The **Email Round-Trip Monitoring** page (Registry > Monitors > Email Round-Trip) displays the following about each email policy:

- **Policy Name.** Name of the policy.
- **Send Address.** Address to which the policy sends test messages.
- **Policy ID.** Unique, numeric ID assigned to the policy automatically by SL1.
- **Device Name.** Name of the device associated with the policy.
- **IP Address.** IP address of the device associated with the policy. This is the IP address SL1 uses to communicate with the device.
- **Device Category.** Device category of the device associated with the policy.
- **Organization.** Organization for the device associated with the policy.

Filtering the List of Email Round-Trip Monitoring Policies

The **Email Round-Trip Monitoring** page (Registry > Monitors > Email Round-Trip) includes seven filters. You can filter the list of policies by one or multiple of the following parameters: policy name, send address, policy ID, device name, IP address, device category, and organization. You can specify one or more parameters to filter the display of policies. Only policies that meet all the filter criteria will be displayed in the **Email Round-Trip Monitoring** page.

You can filter by one or more of the following parameters. The list of policies is dynamically updated as you select each filter.

- For each filter, you must enter text to match against. SL1 will search for policies that match the text, including partial matches. Text matches are not case-sensitive. You can use the following special characters in each filter:
 - , (comma). Specifies an "or" operation. For example:

dell, micro

would match all values that contain the string "dell" OR the string "micro".
 - ! (exclamation point). Specifies a "not" operation. For example:

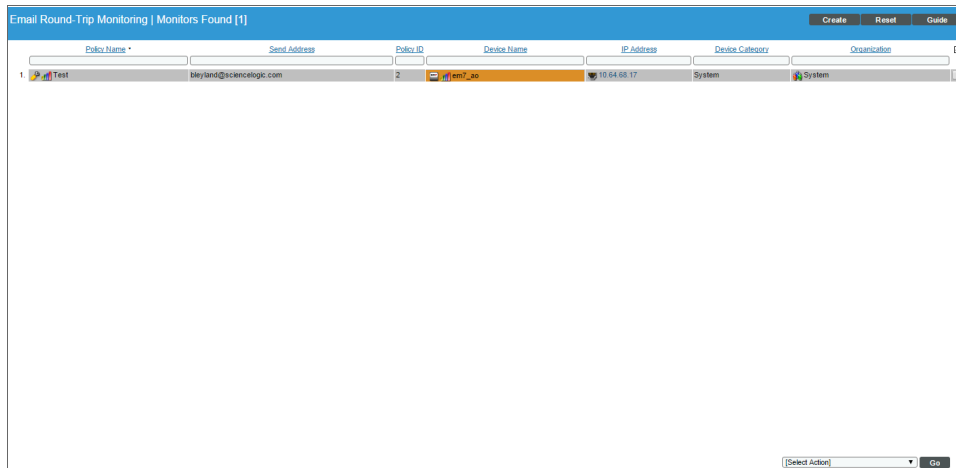
!dell

would match all values that do not contain the string "dell".
- **Policy Name**. You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies that have a matching name.
- **Send Address**. You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies that have a matching send address.
- **Policy ID**. You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies that have a matching policy ID.
- **Device Name**. You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies aligned with a device with a matching device name.
- **IP Address**. You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies aligned with a device with a matching IP address.
- **Device Class**. You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies aligned with a device with a matching device class.
- **Organization**. You can enter text to match, including special characters, and the **Email Round-Trip Monitoring** page will display only policies that have a matching organization.

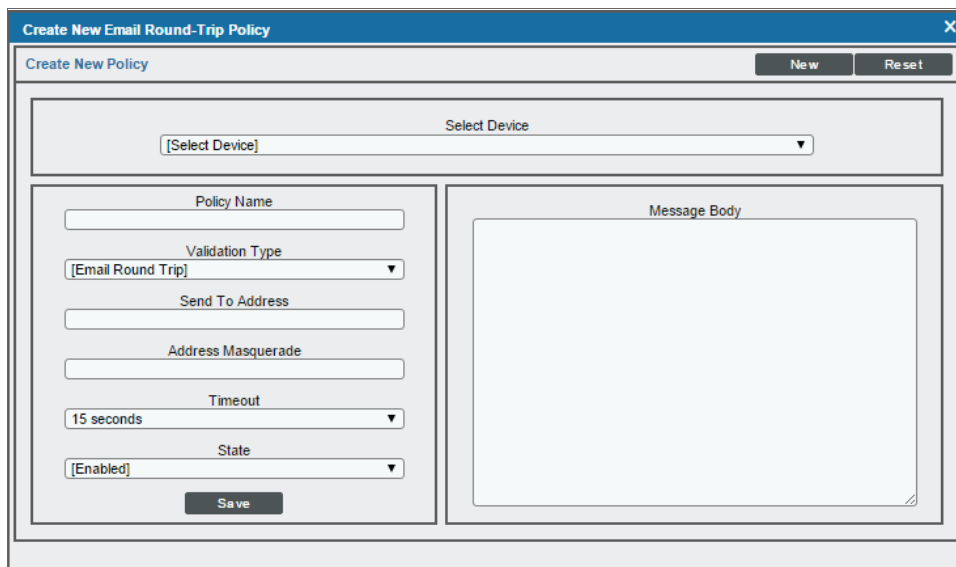
Creating an Email Round-Trip Monitoring Policy

Perform the following steps to configure an Email Round-Trip Monitoring policy:

1. Go to the **Email Round-Trip Monitoring** page (Registry > Monitors > Email Round-Trip):



2. Click the **[Create]** button. The **Create Email Round-Trip Policy** modal window is displayed:



3. To create an Email Round-Trip policy, supply a value in the following fields:

- **Select Device.** From the drop-down list, select the device to monitor. By default, the current device is selected in this field.

NOTE: Before you can define an Email Round-Trip policy, you must decide which managed device you want to associate with the policy. You might want to associate the policy with the device to which SL1 will send test messages, but you aren't required to do so. Alternately, you might want to create a virtual device to associate with an Email Round-Trip policy (for details on defining a virtual device, see the manual *Managing Devices*). Although SL1 will use only the **Send To Address** to execute the policy, the reports that result from the Email Round-Trip policy will be aligned with the device you specify in the **Select Device** field.

- **Policy Name.** Enter a name for the policy.
- **Validation Type.** Can select only *Email Round Trip*.
- **Send To Address.** Email address for external email server. Must be a valid email address. This mailbox must be configured to auto-respond to messages from the Email Round-Trip policy.
- **Address Masquerade.** Email address to use as *From* address. Must be a valid email address. You should choose an address that allows the external email client to easily identify the incoming email as one from the Email Round-Trip policy.
- **Timeout.** Number of seconds SL1 should wait for a response email message. If SL1 does not receive a response message after the specified number of seconds, SL1 generates an event.
- **State.** Specifies whether SL1 should start collecting data specified in this policy from the device. Choices are:
 - *Enabled.* SL1 will collect the data specified in this policy, from the device, at the frequency specified in the **Process Manager** page (System > Settings > Processes) for the **Data Collection: E-Mail round-Trip** process.
 - *Disabled.* SL1 will not collect the data specified in this policy, from the device, until the **State** field is set to *Enabled*.
- **Message Body** Body of the email message to be sent. In some cases, the auto-responder on the external email server may search this message body. Therefore, you should choose a message body that allows the external email client to easily identify the incoming email as one from the Email Round-Trip policy.

4. Click the **[Save]** button.

CAUTION: SL1 will begin sending email to the specified address when the policy is created. You may wish to configure the monitored device before saving the policy.

Configuring the Monitored Device

For an Email Round-Trip Monitoring policy to work correctly, the monitored device must forward the received email back to the SL1 system. You must configure the monitored device to automatically forward the email when policy emails are received. Most email systems allow you to define rules that will automatically forward a received email when the received email meets certain criteria; refer to the documentation for the specific email system on your device for instructions on how to set up a rule for the Email Round-Trip policy. Follow these guidelines when defining your rule:

- Email received from SL1 for Email Round-Trip policies can be identified by the "from" address you defined in the **Address Masquerade** field and the body text you entered in the **Message Body** text area.
- The email generated by the monitored device must be sent from the same address the policy email was delivered to.
- The email generated by the monitored device must be sent to the following address:

`notify@domain-name-of-ScienceLogic-platform`

Where "domain-name-of-ScienceLogic-platform" is one of the fully qualified domain names of the Database Server or All-In-One Appliance, i.e., one of the domain names you entered in the **Authorized Email Domains** field in the **Email Settings** page.

- The subject of the email sent by SL1 must be included in the email generated by the monitored device.
- The body of the email sent by SL1 must be included in the email generated by the monitored device.

© 2003 - 2019, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com



800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010