Best Practices for Escalation

SL1 version 12.2.0

Table of Contents

Chapter

1

Introduction to Escalations

Overview

This chapter provides an overview of SL1 Events and how to use Events with your organization's escalation process.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (☰).
- To view a page containing all of the menu options, click the Advanced menu icon (⋯).

This chapter covers the following topics:

What is an Event?

One of the quickest ways to monitor the health of your network is to look at events. You can view events on the **Events** page in SL1.

Events are alerts that are triggered when a specific condition is met. For example, an event can signal if a server has gone down, if a device is exceeding CPU or disk-space thresholds, or if communication with a device has failed. Alternately, an event can simply display the status of a managed element.

An ***alert*** defines a formula that SL1 evaluates each time data is collected. If the formula evaluates to true during data collection, SL1 generates an alert. Not every alert will trigger an event. An alert must have an ***event policy*** in SL1 that defines the conditions for the event, and when an alert meets the conditions in the event policy, SL1 generates an event.

SL1 generates log messages from incoming trap and syslog data, and also when SL1 executes user-defined policies. SL1 then uses these log messages to generate events. SL1 examines each log message and compares it to each event definition. If a log message matches an event's definition, SL1 generates an event instance and displays the event on the **Events** page.

Each event includes a description of the problem, where the problem occurred (device, network hardware, software, policy violation), a pre-defined severity, the time of first occurrence, the time of most recent occurrence, and the age of the event.

SL1 includes pre-defined events for the most commonly encountered conditions in the most common environments. You can also create custom events for your specific environment or edit the pre-defined events to better fit your specific environment.

What is Escalation?

Escalation is the process through which an organization identifies issues, manages issues, and takes corrective actions related to those issues.

When an issue is ***escalated***, it is sent to a staff member with greater technical knowledge or a higher level of authority than lower-level staff members. Escalation should occur only when all avenues have been exhausted at the lower levels within the organization.

In SL1, automation policies and automation actions allow you to specify the actions you want the system to execute when specific event conditions are met. For example, if nobody in an organization acknowledges an event within 10 minutes, the system can automatically notify a manager. If nobody acknowledges the same event within 20 minutes, the system can notify a director. If nobody acknowledges the same event within 30 minutes, the system can notify a vice president.

For information on how to create an example escalation policy, see ***Escalation Processes***.

Requirements

Before using SL1 to manage event escalation, your organization must include certain business process or standard operating procedures. Examples of these supporting processes and event escalation processes are described in ***Business Processes***.

Chapter 2

Evaluating Your Business Processes and Customizing Events

Overview

Before using SL1 to manage event escalation, your organization must include certain business processes or standard operating procedures:

- Collect and identify critical, major, and minor events.
- Customize events, if necessary, to meet business requirements, such as service level agreements (SLAs).
- Identify the technical and business units that should be involved in event escalation.

These tasks are described in this chapter.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (☰).
- To view a page containing all of the menu options, click the Advanced menu icon (⋯).

This chapter covers the following topics:

Identifying Critical, Major, and Minor Events

Before you can define the escalation procedures for your enterprise, you must determine the severity of events. If you are already using SL1, you can use the **Events** page to collect information about events. You can also examine existing incident records (from outside the system).

In SL1, events are categorized by severity:

- Critical Events indicate a condition that can seriously impair or curtail service and require immediate attention (such as service or system outages).
- Major Events indicate a condition that impacts service and requires immediate investigation.
- Minor Events indicate a condition that does not currently impair service, but needs to be corrected before it becomes more severe.
- Notice Events indicate a condition that does not affect service but about which users should be aware.
- Healthy Events indicate that a device or condition has returned to a healthy state. Frequently, a healthy event is generated after a problem has been fixed.

To determine the severity of an event to your enterprise, ask yourself the following questions about each targeted event:

- Is there service degradation?
    - What levels of degradation are considered Critical? Major? Minor?
- Is there an impact on crucial business processes?
    - What levels of impact are considered Critical? Major? Minor?
- Are internal or external customers affected?
    - How many customers must be affected before the event is considered Critical? Major? Minor?
- Will revenue be lost?
    - Is this issue more or less expensive than other pending issues?
- Will schedules be affected?
    - How likely must delays be before the event is considered Critical? Major? Minor?
- Is there potential for hard failure?
    - How great must this potential be before the event is considered Critical? Major? Minor?

Customizing Pre-Defined Events

After identifying the severity of common events for your business, you might want to customize the default events in SL1 to fit your business requirements.

SL1 includes pre-defined events for common syslog, trap, and SNMP messages, as well as pre-defined events for when SL1 executes user-defined policies. Pre-defined events include event severity, but after identifying events and defining their severity levels for your organization, you can edit the pre-defined severity of events to match your business requirements.

For example, SL1 includes the event "DNS: Nameserver not responding". By default, SL1 assigns this event a severity of "Major". Suppose that your organization determines that this event is a critical event for your business.

To change the severity of the event "DNS: Nameserver not responding":

1. Go to the **Event Policies** page (Events > Event Policies).
2. In the **Event Policies** page, type "DNS: Nameserver Not" in the search bar at the top of the page. The **Event Policies** page displays only the event you want: the event "DNS: Nameserver not responding".
3. To edit the severity of the event, click the Actions menu (•••) and select *Edit*. The **Event Policy Editor** page appears.
4. Click the **[Event Message]** tab and select a new value in the ***Event Severity*** field. For example, change the value from *Major* to *Critical*.
5. Click the **[Save]** button to save the new severity. When this event occurs on any device in your network, SL1 displays an event message with the new Critical severity.
6. For more information about creating your own custom event policy and editing other parameters of an event policy, see the ***Events*** manual .

Customizing Pre-Defined Events in the SL1 Classic User Interface

After identifying the severity of common events for your business, you might want to customize the default events in SL1 to fit your business requirements.

SL1 includes pre-defined events for common syslog, trap, and SNMP messages, as well as pre-defined events for when SL1executes user-defined policies. Pre-defined events include event severity, but after identifying events and defining their severity levels for your organization, you can edit the pre-defined severity of events to match your business requirements.

For example, SL1 includes the event "DNS: Nameserver not responding". By default, SL1 assigns this event a severity of "Major". Suppose that your organization determines that this event is a critical event for your business.

To change the severity of the event "DNS: Nameserver not responding":

1. Go to the **Event Policy Manager** page (Registry > Events > Event Manager).
2. On the **Event Policy Manager** page, type "DNS: Nameserver Not" in the filter-while-you-type search box at the top of the ***Event Policy Name*** column. The **Event Policy Manager** page displays only the event you want: the event "DNS: Nameserver not responding".

3. To edit the severity of the event, click the wrench icon (🔧) to the left of the event name. The **Event Policy Editor** page appears.
4. Select a new value in the ***Event Severity*** field. For example, change the value from *Major* to *Critical*.
5. Click the **[Save]** button at the bottom of the page to save the new severity. When this event occurs on any device in your network, SL1 displays an event message with the new Critical severity.
6. For more information about creating your own custom event policy and editing other parameters of an event policy, see the ***Events*** manual .

Identify Technical Units and Business Units for Event Escalation

When defining an escalation policy, you must determine which technical and business units to include during an escalation. You must also determine each unit's position in the escalation chain.

For the example in ***Example Escalation Processes***, we defined the following units and established their position in the escalation chain):

1. ***Operations staff***. Events are initially handled by the Operations unit.
2. ***Director of Operations***. If the Operations staff does not acknowledge or resolve an event within a predetermined timespan, the event escalates to the Director of Operations.
3. ***Customer Satisfaction Representative***. If the Director of Operations does not acknowledge or resolve an event within a predetermined timespan, the event escalates to a Customer Satisfaction Representative.
4. ***Director of Customer Service***. If the Customer Satisfaction Representative does not acknowledge or resolve an event within a predetermined timespan, the event escalates to the Director of Customer Service.
5. ***Tier-3 Support Engineer***. If the Director of Customer Service does not acknowledge or resolve an event within a predetermined timespan, the event escalates to a Tier-3 Support Engineer.
6. ***Chief Engineer***. If the Tier-3 Support Engineer does not acknowledge or resolve an event within a predetermined timespan, the event escalates to the Chief Engineer.
7. ***Director of Implementation***. If the Chief Engineer does not acknowledge or resolve an event within a predetermined timespan, the event escalates to the Director of Implementation.
8. ***Vice President of Service Delivery***. If the Director of Implementation does not acknowledge or resolve an event within a predetermined timespan, the event escalates to the Vice President of Service Delivery.

Within these units, you must specify which personnel should receive emails during escalation. The units and their position in the escalation chain might differ for your enterprise.

Chapter 3

Escalation Processes and Example Escalation Policy

Overview

This chapter describes sample escalation processes for acknowledging and clearing events, and includes an example of an automation policy that notifies staff if an event has not been acknowledged.

Typically, event escalation includes at least these three escalation processes:

- ***Acknowledgment***. When an event has been acknowledged, the acknowledging user's name appears in the ***Acknowledged*** column for the event on the **Event Console** page. This lets other users know that someone is investigating or taking action on the event. After acknowledgment, the acknowledging user can suppress the event. When a user suppresses an event, he or she specifies that, if this event occurs again on the same device, the event will not appear in the **Event Console**. This prevents the acknowledgment process from being reiterated.
- ***Incident Response***. After an event has been acknowledged (and optionally suppressed), you can then use ScienceLogic Ticketing or another incident response tool to monitor and document the actions required to resolve the event. For more information about managing incident response in SL1, see the ***Incident Management*** manual.
- ***Resolution***. When an event has been resolved, the resolving user can un-suppress the event and then clear it from the **Event Console**. When a user clears an event, he or she removes a single instance of the event from the system. If the event occurs again on the same device, it will reappear in the **Event Console**. The resolution ensures that the event won't occur again on the same device.

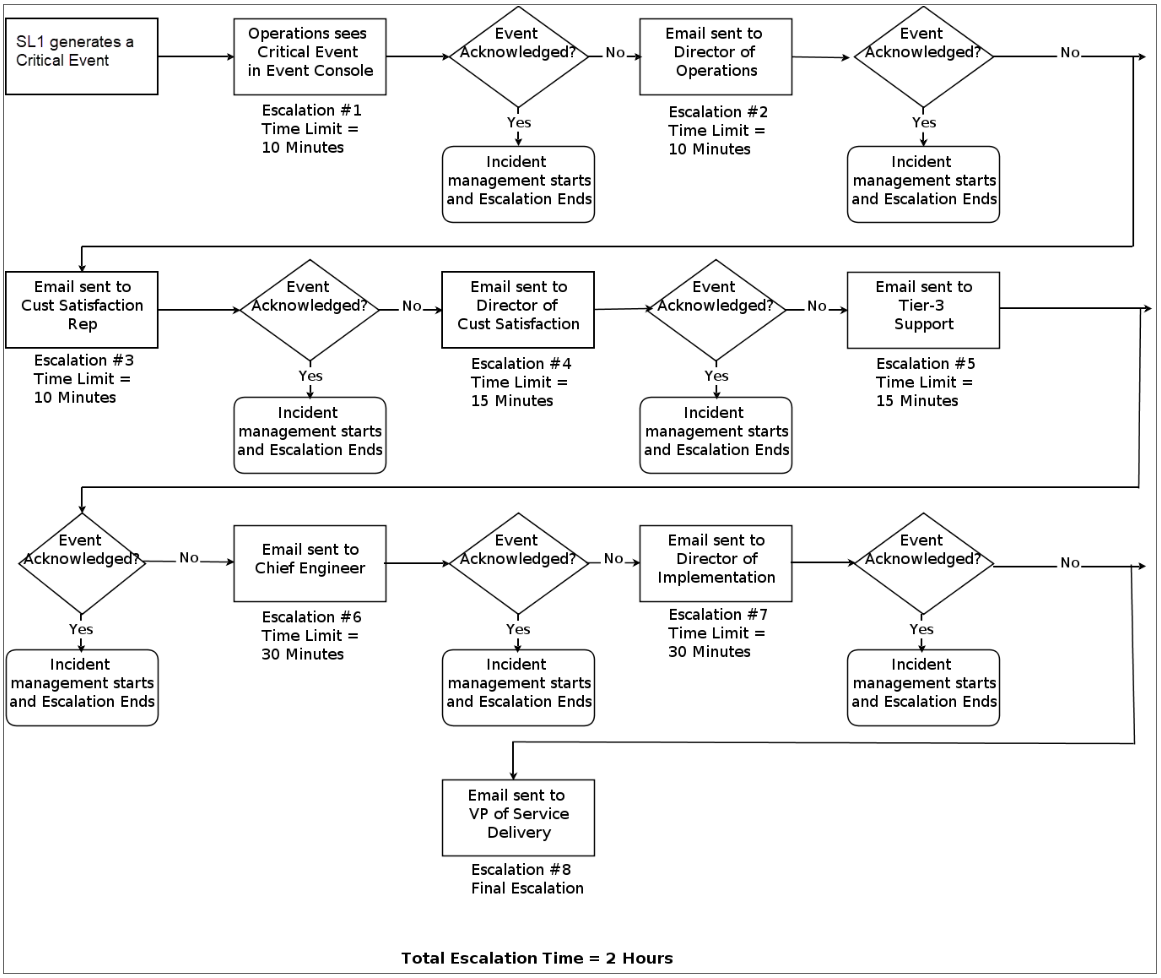
Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon (☰).
- To view a page containing all of the menu options, click the Advanced menu icon (⋯).

This chapter covers the following topics:

Sample Escalation Process for Acknowledging Events

The following is a sample escalation process for acknowledging critical events:


SL1 generates a Critical Event
Operations sees Critical Event in Event Console
Escalation #1 Time Limit = 10 Minutes
Event Acknowledged?
No
Yes
Incident management starts and Escalation Ends
Email sent to Director of Operations
Escalation #2 Time Limit = 10 Minutes
Event Acknowledged?
No
Yes
Incident management starts and Escalation Ends
Email sent to Cust Satisfaction Rep
Escalation #3 Time Limit = 10 Minutes
Event Acknowledged?
No
Yes
Incident management starts and Escalation Ends
Email sent to Director of Cust Satisfaction
Escalation #4 Time Limit = 15 Minutes
Event Acknowledged?
No
Yes
Incident management starts and Escalation Ends
Email sent to Tier-3 Support
Escalation #5 Time Limit = 15 Minutes
Event Acknowledged?
No
Yes
Incident management starts and Escalation Ends
Email sent to Chief Engineer
Escalation #6 Time Limit = 30 Minutes
Event Acknowledged?
No
Yes
Incident management starts and Escalation Ends
Email sent to Director of Implementation
Escalation #7 Time Limit = 30 Minutes
Event Acknowledged?
No
Yes
Incident management starts and Escalation Ends
Email sent to VP of Service Delivery
Escalation #8 Final Escalation
Total Escalation Time = 2 Hours

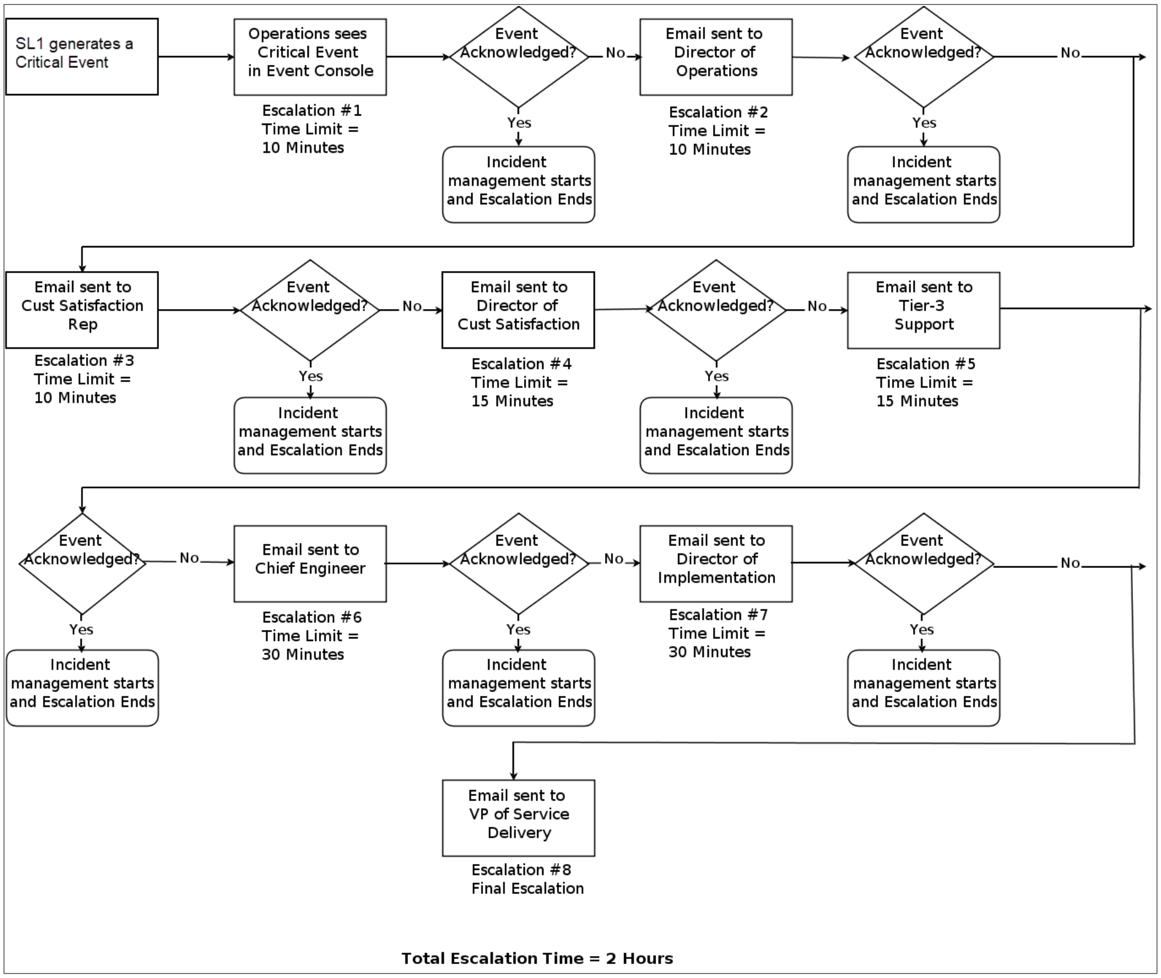
- ***Escalation #1. Operations***. Events are initially handled by the Operations unit. If the Operations staff does not acknowledge a critical event within 10 minutes, the event escalates to the Director of Operations.
- ***Escalation #2. Director of Operations***. If the Director of Operations does not acknowledge a critical event within 10 minutes, the event escalates to a Customer Satisfaction Representative.
- ***Escalation #3. Customer Satisfaction Representative***. If the Customer Satisfaction Representative does not acknowledge a critical event within 10 minutes, the event escalates to the Director of Customer Service.
- ***Escalation #4. Director of Customer Service***. If the Director of Customer Service does not acknowledge a critical event within 15 minutes, the event escalates to a Tier-3 Support Engineer.

- ***Escalation #5. Tier-3 Support Engineer***. If the Tier-3 Support Engineer does not acknowledge a critical event within 15 minutes, the event escalates to the Chief Engineer.
- ***Escalation #6. Chief Engineer***. If the Chief Engineer does not acknowledge a critical event within 30 minutes, the event escalates to the Director of Implementation.
- ***Escalation #7***. ***Director of Implementation***. If the Director of Implementation does not acknowledge a critical event within 30 minutes, the event escalates to the Vice President of Service Delivery.
- ***Escalation #8. Vice President of Service Delivery***. This is the final escalation point.

For major and minor events, the escalation process is similar, except that the time limit for each escalation is longer than the escalations for critical events.

Sample Escalation Process for Clearing Events

The following is a sample escalation process for clearing critical events:


SL1 generates a Critical Event
Operations sees Critical Event in Event Console
Escalation #1 Time Limit = 10 Minutes
Event Acknowledged?
No
Yes
Incident management starts and Escalation Ends
Email sent to Director of Operations
Escalation #2 Time Limit = 10 Minutes
Event Acknowledged?
No
Yes
Incident management starts and Escalation Ends
Email sent to Cust Satisfaction Rep
Escalation #3 Time Limit = 10 Minutes
Event Acknowledged?
No
Yes
Incident management starts and Escalation Ends
Email sent to Director of Cust Satisfaction
Escalation #4 Time Limit = 15 Minutes
Event Acknowledged?
No
Yes
Incident management starts and Escalation Ends
Email sent to Tier-3 Support
Escalation #5 Time Limit = 15 Minutes
Event Acknowledged?
No
Yes
Incident management starts and Escalation Ends
Email sent to Chief Engineer
Escalation #6 Time Limit = 30 Minutes
Event Acknowledged?
No
Yes
Incident management starts and Escalation Ends
Email sent to Director of Implementation
Escalation #7 Time Limit = 30 Minutes
Event Acknowledged?
No
Yes
Incident management starts and Escalation Ends
Email sent to VP of Service Delivery
Escalation #8 Final Escalation
Total Escalation Time = 2 Hours

- ***Escalation #1. Operations***. Events are initially handled by the Operations unit. If the Operations staff does not resolve a critical event within 10 minutes, the event escalates to the Director of Operations.
- ***Escalation #2. Director of Operations***. If the Director of Operations does not resolve a critical event within 10 minutes, the event escalates to a Customer Satisfaction Representative.
- ***Escalation #3. Customer Satisfaction Representative***. If the Customer Satisfaction Representative does not resolve a critical event within 10 minutes, the event escalates to the Director of Customer Service.
- ***Escalation #4. Director of Customer Service***. If the Director of Customer Service does not resolve a critical event within 15 minutes, the event escalates to a Tier-3 Support Engineer.
- ***Escalation #5. Tier-3 Support Engineer***. If the Tier-3 Support Engineer does not resolve a critical event within 15 minutes, the event escalates to the Chief Engineer.
- ***Escalation #6. Chief Engineer***. If the Chief Engineer does not resolve a critical event within 30 minutes, the event escalates to the Director of Implementation.
- ***Escalation #7. Director of Implementation***. If the Director of Implementation does not resolve a critical event within 30 minutes, the event escalates to the Vice President of Service Delivery.
- ***Escalation #8. Vice President of Service Delivery***. This is the final escalation point.

For major and minor events, the escalation process is similar, except that the time limit for each escalation is longer than the escalations for critical events.

Defining Escalation Policies

SL1 includes the **Automation Policy Editor** and the **Action Policy Editor**, which allow you to define escalation policies based upon event severity, elapsed time, and event status (for example, event acknowledged, ticket assigned, event cleared). When specified conditions are met, SL1 automatically performs one or more actions. The action in this example notifies specified team members through email.

For details on defining automation, see the manual ***Run Book Automation***.

Example Escalation Policy for Event Acknowledgment

This section shows how to use the **Automation Policy Editor** and **Action Policy Editor** to create an escalation policy for event acknowledgment.

Creating the Action Policy

Using the escalation processes from the section on *Sample Escalation Processes for Event Acknowledgment*, you can first create an action policy that sends an email message to the Director of Operations.

To create this action policy:

1. Go to the **Action Policy Manager** page (Registry > Run Book > Actions).
2. From the **Action Policy Manager** page, click the **[Create]** button. The **Action Policy Editor** page appears.
3. In the **Action Policy Editor** page, supply values in the following fields:

- ***Action Name***. Type "event_escalation_Dir_of_Ops".
- ***Description***. Type "Email to Director of Operations".
- ***Action Type***. Select *Send an Email Notification*.
- ***Email Subject***. At the beginning of the field, type "Not Acknowledged: " and leave the other values in the field. The entire field should read "Not Acknowledged: %S Events: %M".
- ***Available Emails.*** We selected the email address for our example Director of Operations, *em7admin: mjtest@sciencelogic.com*. If you want to see the emails that result from this action policy, you can select your own email address in this field. After selecting an email address, click the **[>>]** button to add it to the ***Assigned Emails*** field.
- For all other fields, accept the default values.

4. Click the **[Save]** button to save the new action policy.

To create additional action policies for all the steps in section on *Sample Escalation Processes for Event Acknowledgment*, perform the steps above, but supply the following values:

Action Name	Available Emails
event_escalation_CS_rep	Select the appropriate email address for a Customer Satisfaction Representative. If you want to see the emails that result from this action policy, you can select your own email address in this field.
event_escalation_Dir_of_CS	Select the appropriate email address for the Director of Customer Service.
event_escalation_tier3	Select the appropriate email address for a Tier-3 Support Representative.
event_escalation_chief_eng	Select the appropriate email address for a Chief Engineer.
event_escalation_Dir_of_Impl	Select the appropriate email address for a Director of Implementation.
event_escalation_VP_of_Service	Select the appropriate email address for a Vice President of Service Delivery.

Creating the Automation Policy

Using the escalation processes from the section on *Sample Escalation Processes for Event Acknowledgment*, you can create an automation policy that sends an email to the Director of Operations when an event has not been acknowledged for 10 minutes.

To create this automation policy:

1. Go to the **Automation Policy Manager** page (Registry > Run Book > Automation).
2. Click the **[Create]** button. The **Automation Policy Editor** page appears.
3. Supply the following values in the following fields:
   - ***Policy Name***. Type "event_not_acknowleged_10_minutes".
   - ***Organization***. Select *System*. This automation policy will act on all events in your SL1 system.
   - ***Criteria Logic***. These fields specify the conditions that must be met before the system executes the action specified in the automation policy. All conditions must be met for at least one of the selected events on at least one of the selected devices.

    - *Severity Operator*. Select *Severity =*.
    - *Severity*. Select *Critical*.
    - *Elapsed time*. The length of time that must elapse after the event occurs but before the system evaluates the other criteria in the automation policy. Select *and 10 minutes has elapsed*.
    - *Status*. Event must have the specified status. Select *and event is NOT acknowledged*.

- ***Available Actions.*** Select the action policy you defined in the ***Creating the Action Policy*** section, *Send Email: event_escalation_Dir_of_Ops*. Click on the **[>>]** button. The selected action policy will appear in the ***Aligned Actions*** field.
- For all other fields, accept the default values.

4. Click the **[Save]** button to save the new automation policy. Now when an event occurs with a severity of Critical, on any device, and that event is not acknowledged within ten minutes, the system sends an email to the Director of Operations.

To create additional automation policies for all the steps in the section on ***Sample Escalation Processes for Event Acknowledgment***, perform the steps above, but supply the following values:

Policy Name	Elapsed Time	Available Actions
event_not_acknowleged_20_minutes	and 20 minutes have elapsed.	event_escalation_CS_rep
event_not_acknowleged_30_minutes	and 30 minutes have elapsed.	event_escalation_Dir_of_CS
event_not_acknowleged_45_minutes	and 45 minutes have elapsed.	event_escalation_tier3
event_not_acknowleged_60_minutes	and 1 hour has elapsed	event_escalation_chief_eng
event_not_acknowleged_90_minutes	and 1 hour 30 minutes has elapsed	event_escalation_Dir_of_Impl
event_not_acknowleged_120_minutes	and 2 hours has elapsed.	event_escalation_VP_of_Service

Example Email and Example Logs

When the system generates an event with a severity of "Critical" and the event is not acknowledged within 10 minutes, the system automatically sends an email, as defined in the example policy above.

In the **Events** page, you can view the escalation actions by clicking the number hyperlink in the ***Automated Actions*** column for a critical event.

If you are using the SL1 classic user interface, you can go to the **Event Console** and view the escalation actions by clicking the mail icon (✉) for a critical event.

The user interface displays the **Event Actions Log** page, where you can view a record of the escalation action.

Chapter

4

Compliance

Overview

If your organization must comply with government regulations like HIPAA, Sarbanes-Oxley, or Gramm-Leach-Bliley, or if your organization is adopting standards like PCI DSS, CoBIT, ISO, or ITIL, you should take close note of the requirements for compliance when designing an escalation policy. Commonly, IT compliance requires scrutiny of:

- Risk Management
- Security
- Data Management
- Business Continuity and Disaster Recovery
- Incident Response
- Documentation and Audit Logs

A well-planned escalation policy can address all of these functional areas and aid with compliance.

SL1 centrally monitors and manages events and escalations. For compliance purposes, controls that are standardized, centrally administered, and repeatable encompass "best practices."

SL1 standardizes and automates the escalation workflow. Automated processes provide greater efficiencies and improved controls by minimizing vulnerabilities to fraud, user error, and malicious use. Because of this, automated processes greatly aid compliance efforts.

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. For more information, see https://sciencelogic.com/company/legal.

ScienceLogic

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

International: +1-703-354-1010