Incident Management

SL1 version 12.2.0

Table of Contents

Chapter

1

Overview of Concepts for Incident Management

Overview

This chapter introduces the concepts of Incident Management in SL1.

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:

Super Service Provider

The following examples use the fictional company Super Service Provider.

The Network Operations Center (NOC) for Super Service Provider is responsible for monitoring service delivery, customer satisfaction, SLA compliance, and emergency management.

The NOC acts as the initial point of contact for all customer requests, incidents, and problems. NOC personnel either resolve the problem or escalate the ticket to the appropriate Engineering teams.

Super Service Provider is governed by Service Level Agreements (SLAs) in place between Super Service Provider and its customers.

Organizations

An *organization* is a group for managing elements and user accounts. All hardware, software, policies, events, tickets, and users in SL1 are associated with an organization.

The bare-bones characteristics of an organization are:

- A unique name (required)
- Users who are members of the organization
- Elements, such as devices, that are associated with the organization

Organizations can be defined by geographic areas, departments, types of devices, or any structure that works best for your needs.

> NOTE: For more details on organizations, see the **Organizations and Users** manual.

For this example, we will create two organizations:

- *NOC*. Personnel who work in the NOC will be members of the NOC organization.
- *Engineering*. Personnel who work in the Engineering department will be members of the Engineering organization.

Tickets

A *ticket* is a request for work. This request can be in response to a problem that needs to be fixed, for routine maintenance, or for any type of required work.

In this example, tickets can come from customers, an automated monitoring system, or an internal employee.

In this example, the request in each ticket can be classified into one of the following categories:

- **Request**. A minor change or request for information.

- **Incident**. A service interruption or degradation.

- **Event**. An alert or notification created by a monitoring tool.

- **Project**. A temporary endeavor undertaken to meet unique goals and objectives.

- **Emergency**. An incident that impacts more than one customer.

- **Other**. Any item not classified as one of the types listed above.

Ticket Source

Ticket source is a description of where the ticketed originated.

In this example, tickets originate from one of the following sources:

- **Email**. Email ticket created by a customer and received by NOC staff.

- **Portal**. Ticket created by a customer through the portal.

- **Phone**. Telephone call from customer to NOC staff. NOC staff creates a ticket and assigns the ticket to an engineering queue for resolution.

- **Event**. Event created by an automated management system. NOC staff creates a ticket and assigns the ticket to an Engineering queue for resolution.

- **Other**. Any ticket opened not as a result of one of the sources listed above. An example might be a ticket opened by an internal employee of Super Service Provider suggesting an improvement.

To comply with their Service Level Agreements and to improve operational efficiency or workflow, Super Service Provider has policies in place to handle tickets based on the ticket source.

For example, NOC staff must review and triage tickets that are generated by customers through email or the online portal. The NOC personnel determines the appropriate severity and actions, and the correct Engineering team to engage.

Tickets created by employees of Super Service Provider, or tickets from an automated management system, can be placed directly into the queue that corresponds to the engineering team responsible for resolving the ticket.

Ticket Severity

Tickets are assigned a *severity* based on the importance of the issue that needs to be fixed or worked on. For example, a server failing might require a critical ticket, while a routine maintenance issue might require only a minor ticket. Ticket severities include healthy, notice, minor, major, and critical.

In this example, Super Service Provider uses severities to define the urgency of the problem, required response times, and SLAs. Super Service Provider classifies work by using one of the following severities:

- **Critical**. A service outage that requires an immediate response.

- **Major**. A service degradation or imminent service outage that requires a response within one hour.

- **Minor**. A minor change or request for information that requires a response within four hours.

- **Notice**. A minor change or request for information that requires a response within one day.

- **Healthy**. A minor change or request for information that requires a response within three days.

Ticket Status

Ticket status provides a quick way to identify the current state of the ticket. The possible ticket statuses include:

- **Open**. The ticket has been created.

- **Pending**. Someone acknowledged the ticket and is awaiting the next action.

- **Working**. Someone is working on the ticket.

- **Resolved**. The issue has been resolved.

In this example, Super Service Provider examines ticket status to monitor compliance with Service Level Agreements. In addition, Super Service Provider also examines the following information about each ticket to monitor compliance with Service Level Agreements:

- **Assigned To**. Specifies a user, who must be a member of the current ticket queue, to whom the ticket has been assigned.

Ticket Queues

Ticket queues allow you to organize and filter tickets. Organizing tickets by ticket queues and then assigning users to ticket queues allows each user to see only the tickets that are relevant to him or her.

You can also use ticket queues to move tickets through a pre-defined workflow. In our example, Super Service Provider uses the following ticket queues:

- **Triage**. All new tickets from customer emails or customer access to the portal are assigned to this queue. The NOC staff manages this queue.

- **Network Engineering**. Tickets are assigned to this queue if someone from the Network Engineering team must work on and resolve the ticket. Only employees of Super Service Provider can assign tickets to this queue.

- **Windows Engineering**. Tickets are assigned to this queue if someone from the Windows Engineering team must work on and resolve the ticket. Only employees of Super Service Provider can assign tickets to this queue.

- **Linux Engineering**. Tickets are assigned to this queue if someone from the Linux Engineering team must work on and resolve the ticket. Only employees of Super Service Provider can assign tickets to this queue.

- **Follow-up**. Tickets are assigned to this queue after the request or repair has been completed, but the NOC staff or Engineering staff are waiting for customer confirmation or approval before setting the status of the tickets to Resolved.

Service Level Agreements

A *Service Level Agreement* or *SLA* is a written contract between a service provider and its customers. An SLA describes the service that will be provided for each fee, the level of customer support, and the penalty when that service is not provided. For example, many Internet service providers use SLAs that specify percentage of uptime, guaranteed performance benchmarks, help-desk response time, and advance notification of changes that could affect the customer.

In our example, SLAs are based on ticket status (open, pending, working, resolved), the **Assigned To** value, and the severity (healthy, notice, minor, major, critical) of each ticket.

In our example, Super Service Provider is governed by several Service Level Agreements (SLAs) between Super Service Provider and its customers.

New Ticket SLAs

These SLAs determine the actions that Super Service Provider must perform on each **new ticket** and how quickly Super Service Provider must perform these actions.

- *New Acknowledgment SLA*. All new tickets must be **acknowledged within 15 minutes** of creation. A ticket is considered acknowledged when its status changes from Open to Pending.

- *New Assignment SLA*. All new tickets must be **assigned to an engineer within 30 minutes** of creation. A ticket is considered assigned when a user is associated with the ticket.

Existing Ticket SLAs

These SLAs determine the actions that Super Service Provider must perform on each existing ticket **after it has been assigned** to an engineer, and how quickly Super Service Provider must perform these actions.

- *Existing Updated SLA*. After a ticket has been assigned to Engineering, the ticket severity determines the required acknowledgment as follows:

  - *Critical*. Tickets with a severity of Critical must be **updated within 35 minutes** of assignment. To update the ticket, the assigned user can assign the ticket to someone else, change the status of the ticket to Working, or add a note to the ticket.

  - *Major*. Tickets with a severity of Major must be **updated within one hour** of assignment. To update the ticket, the assigned user can assign the ticket to someone else, change the status of the ticket to Working, or add a note to the ticket.

  - *Minor*. Tickets with a severity of Minor must be **updated within four hours** of assignment. To update the ticket, the assigned user can assign the ticket to someone else, change the status of the ticket to Working, or add a note to the ticket.

  - *Notice*. Tickets with a severity of Notice must be **updated within one day** of assignment. To update the ticket, the assigned user can assign the ticket to someone else, change the status of the ticket to Working, or add a note to the ticket.

○ *Healthy*. Tickets with a severity of Healthy must be **updated within three days** of assignment. To update the ticket, the assigned user can assign the ticket to someone else, change the status of the ticket to Working, or add a note to the ticket.

Escalation

Ticket escalation policies automatically perform actions on a ticket when specified conditions have been met.

For example, the escalation conditions could be "if a ticket has a severity of 'major,' is three days old, and has not yet been assigned to a user." When a ticket meets those conditions, the escalation policy performs the actions "change ticket's severity to 'critical' and assign the ticket to the queue administrator."

The example uses the following escalation policies:

- *NEW ACKNOWLEDGMENT SLA VIOLATION IMMINENT*. When the ticket age is 10 minutes AND the ticket has not been acknowledged (status changed from Open to Pending), SL1 sends a notification to all NOC queue members indicating an SLA violation is imminent.

- *NEW ACKNOWLEDGMENT SLA VIOLATION HAS OCCURRED*. When the ticket age is 15 minutes AND the ticket has not been acknowledge (status changed from Open to Pending), SL1 sends a notification to the Director of Operations indicating an SLA violation has occurred.

- *NEW ASSIGNMENT SLA VIOLATION IMMINENT*. When the ticket age is 25 minutes AND the ticket has not been assigned to a user, SL1 sends a notification to all NOC queue members indicating an SLA violation is imminent.

- *NEW ASSIGNMENT SLA VIOLATION HAS OCCURRED*. When the ticket age is 30 minutes AND the ticket has not been assigned, SL1 sends a notification to the Director of Operations indicating an SLA violation has occurred.

- *CRITICAL UPDATE SLA VIOLATION IS IMMINENT*. When the ticket has not been modified in 30 minutes AND the ticket has not been updated, SL1 sends a notification to all Engineering queue members.

- *CRITICAL UPDATE SLA VIOLATION HAS OCCURRED*. When the ticket has not been modified in 35 minutes AND the ticket has not been updated, SL1 sends a notification to the Director of Engineering.

- *MAJOR UPDATE SLA VIOLATION IS IMMINENT*. When the ticket has not been modified in 55 minutes AND the ticket has not been updated, SL1 sends a notification to all Engineering queue members.

- *MAJOR UPDATE SLA VIOLATION HAS OCCURRED*. When the ticket has not been modified in one hour AND the ticket has not been updated, SL1 sends a notification to the Director of Engineering.

- *MINOR UPDATE SLA VIOLATION IS IMMINENT*. When the ticket hasn't been modified in three hours and 55 minutes AND the ticket has not been updated, SL1 sends a notification to all Engineering queue members.

- *MINOR UPDATE SLA VIOLATION HAS OCCURRED*. When the ticket hasn't been modified in four hours AND the ticket has not been updated, SL1 sends a notification to the Director of Engineering.

- *NOTICE SLA VIOLATION IS IMMINENT*. When the ticket hasn't been modified in 23 hours and 55 minutes AND the ticket has not been updated, a notification is sent to all Engineering queue members.

- *NOTICE UPDATE SLA VIOLATION HAS OCCURRED*. When the ticket hasn't been modified in one day AND the ticket has not been updated, SL1 sends a notification to the Director of Engineering.

- ***HEALTHY UPDATE SLA VIOLATION IS IMMINENT***. When the ticket hasn't been modified in two days, 23 hours, and 55 minutes AND the ticket has not been updated, SL1 sends a notification to all Engineering queue members.

- ***HEALTHY UPDATE SLA VIOLATION HAS OCCURRED.*** When the ticket hasn't been modified in three days AND the ticket has not been updated, SL1 sends a notification to the Director of Engineering.

Chapter

2

Workflow for Tickets

Workflow for Tickets

This chapter describes the ticketing workflow.

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:

Ticket Source and Queues

At Super Service Provider, NOC staff monitor all incoming tickets.

Tickets created by customer emails and tickets created by customers through the portal are sent directly to the **Triage** ticket queue. The policies for tickets from email and the policies for the portal specify that tickets from these sources must be placed in the **Triage** ticket queue.

NOC staff monitor the **Triage** queue and assign to each ticket the appropriate severity, status, queue, and user account.

Tickets created by NOC staff (all other sources) are assigned to the appropriate severity, status, queue, and user account upon creation. As a result, these tickets go directly to the appropriate **Engineering** ticket queue: Network Engineering, Windows Engineering, or Linux Engineering.

The **Followup** queue is a holding area for tickets that need approval before they are assigned the status Resolved.
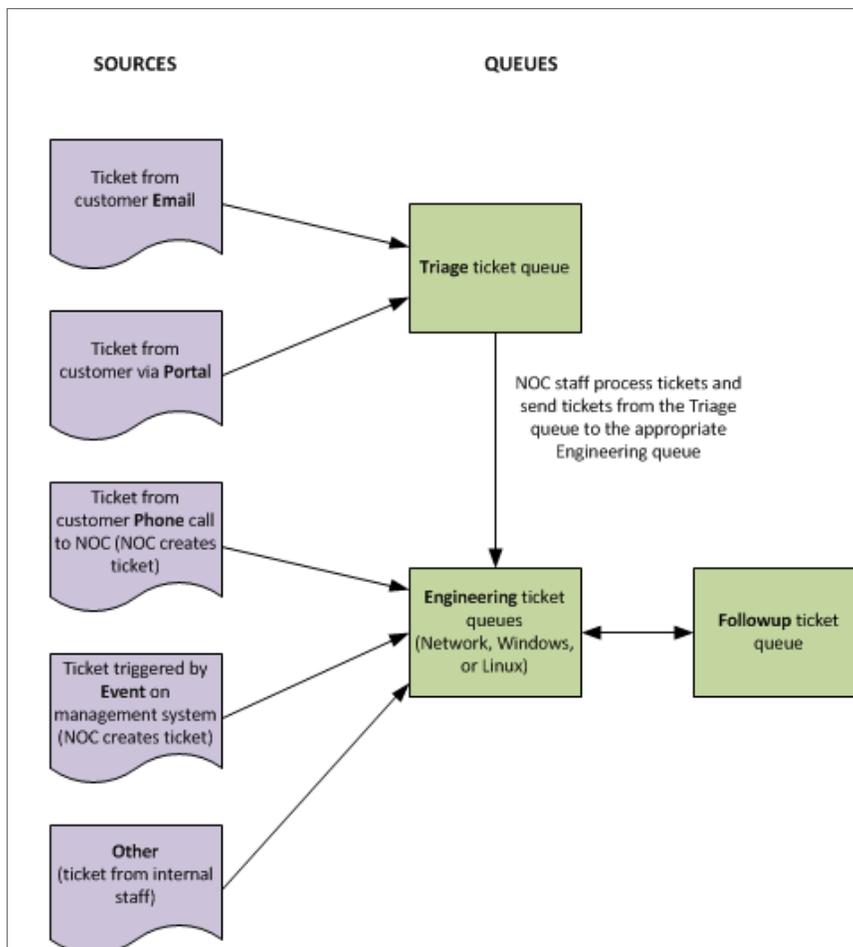
Use the following menu options to navigate the SL1 user interface:

- 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 (⋯).

Workflow for Compliance with SLA

This section shows how a customer-generated ticket moves through the workflow at Super Service Provider to comply with the SLAs:

Remember that the SLAs for Super Service Provider are:

- *New Acknowledgment SLA*. All new tickets must be **acknowledged within 15 minutes** of creation. A ticket is considered acknowledged when its status changes from Open to Pending.
- *New Assignment SLA*. All new tickets mustbe **assigned to an engineer with 30 minutes** of creation. A ticket is considered assigned when a user is associated with the ticket.
- *Existing Updated SLA*. After a ticket is assigned to Engineering, the ticket severity determines the required acknowledgment as follows:

- *Critical*. Tickets with a severity of Critical must be **updated within 35 minutes** of assignment. To update the ticket, the assigned user can assign the ticket to someone else, change the status of the ticket to Working, or add a note to the ticket.

- *Major*. Tickets with a severity of Major must be **updated within one hour** of assignment. To update the ticket, the assigned user can assign the ticket to someone else, change the status of the ticket to Working, or add a note to the ticket.

- *Minor*. Tickets with a severity of Minor must be **updated within four hours** of assignment. To update the ticket, the assigned user can assign the ticket to someone else, change the status of the ticket to Working, or add a note to the ticket.

- *Notice*. Tickets with a severity of Notice must be **updated within one day** of assignment. To update the ticket, the assigned user can assign the ticket to someone else, change the status of the ticket to Working, or add a note to the ticket.

- *Healthy*. Tickets with a severity of Healthy must be **updated within three days** of assignment. To update the ticket, the assigned user can assign the ticket to someone else, change the status of the ticket to Working, or add a note to the ticket.

Chapter

3

Creating Organizations and Users

Overview

This chapter covers how to create organizations and users to use in the example workflow. This chapter does not go into detail about organizations and users beyond the examples in this manual. For details on organizations and users, see the manual *Organizations and Users*.
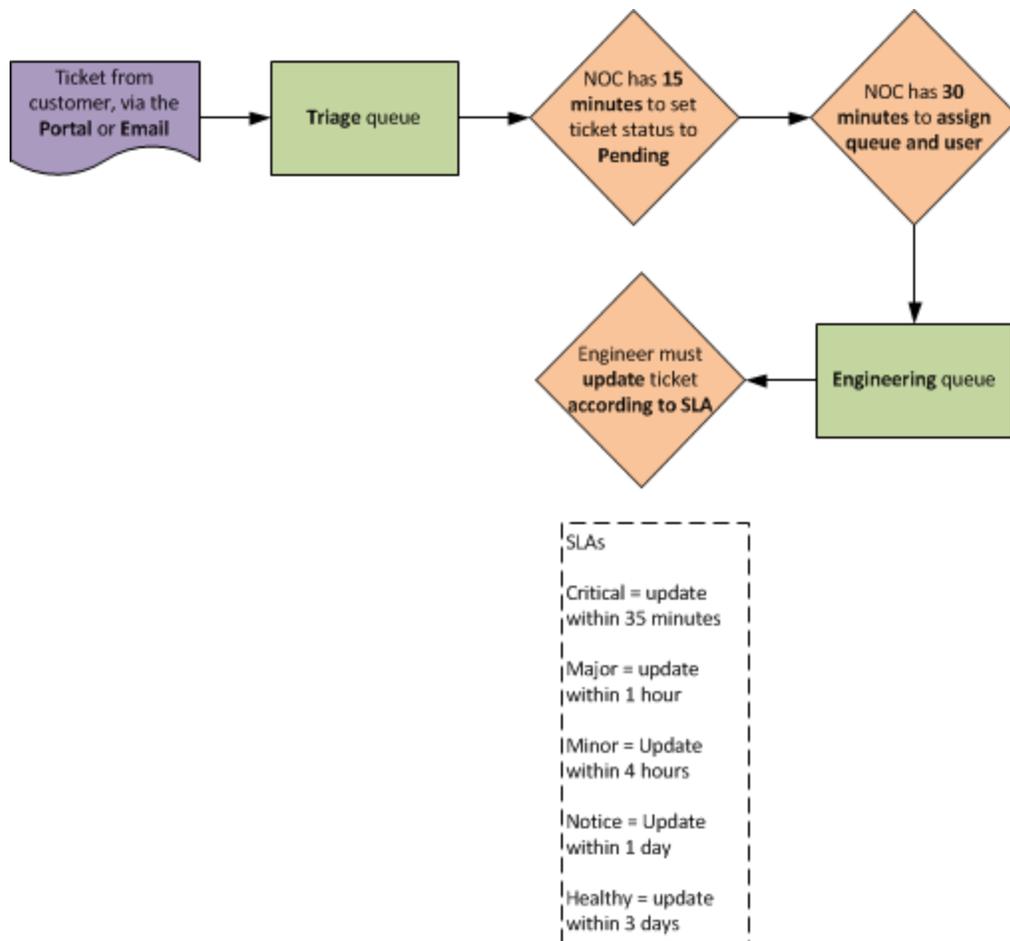
Use the following menu options to navigate the SL1 user interface:

- 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:

Creating the Organizations

We need to create two organizations:

- NOC
- Engineering

To create an organization:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. Click the **[Create]** button. The **Add Organizational Record** page appears.
3. Supply the following values in the **Add Organizational Record** page:

    - *Organization Name*. Type "NOC".
    - *City*. Type "Reston".
    - *State*. Type "Virginia".

4. Click the **[Save]** button.
5. Click the **[Close]** button.
6. On the **Organizational Account Administration** page, click the **[Create]** button. The **Add Organizational Record** page appears.
7. Supply the following values on the **Add Organizational Record** page:

    - *Organization Name*. Type "Engineering".
    - *City*. Type "Reston".
    - *State*. Type "Virginia".

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

Creating the User Accounts

To see how tickets move through the workflow at Super Service Provider, we need to create user accounts for each organization.

To create the user accounts, we need to first create two user policies:

- *NOC* policy, for members of the NOC organization
- *Engineering* policy, for members of the Engineering organization

User Policies allow you to define a custom set of account properties and key privileges, and then save them as a policy for reuse. When you create a user account, you can use the User Policy to quickly apply settings to the new account.

To create the user policies and apply the policies to user accounts, follow the instructions in the next two sections.

Creating the User Policies

To create user policies:

1. Go to the **User Policies** page (Registry > Accounts > User Policies) and then click the **[Create]** button. The **User Policy Properties Editor** page appears.

2. On the **User Policy Properties Editor** page, you can:

   - Supply a value in each field that you want to include in the user policy.

   - Click on the field name for each field you want to disable in the user policy. When you disable a field, its value is not applied to member User Accounts.

   > **NOTE**: If you have disabled fields in the User Policy, you must manually define these fields in the **Account Permissions** page for each aligned user account.

3. First, create the user policy **NOC**. Supply the following values in the **User Policy Property Editor** page:

   - *Policy Name*. Type "NOC".

   - *Login State*. Select *Active*. User accounts created with this policy are active and can log in to SL1.

   - *Account Type*. Select *Administrator*. This type of user has unlimited permissions in SL1.

   > **NOTE**: For security purposes in production environments, you might want to create accounts of type *User* and assign only the required Privilege Keys to the user policy. For details on Privilege Keys, see the manual **Access Permissions**.

   - *Password Strength*. Accept the default value of *Good*. Passwords must be at least eight characters long and contain at least one number or one symbol.

   - *Password Expiration*. Accept the default value of *Disabled*. Passwords do not expire.

   - *Password Shadowing*. Accept the default value of *Default*. Users cannot reuse passwords from the past year.

   - *Require Password Reset*. Accept the default value of (*unselected*). If selected, the user will be prompted to change his or her password at the next login.

   - *Authentication Method*. Accept the default value of *EM7 Session*. The user's username and password are authenticated by the database.

   - *Restrict to IP*. Leave this field blank.

   - *Event Console Default Display*. Accept the default value of *Flat events table*.

   - *Ticket Queue Memberships*. Leave this field blank. After you *define ticket queues*, you must come back to this user policy and select the following ticket queues:

- ○ *Triage*
- ○ *Linux Engineering*
- ○ *Network Engineering*
- ○ *Windows Engineering*
- ○ *Followup*

- *Primary Organization*. Select *NOC*. This specifies the primary organization, and will be the default organization for user accounts aligned with this policy.

- *Theme*. Accept the default value, *ScienceLogic: White + Blue Titlebars*. This specifies the backgrounds, colors, fonts, and graphics that will appear when a user logs in.

- *Time Zone*. Accept the default (*New_York*).

- *Additional Organization Memberships*. Select *(All organizations)*. This allows NOC members to view tickets from all users and process those tickets. To select, highlight one or more organizations.

- *Privilege Keys*. Leave this field blank. Users of type "Administrator" automatically have access to all pages and actions in SL1. The Privilege Keys section is grayed-out for "Administrator" policies.

- *Re-Apply All Settings to All Policy Members*. Select this checkbox. When you update and save the policy, all settings are re-applied to all policy members.

4. Click the **[Save]**button to save your new user policy. The new policy now appears in the **User Policies** page.

5. To create the *Engineering* user policy, perform steps 1-4 using the values in the table below. If a field is not specified in the table below, accept the default value for the field.

Field	Value
Policy Name	Engineering
Login State	Active
Account Type	Administrator
Ticket Queue Membership	*None*. You will come back later and assign: • *Linux Engineering* • *Network Engineering* • *Windows Engineering* • *Followup*
Primary Organization	Engineering
Additional Organization Memberships	NOC, System (allows work between ticket queues)

Aligning User Policies with User Accounts

For our example, we create the following users:

User	User Policy	Role
David Kahane	NOC	NOC staff
Larry Levy	NOC	NOC staff
Griffin Mill	NOC	Director of Operations
Bonnie Sherow	NOC	NOC staff
Fred Fenster	Engineering	Windows Engineer
Dean Keaton	Engineering	Linux Engineer
Roger Kint	Engineering	Director of Engineering
Jeff Rabin	Engineering	Network Engineer

NOTE: The examples in the *Scenarios* explicitly use Larry Levy, Bonnie Sherow, Griffin Mill, Dean Keaton, and Roger Kint.

To align a user with a user policy:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).

2. Click the **[Create]** button. The **Create New Account** page appears.

3. On the **Create New Account** page, supply the following information:

   - *Account Type*. Select *Policy Membership*. This activates the list of user policies in the Policy Membership pane.

   - *Account Templates*. Select *Admin:NOC*. The settings from the NOC user policy are applied to this account. Fields that are defined in the user policy are grayed out.

   - *First Name*. Type "David".

   - *Last Name*. Type "Kahane".

   - *Account Login Name.* Type "dkahane".

   - *Primary Email*. Type "dkahane@super.com".

   - *Password*. Type a password of your choice.

   - *Confirm Password*. Type the password again.

   - *Country*. Use the default of *United States*.

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

5. When prompted, click the **[OK]** button to confirm that you want to save changes to the user account. The **Account Permissions** page appears, with the permissions from the user policy applied. All fields that are included in the user policy are grayed-out.

6. You can perform steps 1-5 to create the other users for the examples in this chapter. The **Account Login Name** is always first initial plus last name. The **Primary Email** is always *account login name*@super.com, such as dkahane@super.com.

Chapter

4

Customizing Ticket Source

Overview

Ticket source is a description of where the ticket originated. Super Service Provider uses the following types of Ticket Sources:

- **Email**. Email ticket created by a customer and received by the NOC staff.
- **Portal**. Ticket created by a customer through the portal.
- **Phone**. Telephone call from a customer to the NOC staff. The NOC staff creates a ticket and assigns the ticket to an Engineering queue for resolution.
- **Event**. Event created by an automated management system. The NOC staff creates a ticket and assigns the ticket to an engineering queue for resolution.
- **Other**. Any ticket opened not as a result of one of the sources list above. For example, a ticket that was opened when an internal employee of Super Service Provider suggests an improvement.

Email and **Phone** are default values that appear in the **Source** drop-down list in the **Ticket Editor** page. The remaining values are not the default values that appear in the **Source** drop-down list in the **Ticket Editor** page. However, you can edit the values that appear in the **Source** drop-down list. This chapter explains how to customize these values.

The **Select Objects Editor** page allows you to define and edit the entries that appear in drop-down fields in the the user interface.

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:

Deprecating the Default Values for Source

Before you can add new values for the *Source* drop-down list in the **Ticket Editor** page, you must deprecate the current default values that Super Service Provider does not plan to use.

To deprecate the default values:

1. Go to the **Select Objects Editor** page (System > Customize > Select Objects).

2. On the **Select Objects Editor** page, use the *Filter* drop-down list to select **Ticketing: Source**.

3. The **Select Objects Registry** pane updates with all of the entries for the *Source* drop-down list.

4. Find the entry for *Automated* and click its wrench icon (🔧). The **Select Objects Editor** section at the top updates with the values from *Automated*.

5. Select the *Deprecate* checkbox. When you select this checkbox, *Automated* no longer appears in the *Source* drop-down list. In instances of a page where *Automated* was previously selected, the entry still appears as the selected value for the *Source* drop-down list. In instances of a page where *Automated* was not previously selected, it no longer appears in the *Source* drop-down list.

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

7. Repeat steps 2-6 for the following entries:

   - *External*
   - *Internal*

Creating New Values for Source

On the **Select Objects Editor** page, you can create the three new entries for the *Source* drop-down list on the **Ticket Editor** page.

To create a new entry for the *Source* drop-down field:

1. Go to the **Select Objects Editor** page (System > Customize > Select Objects).

2. In the **Select Objects Editor** page, use the *Filter* drop-down list to select **Ticketing: Source**. The **Select Objects Registry** pane updates with all the entries for the *Source* drop-down list.

3. To add an entry to the selected drop-down list, go to the top pane in the **Select Objects Editor** page and supply values in the following fields:

   - *Definition/Value*. Type "Portal".

   - *Access*. Select >=*Users* to allow users of account type "user" and users of account type "administrator" to see this new entry.

   - *Permission Keys*. Do not select any entries.

   - *Ignore Keys for New Tickets*. Do not select this checkbox.

   - *Deprecate*. Do not select this checkbox.

4. Click the **[Add]** button to add the new entry. The entry now appears in the **Select Objects Registry** pane for the selected drop-down list, and the entry also appears in the *Source* drop-down list on the **Ticket Editor** page.

5. Repeat steps 3-4 for the remaining new entries, using the following values:

Definition/Value	Access	Permission Keys	Ignore Keys for New Tickets	Deprecate
Event	>=Users	Do not select any entries	Do not select this checkbox	Do not select this checkbox
Other	>=Users	Do not select any entries	Do not select this checkbox	Do not select this checkbox

> **NOTE**: If a page in the user interface includes a gray plus sign icon (+) next to a drop-down list, you can create a new entry in the drop-down list directly from that page. To add an entry, click the plus icon and type the text you want to appear in the drop-down list. Click the **[Save]** button on that page to save the entry. The entry is added to the **Select Objects Registry** page.

Chapter

5

Creating Ticket Queues

Overview

Ticket queues allow you to organize and filter tickets. Organizing tickets by ticket queues and then assigning users to ticket queues allows each user to see only the tickets that are relevant to him or her. You can also use ticket queues to move tickets through a pre-defined workflow.

In this example, Super Service Provider uses the following ticket queues:

- **Triage**. All new tickets from customer emails or customer access to the portal are assigned to this queue. The NOC staff manages this queue.

- **Network Engineering**. Tickets are assigned to this queue if someone from the Network Engineering team must work on and resolve the ticket. Only employees of Super Service Provider can assign tickets to this queue.

- **Windows Engineering**. Tickets are assigned to this queue if someone from the Windows Engineering team must work on and resolve the ticket. Only employees of Super Service Provider can assign tickets to this queue.

- **Linux Engineering**. Tickets are assigned to this queue if someone from the Linux Engineering team must work on and resolve the ticket. Only employees of Super Service Provider can assign tickets to this queue.

- **Follow-up**. Tickets are assigned to this queue after the request or repair has been completed, but the NOC staff or Engineering staff are awaiting customer confirmation and approval before setting the tickets' status to Resolved.

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:

Creating the Ticket Queues for Super Service Provider

To create the ticket queues for Super Service Provider:

1. Go to the **Ticket Queue Management** page (Registry > Ticketing > Queues).

2. Click the **[Create]** button. The **Ticket Queue Properties** page appears.

3. Supply values in the following fields:

   - *Ticket Queue Name*. Type "Triage".

   - *Description*. Type "tickets from email, portal".

   - *Custom Forms*. Accept the default value of (*No Custom Apps Available*). This options allows users to add custom fields to existing pages and to add custom tabbed-pages to sets of pages. When you select a custom form, it appears in the ticket panel for each ticket in the queue.

   - *Required Custom Fields*. Accept the default value of (*No Custom Fields Available*). Each ticket assigned to the queue includes a list of custom fields that the user must populate before saving the ticket. The user interface will not save the ticket until the user populates these custom fields. These custom fields and custom tabs are defined in the **Application Forms** page (System > Customize > Form Fields).

   - *Queue Administrator*. Accept the default value of (*None*). The queue administrator is a user who is visible to all members of the queue and to whom all members, regardless of account type or organization, can assign tickets.

   - *Ticket Email Type*. Accept the default value of (*Authenticated User*). Specifies what outgoing ticket emails will contain in the "From" field. The "From" field in outgoing emails sent from the **[Message]** tab in the **Ticket Editor** page will contain the name of the user who last edited the ticket.

   - *Queue Email Address*. Accept the default value of (*blank*).

   - *Notify Watchers of Changes*. Select this checkbox. When you define a list of "watchers" for a ticket queue or for an individual ticket, SL1 automatically notifies those watchers when a ticket is created or assigned, or if its status changes.

   - *Queue Locked to Admin Only*. Accept the default value of (*not selected*). If this checkbox is selected, only the user designated as the Queue Administrator or a user of type "Administrator" can edit this queue definition.

   - *Email Last Ticket Comment In Updates*. Select this checkbox. When a ticket is edited and SL1 automatically sends an email to the ticket creator, ticket assignee, and optionally the ticket's watchers, the email includes the text of the last note added to the ticket.

   - *Hide queue name from non-queue members*. Accept the default value of (*not selected*). If this checkbox is selected, any tickets assigned to this queue display the queue name only for queue members; "Restricted Queue" displays as the name to non-queue members.

   - *Auto-Resolve Children with Parent Ticket*. Select this checkbox. This option enables SL1 to automatically resolve all children tickets when a parent ticket is resolved.

   - *Queue Members*. Do not select any members in this section, because you will update the user policies to apply queue membership. This section displays a list of all users defined in SL1.

4. Click the **[Save]** button to save the new ticket queue. This queue now appears in the list on the **Ticket Queue Management** page.

5. Perform steps 2-4 for each for the remaining ticket queues, supplying the following values. If a field does not appear in this table, accept the default value:

Ticket Queue Name	Description	Notify Watchers of Changes	Email Last Ticket Comment in Updates	Queue Members	Save button
Network Engineering	work for network engineers	Select	Select	*Do not select*. You will update the user policies to apply queue membership.	Click
Windows Engineering	work for Windows engineers	Select	Select	*Do not select*.	Click
Linux Engineering	work for Linux engineers	Select	Select	*Do not select*.	Click
Followup	tickets awaiting final approval	Select	Select	*Do not select*.	Click

Updating the User Policies

After you have created the ticket queues, you must update the *user policies*.

To update the user policies:

1. Go to the **User Policies** page (Registry > Accounts > User Policies).

2. Find the *NOC* policy and click its wrench icon (🔧). The **User Policy Properties Editor** page appears.

3. In the *Ticket Queue Membership* field, press **Ctrl** and select the following:

   - *Triage*
   - *Linux Engineering*
   - *Network Engineering*
   - *Windows Engineering*
   - *Followup*

4. Select the **Re-apply All Settings To All Policy Members** checkbox.

5. Click the **[Save]** button. Exit from the policy.

6. Find the *Engineering* policy and click its wrench icon (🔧). The **User Policy Properties Editor** page appears.

7. In the *Ticket Queue Membership* field, press **Ctrl** and select the following:

- *Linux Engineering*
- *Network Engineering*
- *Windows Engineering*
- *Followup*

8. Select the **Re-apply All Settings To All Policy Members** checkbox.

9. Click the **[Save]** button. Exit from the policy.

Chapter

6

Tickets from Email and Tickets from Portal

Overview

This chapter explains how to create tickets from email and from a Portal.

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:

Ticket Templates

To ensure that tickets with a source of email are assigned the correct status, source, and ticket queue, you can create a ticket template. This ticket template applies to all tickets that are generated by an email from a customer to Super Service Provider. Ticket templates can be created, edited, and deleted from the **Ticket Templates** page.

To create a ticket template for tickets with a source of email:

1. Go to the **Ticket Templates** page (Registry > Ticketing > Templates).

2. Click the **[Create]** button. The **Template Editor** page appears.

3. On the **Template Editor** page, supply values in the following fields:

   - *Description*. This is a read-only field that displays the value of the **Ticket Description** field.

   - *Organization*. Select *Automatically assign*. The resulting ticket is automatically assigned to an organization. If this field is set to *Automatically assign*, when SL1 receives an email for a Tickets from Email policy, SL1 attempts to match the "From" address in the email to a user. If successful, SL1 assigns the resulting ticket to the user's organization. If SL1 cannot match the "From" address to a user, SL1 assigns the resulting ticket to the **System** organization.

> **NOTE**: In the section on *Organizations and Users*, you assigned NOC users to all organizations, including the **System** organization as an additional organization. As a result, each NOC user can view tickets associated with this Tickets from Email policy.

   - *Element*. *Accept the default value*.

   - **Feature Use**. Select *Ticketing*. This option specifies where in SL1 this template is used.

   - *Template Name*. Type "Email Source Tickets" for the name of this template.

   - *Ticket Description*. Type "**%7**". SL1 uses the subject line of the inbound email as part of the ticket description. SL1 substitutes the subject line of the inbound email for the **%7** variable.

   - *Ticket State*. *Leave blank*. This field is a custom parameter that is defined in the **Ticket States** page (Registry > Ticketing > Custom States). This field lets you add additional workflow restrictions to a ticket.

   - *Severity*. *Accept the default value*. Severity of the ticket will be determined during review by NOC staff.

   - *Category*. *Accept the default value*.

   - *Source*. Select *Email*.

   - *Queue*. Select *Triage*.

   - *Assigned User*. Select *None*. The ticket will be assigned to an engineer during review by NOC staff.

4. Click the **[Save]** button to save the template.

Tickets from Email

SL1 can create tickets based on received email. The **Tickets From Emails** page allows users to configure:

- One or more destination addresses to which external programs can send email. SL1 turns all emails sent to the specified email addresses into tickets.

- Default ticket templates to use when creating the tickets.

- Default reply messages to send back to the email originator.

Before you can create a Tickets from Email policy, you must configure SL1 and your DNS records:

- Define **System Settings** that allow SL1 to receive incoming email.

- Ensure that the **DNS server** that handles name-service for SL1 network is configured correctly to **direct email to SL1**.

- For details on performing these tasks, see the manual on **Inbound Email**.

To create a Ticket From Email policy:

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

2. Click the **[Create]** button. The **Add Policy** page appears.

3. Type a value in each of the following fields:

   - *Policy Name.* Type "customer_tickets".

   - *Destination Email.* Type the email address that includes SL1 email domain. Emails that are sent to this address are placed in a specific mailbox and converted into tickets. On the example system, we used *customer_tickets@patch-aio.qa.sciencelogic.local*. The value after the @ characters will be specific to your network.

   - *Reply Email.* Type the email address that includes SL1 email domain. Each policy can automatically send messages when tickets are created or edited and can also send messages when an error occurs. The email address supplied in this field allows users to reply to these automated policy messages. When a user replies to an automated policy message, SL1 automatically copies the text in the body of the reply email message and adds that text as a note to the associated ticket. On the example system, we used *reply_tickets@patch-aio.qa.sciencelogic.local*. The value after the @ characters will be specific to your network

   - *Ticket Template.* Select the template you created earlier, which you named **Email Source Tickets**. The ticket template defines the ticket queue and other attributes of tickets created by this policy.

   - *Ticket Access.* Select *Open Access*. Any email sent to the **Destination Email** address creates a ticket.

   - *Email Note Visibility*. Leave the default value of *Message body as uncloaked note*. The message body of incoming emails is added to the ticket as an uncloaked note that is visible to all users who can view the ticket.

SL1 can send automatic notification emails from the **Reply Email** address. You can specify message text for any of the five results. If there is no message defined for a result, no reply mail is sent when that result occurs. The possible results are:

- **Ticket Creation Successful**. Type "Successfully created ticket %t."

- **Error: Sender not in Queue**. Leave blank.

- **Ticket Creation Failed**. Type "Failed to create ticket from email."

- **Ticket Change Status/Update**. Type "Successfully updated ticket %t."

- **Error: Sender not Registered.** Leave blank.

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

Tickets from an External Website (Portal)

To allow customers to create tickets in SL1 from an external website, such as the ScienceLogic Support Site, you can use the ScienceLogic API. The ScienceLogic API allows external systems to programmatically access data in SL1. The API gives access to SL1 resources—such as tickets—using standard HTTP request/response protocols. Much like the user interface provides access to SL1 for end users, the API provides access to SL1 for external systems.

You can use the API to build a ticketing interface. For Super Service Provider, the ticketing interface should automatically set the following values in each ticket:

Ticketing Field	Value
Status	Open
Source	Portal
Ticket Queue	Triage

To create a ticket in SL1, the customer must have an account. Before allowing a customer to access the ticketing interface, Super Service Provider must create accounts for the customer. The account must include Access Keys that allow the customer to create a ticket and add a note to a ticket.

For details on using the API, see the manual **The ScienceLogic API**.

Chapter

7

Creating Escalation Policies

Overview

For Super Service Provider, escalation policies help NOC personnel and engineers comply with the SLAs between Super Service Provider and its customers.

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:

Service Level Agreements

Remember that the SLAs for Super Service Provider are:

- *New Acknowledgment SLA*. All new tickets must be **acknowledged within 15 minutes** of creation. A ticket is considered acknowledged when its status changes from Open to Pending.

- *New Assignment SLA*. All new tickets mustbe **assigned to an engineer with 30 minutes** of creation. A ticket is considered assigned when a user is associated with the ticket.

- *Existing Updated SLA*. After a ticket is assigned to Engineering, the ticket severity determines the required acknowledgment as follows:

    - *Critical*. Tickets with a severity of Critical must be **updated within 35 minutes** of assignment. To update the ticket, the assigned user can assign the ticket to someone else, change the status of the ticket to Working, or add a note to the ticket.

    - *Major*. Tickets with a severity of Major must be **updated within one hour** of assignment. To update the ticket, the assigned user can assign the ticket to someone else, change the status of the ticket to Working, or add a note to the ticket.

    - *Minor*. Tickets with a severity of Minor must be **updated within four hours** of assignment. To update the ticket, the assigned user can assign the ticket to someone else, change the status of the ticket to Working, or add a note to the ticket.

    - *Notice*. Tickets with a severity of Notice must be **updated within one day** of assignment. To update the ticket, the assigned user can assign the ticket to someone else, change the status of the ticket to Working, or add a note to the ticket.

    - *Healthy*. Tickets with a severity of Healthy must be **updated within three days** of assignment. To update the ticket, the assigned user can assign the ticket to someone else, change the status of the ticket to Working, or add a note to the ticket.

Escalation Policies

Ticket escalation policies automatically perform actions on a ticket when the specified conditions have been met.

For example, the escalation conditions could be "if a ticket has a severity of 'major,' is three days old, and has not yet been assigned to a user." When a ticket meets those conditions, the escalation policy could perform the actions "change ticket's severity to 'critical' and assign the ticket to the queue administrator."

In our example, we will create and use the following escalation policies:

- *NEW ACKNOWLEDGMENT SLA VIOLATION IMMINENT*. When the ticket age is 10 minutes AND the ticket has not been acknowledged (status changed from Open to Pending), SL1 sends a notification to all NOC queue members indicating an SLA violation is imminent.

- *NEW ACKNOWLEDGMENT SLA VIOLATION HAS OCCURRED*. When the ticket age is 15 minutes AND the ticket has not been acknowledge (status changed from Open to Pending), SL1 sends a notification to the Director of Operations indicating an SLA violation has occurred.

- *NEW ASSIGNMENT SLA VIOLATION IMMINENT*. When the ticket age is 25 minutes AND the ticket has not been assigned to a user, SL1 sends a notification to all NOC queue members indicating an SLA violation is imminent.
- *NEW ASSIGNMENT SLA VIOLATION HAS OCCURRED*. When the ticket age is 30 minutes AND the ticket has not been assigned, SL1 sends a notification to the Director of Operations indicating an SLA violation has occurred.
- *CRITICAL UPDATE SLA VIOLATION IS IMMINENT*. When the ticket has not been modified in 30 minutes AND the ticket has not been updated, SL1 sends a notification to all Engineering queue members.
- *CRITICAL UPDATE SLA VIOLATION HAS OCCURRED*. When the ticket has not been modified in 35 minutes AND the ticket has not been updated, SL1 sends a notification to the Director of Engineering.
- *MAJOR UPDATE SLA VIOLATION IS IMMINENT*. When the ticket has not been modified in 55 minutes AND the ticket has not been updated, SL1 sends a notification to all Engineering queue members.
- *MAJOR UPDATE SLA VIOLATION HAS OCCURRED*. When the ticket has not been modified in one hour AND the ticket has not been updated, SL1 sends a notification to the Director of Engineering.
- *MINOR UPDATE SLA VIOLATION IS IMMINENT*. When the ticket hasn't been modified in three hours and 55 minutes AND the ticket has not been updated, SL1 sends a notification to all Engineering queue members.
- *MINOR UPDATE SLA VIOLATION HAS OCCURRED*. When the ticket hasn't been modified in four hours AND the ticket has not been updated, SL1 sends a notification to the Director of Engineering.
- *NOTICE SLA VIOLATION IS IMMINENT*. When the ticket hasn't been modified in 23 hours and 55 minutes AND the ticket has not been updated, a notification is sent to all Engineering queue members.
- *NOTICE UPDATE SLA VIOLATION HAS OCCURRED*. When the ticket hasn't been modified in one day AND the ticket has not been updated, SL1 sends a notification to the Director of Engineering.
- *HEALTHY UPDATE SLA VIOLATION IS IMMINENT*. When the ticket hasn't been modified in two days, 23 hours, and 55 minutes AND the ticket has not been updated, SL1 sends a notification to all Engineering queue members.
- *HEALTHY UPDATE SLA VIOLATION HAS OCCURRED*. When the ticket hasn't been modified in three days AND the ticket has not been updated, SL1 sends a notification to the Director of Engineering.

Creating the Escalation Policies

To create the escalation policies for Super Service Provider:

1. Go to the **Ticketing Escalation Policies** page (Registry > Ticketing > Escalations).
2. Click the **[Create]** button. The **Create New Escalation Policy**the **Create New Escalation Policy** page appears.
3. Supply the following values:

- *For Ticket Queue*. Select *Triage*. This escalation policy acts on tickets in this ticket queue.

- *Policy Name*. Type "NEW ACKNOWLEDGMENT SLA VIOLATION IMMINENT".

- *State*. Select *Enabled*. Specifies that the escalation policy is active.

Escalation Condition

These seven fields specify the conditions that must be met before SL1 executes the ticket escalation policy:

- *Ticket Status Threshold*. Select *When ticket state is open*. A ticket must have this specified status before SL1 will execute the escalation policy.

- *Ticket Severity Threshold*. Select *and severity is >= "Sev 5 / Healthy"* to include all severities. A ticket must have the specified severity before SL1 will execute the escalation policy.

- *Age Type Threshold*. Select *and ticket's create age is*. A ticket must have the age specified in this field (and the next three fields) before SL1 will execute the escalation policy.

- *Minutes Threshold*. Select *10 minutes* as the number of minutes that have elapsed.

- *Hours Threshold*. Select *None* as the number of hours that have elapsed.

- *Days Threshold*. Select *None*as the number of days that have elapsed.

- *User Action Threshold*. Select *and ticket is not updated*. A ticket must have the specified user action before SL1 will execute the escalation policy.

Escalation Action

These four fields specify the actions that the ticket escalation policy will execute:

- *Severity Action*. Accept the default, *Make no change to ticket severity*. If selected, when a ticket meets all the thresholds specified in the **Escalation Condition** fields, the escalation policy automatically changes the ticket's severity.

- *Queue Action*. Accept the default value, *LEAVE in "Triage" queue*. If selected, when a ticket meets all the thresholds specified in the **Escalation Condition** fields, the escalation policy automatically changes the ticket's queue.

- *User Action*. Accept the default, *Keep MEMBER assignment (if possible)*. If selected, when a ticket meets all the thresholds specified in the **Escalation Condition** fields, the escalation policy automatically changes the ticket's assigned user.

- *Notify Action*. Select *Notify selected queue members*. When a ticket meets all the thresholds specified in the **Escalation Condition** fields, the escalation policy automatically notifies these users.

- *Status ticket*. Accept the default value, *Make no change to ticket status*. If selected, when a ticket meets all the thresholds specified in the **Escalation Condition** fields, the escalation policy automatically changes the ticket status.

Notification Action

If a ticket meets all of the conditions specified in the *Escalation Condition* fields, the escalation policy can automatically notify users. In this section, you can specify who the escalation policy will notify when the policy is executed:

- *Queue Members*. Select *all queue members*. If a ticket meets all the thresholds in the escalation policy, the selected users are notified of changes executed by the escalation policy and of the current status of the ticket.

- *Non-Queue Members*. Accept the default (*no selections*). If selected, when a ticket meets all the thresholds in the escalation policy, the selected users are notified of changes executed by the escalation policy and of the current status of the ticket.

- **Add Message to Ticket**. In this field, you can type text that is automatically added to the *Notes & Attachments* field of the **Ticket Editor** page for the ticket. This field is optional. Type "NEW ACKNOWLEDGMENT SLA VIOLATION IMMINENT. Acknowledge ticket immediately."

- *Cloaked*. *Don't select*. If selected, when a note is added to the ticket as part of the escalation, that note is cloaked. A cloaked note can be viewed only by:

  ○ The user who created the note

  ○ All users of type "administrator"

  ○ Users in the same organization as the user who created the note who have Access Hooks that allow them to view the ticket where the cloaked note resides and who also have the Access Hook "Ticket:Notes:Cloaked"

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

5. Click the **[Close]** button. For information on creating the other escalation policies, see the *Data for Escalation Policies* section.

Chapter

8

Example Scenarios

Overview

This chapter provides five examples of the workflow for incident management for Super Service Provider.

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:

New Ticket Was Not Acknowledged
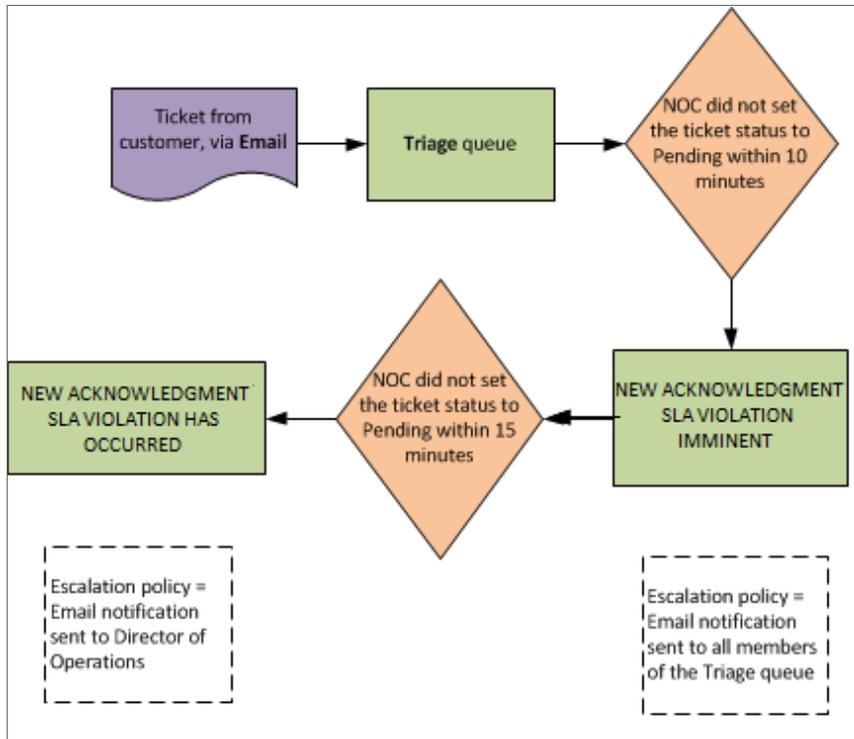
1. A customer sends a ticket email to the address in the *Tickets from Email policy*, customer_tickets@patch-aio.qa.sciencelogic.local.

2. The *ticket template Email Source Tickets* processes the email and creates a ticket.

3. When the ticket is not acknowledged for 10 minutes, SL1 sends the following email to each member of the Triage queue:

From: EM7 Event Notifier [mailto:rtt@patch-aio.qa.sciencelogic.local]
Sent: Wednesday, March 14, 2015 9:07 PM
To: Larry Levy
Subject: TICKET ESCALATED: #8982 | Can't log in to customer portal | 2015-03-14 20:47:35 | 2015-03-14 20:47:35

DESCRIPTION: Can't log in to customer portal

CREATED ON: 2015-03-14 20:47:35

LAST UPDATED AT: 2015-03-14 20:47:35

ESCALATED BY POLICY: NEW ACKNOWLEDGMENT SLA VIOLATION IS IMMINENT. Acknowledge ticket immediately.

TICKET STATE: OPEN

TICKET QUEUE: Triage

NEW ACKNOWLEDGMENT SLA VIOLATION IS IMMINENT. Acknowledge ticket immediately.

http://ap.server.url//em7/index.em7?exec=ticket_management&pop_modal=1&q_type=tid&q_val=16986&q_status=0.1.2&q_arg=8982

4. When the ticket is not acknowledged for 15 minutes, SL1 sends the following email to the Director of Operations:

From: EM7 Event Notifier [mailto:rtt@patch-aio.qa.sciencelogic.local]
Sent: Wednesday, March 14, 2015 9:07 PM
To: Griffin Mill
Subject: TICKET ESCALATED: #8982 | Can't log in to customer portal | 2015-03-14 20:47:35 | 2015-03-14 20:47:35

DESCRIPTION: Can't log in to customer portal

CREATED ON: 2015-03-14 20:47:35

LAST UPDATED AT: 2015-03-14 20:47:35

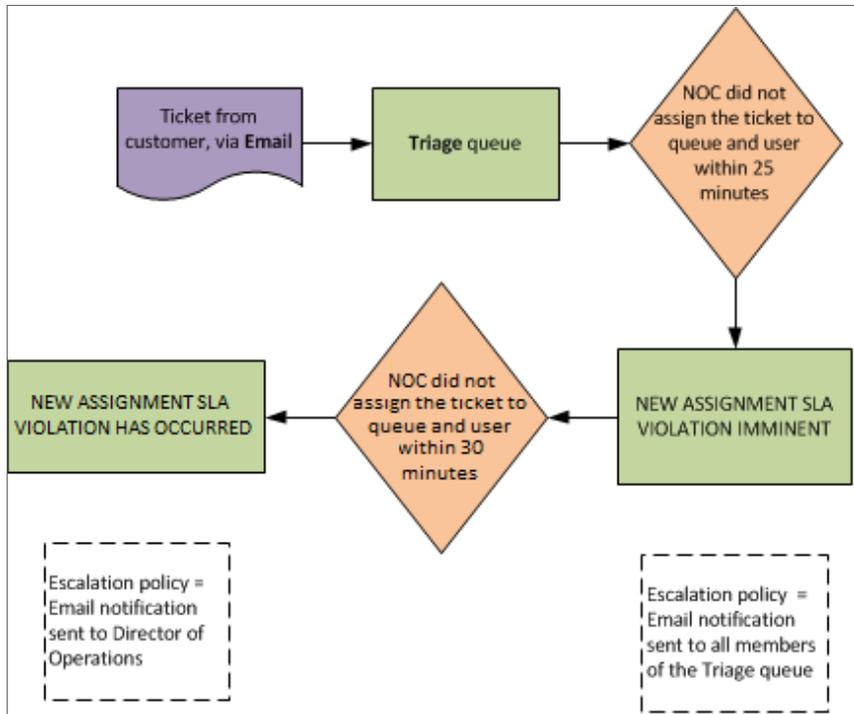ESCALATED BY POLICY: NEW ACKNOWLEDGMENT SLA VIOLATION HAS OCCURRED

TICKET STATE: OPEN

TICKET QUEUE: Triage

NEW ACKNOWLEDGMENT SLA VIOLATION HAS OCCURRED

http://ap.server.url//em7/index.em7?exec=ticket_management&pop_modal=1&q_type=tid&q_val=16986&q_status=0.1.2&q_arg=8982

New Ticket Was Not Assigned

1. A customer sends a ticket email to the address in the *Tickets from Email policy*, customer_tickets@patch-aio.qa.sciencelogic.local.

2. The *ticket template Email Source Tickets* processes the email and creates a ticket.

3. When the ticket is not assigned after 25 minutes, SL1 sends the following email to each member of the Triage queue:

```
From: EM7 Event Notifier [mailto:rtt@patch-aio.qa.sciencelogic.local]
Sent: Wednesday, April 8, 2015 9:56 PM
To: Bonnie Sherow
Subject: TICKET ESCALATED: #8983 | Web server not allowing uploads | 2015-04-08 21:31:22 | 2015-04-08 01:32:04

DESCRIPTION: Web server not allowing uploads

CREATED ON: 2015-04-08 21:31:22

LAST UPDATED AT: 2015-04-08 21:32:04

ESCALATED BY POLICY: NEW ASSIGNMENT SLA VIOLATION IS IMMINENT

TICKET STATE: PENDING

TICKET QUEUE: Triage

NEW ASSIGNMENT SLA VIOLATION IMMINENT.  Assign ticket immediately.


http://ap.server.url//em7/index.em7?exec=ticket_management&pop_modal=1&q_type=tid&q_val=16986&q_status=0.1.2&q_arg=8983
```

4. When the ticket is not assigned after 30 minutes, SL1 sends the following email to the Director of Operations:

```
From: EM7 Event Notifier [mailto:rtt@patch-aio.qa.sciencelogic.local]
Sent: Wednesday, April 8, 2015 9:56 PM
To: Griffin Mill
Subject: TICKET ESCALATED: #8983 | Web server not allowing uploads | 2015-04-08 21:31:22 | 2015-04-08 01:32:04

DESCRIPTION: Web server not allowing uploads

CREATED ON: 2015-04-08 21:31:22

LAST UPDATED AT: 2015-04-08 21:32:04

ESCALATED BY POLICY: NEW ASSIGNMENT SLA VIOLATION HAS OCCURRED

TICKET STATE: PENDING

TICKET QUEUE: Triage

NEW ASSIGNMENT SLA VIOLATION HAS OCCURRED

http://ap.server.url//em7/index.em7?exec=ticket_management&pop_modal=1&q_type=tid&q_val=16986&q_status=0.1.2&q_arg=8983
```
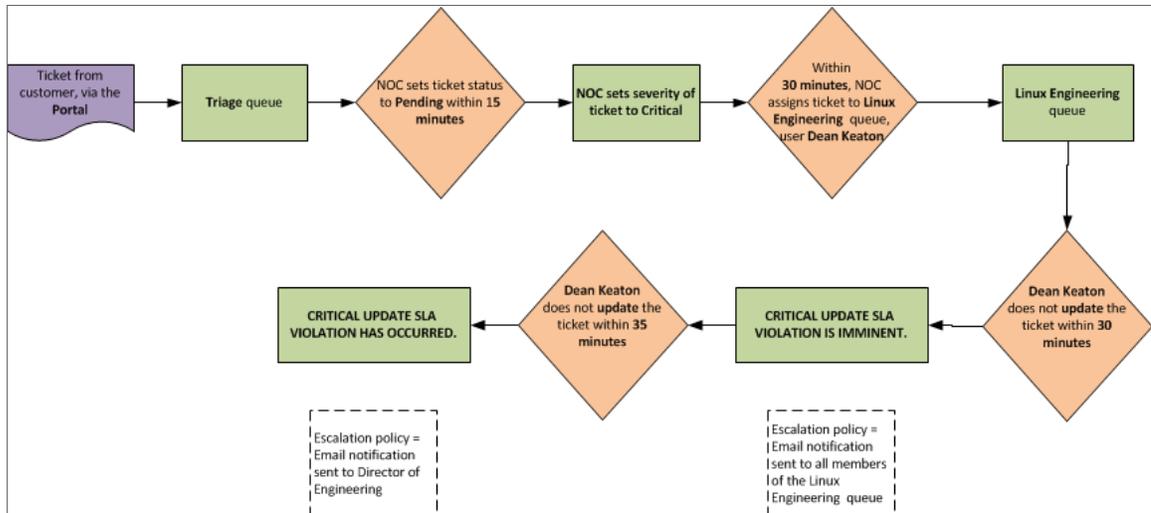
Critical Ticket was Not Updated

1. A customer creates a ticket through the ScienceLogic Support Site.

2. After examining the ticket, the NOC staff determines that the ticket is **Critical**. NOC staff assigns the ticket to **Dean Keaton** in the **Linux Engineering** queue.

3. When the ticket is not updated 30 minutes after it is assigned to a user and queue (as per the SLA for critical tickets), SL1 sends the following email to each member of the Linux Engineering queue:

4. When the ticket is not updated after 35 minutes (as per the SLA for critical tickets), SL1 sends the following email to the Director of Engineering:

From: EM7 Event Notifier [mailto:rtt@patch-aio.qa.sciencelogic.local]
Sent: Wednesday, April 8, 2015 10:48 PM
To: Roger Kint
Subject: TICKET ESCALATED: #8985 | Can't access my web server | 2015-04-08 22:06:14 | 2015-04-08 22:12:32

DESCRIPTION: Can't access my web server

CREATED ON: 2015-04-08 22:06:14

LAST UPDATED AT: 2015-04-08 22:12:32

ESCALATED BY POLICY: CRITICAL UPDATE SLA VIOLATION HAS OCCURRED
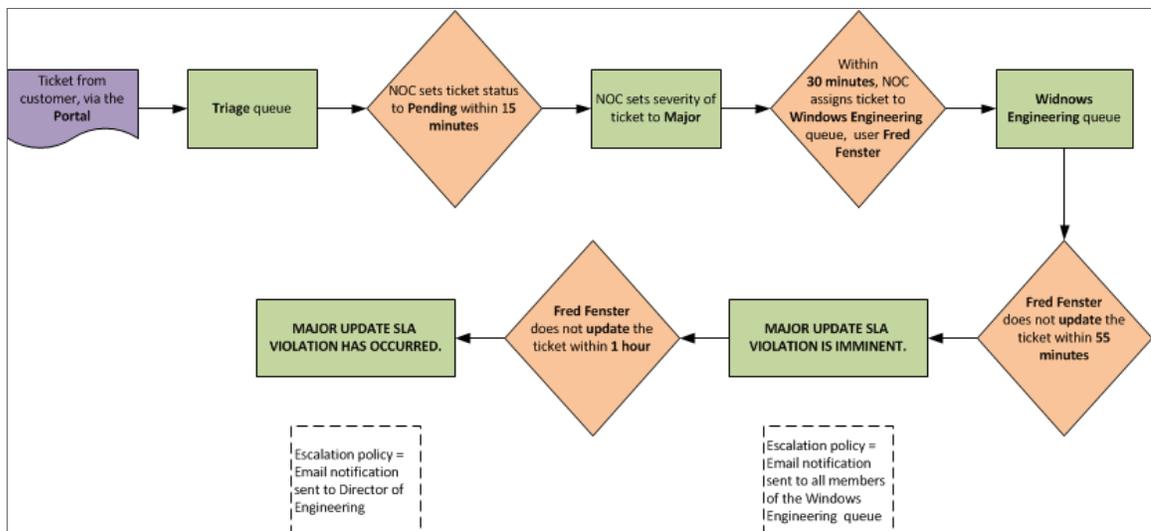
TICKET STATE: PENDING

TICKET QUEUE: Linux Engineering

CRITICAL UPDATE SLA VIOLATION HAS OCCURRED.

http://ap.server.url//em7/index.em7?exec=ticket_management&pop_modal=1&q_type=tid&q_val=16986&q_status=0.1.2&q_arg=8985
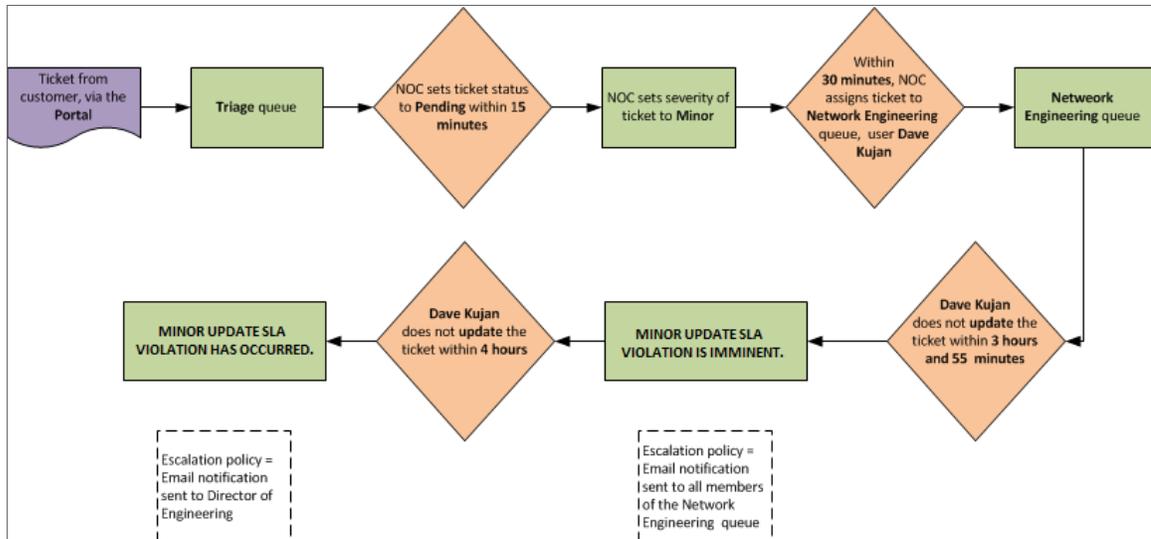
Major Ticket was Not Updated

1. A customer creates a ticket through the ScienceLogic Support Site.
2. After examining the ticket, the NOC staff determines that the ticket is **Major**. NOC staff assigns the ticket to **Fred Fenster** in the **Windows Engineering** queue.

3. When the ticket is not updated 55 minutes after it is assigned to a user and queue (as per the SLA for major tickets), SL1 sends a warning email to each member of the Linux Engineering queue. The email states that an SLA violation is imminent.

4. When the ticket is not updated after one hour (as per the SLA for major tickets), SL1 sends an email to the Director of Engineering. The email states that an SLA violation has occurred.

Minor Ticket was Not Updated

1. A customer creates a ticket through the ScienceLogic Support Site.

2. After examining the ticket, the NOC staff determines that the ticket is **Minor**. NOC staff assigns the ticket to **Jeff Rabinn**, in the **Network Engineering** queue.

3. When the ticket is not updated 3 hours and 55 minutes after it is assigned to a user and queue (as per the SLA for minor tickets), SL1 sends a warning email to each member of the Network Engineering queue. The email states that an SLA violation is imminent.

4. When the ticket is not updated after four hours (as per the SLA for minor tickets), SL1 sends an email to the Director of Engineering. The email states that an SLA violation has occurred.

Chapter

9

Creating Dashboards

Overview

A *dashboard* is a page that displays one or more graphical reports, called *widgets*. Each widget displays in its own pane.

To add a widget to a dashboard, you select from a list of pre-defined widget definitions and then select the data and parameters to include in the graphical report. The customized widget is then displayed as a graph, chart, or table in a pane in the dashboard.

SL1 includes many pre-defined widgets that generate customizable reports on devices, monitored applications on devices, events, networking, systems, and tickets.

In this chapter, you can populate some example dashboards with pre-defined widgets for ticketing.

For details on using dashboards and widgets, see the **Dashboards** manual.

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:

NOC Dashboard

This example dashboard could be displayed in Kiosk mode, on a large screen in the NOC. This dashboard uses pre-defined widgets.

- *Ask EM7: Unresolved Tickets*. This widget displays all tickets in the Triage ticket queue (the ticket queue that customer tickets are sent to initially) that were created 15 minutes ago or more and still have an Open status. To acknowledge a new ticket, a member of the NOC staff must change the ticket status from Open to Pending.

- *Ticketing Summary*.This widget shows all tickets in the Triage queue, grouped by status (Open, Pending, Working, Resolved). Again, to acknowledge a new ticket, a member of the NOC staff must change the ticket status from Open to Pending.

Engineering Dashboard

This example dashboard could be displayed in Kiosk mode, on a large screen in the Engineering bullpen. This dashboard uses pre-defined widgets.

- *Ticketing Summary*. This widget displays all tickets assigned to the Engineering organization (which uses three queues: Linux Engineering, Network Engineering, and Windows Engineering) and displays the number of tickets of each status.

- *Ask EM7: Unresolved Tickets*. This widget displays all tickets that have a severity of Critical and have not been updated within the 30-minute timespan, as required by the SLA. The table displays the ticket description, ticket queue, and assigned user for each ticket in the table.

Chapter

10

Additional Features

Overview

This chapter provides a brief overview of additional features in SL1 that can help you with incident management and workflow.

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:

Parent & Child Tickets

SL1 allows you to align tickets in *parent-child* relationships. You can create parent-child relationships when multiple tickets exist for a single issue, or if multiple tickets are related or interdependent. Keep in mind when creating parent-child relationships that:

- When the parent ticket is resolved, all children tickets are automatically resolved.

- Moving the parent ticket to another queue has no effect on the children tickets.

- Changing the severity of the parent ticket has no effect on the children tickets.

- Except for "Resolved," changing the status of the parent ticket has no effect upon the children tickets.

- Likewise, changing the queue, severity, or status of a child ticket has no effect upon the parent ticket.

For details on parent-child relationships, see the manual on *Ticketing*.

Multiple Events Aligned with a Single Ticket

SL1 allows you to associate an existing ticket with an event, even if the ticket was not originally created from an event. This is helpful when you want to automatically clear an event when a ticket has been resolved. You can also change the event associated with an existing ticket.

If a ticket addresses multiple events, you might find it helpful to align the ticket with multiple events. When the ticket is resolved, SL1 can automatically clear the selected event or events.

For details on aligning events and tickets, see the manual on *Ticketing*.

Chargeback

SL1 includes a tool that allows you to align a ticket with a product or service and then track the hours worked on a ticket. The combination of product or service plus the number of hours worked make up a *chargeback service*.

To view a list of product or service offerings, see the **Product Catalog** page (Registry > Business Services > Product Catalog). When you align a chargeback service with a ticket, SL1 automatically adds a note to the Notes & Attachments pane of the ticket.

You can also generate a Quick Report on chargeback services for each organization (Reports > Create Report > Quick Report > Ticket Billing). You can use this Quick Report to create a bill for each organization.

For details on chargeback services, see the manual on *Ticketing*.

For details on products and services, see the manual on *Business Services*.

For more details on the Ticket Billing report, see the manual on *Reports*.

Watchers

By default, SL1 automatically generates an email to the ticket creator and ticket assignee when:

- A ticket is created
- A ticket is assigned to a user
- A ticket is updated

You can also assign a *watcher* to the ticket. A ticket watcher is a user (in addition to the ticket's creator or assignee) who receives email updates about the ticket. If a watcher is added to a ticket, SL1 automatically sends the watcher emails when the ticket is created, assigned to another user, or changes status.

For details on watchers, see the manual on ***Ticketing***.

Scheduled Tickets

Scheduled tickets, also called *recurring tickets*, are tickets that are automatically generated at regular intervals. For example, recurring tickets can be defined for daily, monthly, or weekly maintenance tasks. Users can then use all the ticket tools and reports in SL1 to track and monitor these recurring tasks.

For details on creating and managing scheduled tickets, see the manual on ***Ticketing***.

Custom States

A *custom ticket state* is an additional ticket parameter. The definition of a ticket state includes logic that you can use to control workflow.

Using a custom ticket state, you can specify that tickets with the custom state always have a specified status and ticket queue. You can also specify that tickets with a custom state can be moved only to specified ticket queues and can be changed only to specified custom states.

For details on custom states, see the manual on ***Ticketing***.

Ticket History

The **Ticket Editor** page for each ticket includes a Logs tab that leads to the **Ticket Logs** page. The **Ticket Logs** page displays a history of the selected ticket. Each change to the ticket, from its creation to the current time, is displayed in a table in the **Ticket Logs** page. The table lists these changes chronologically, with the oldest first.

For details on ticket logs, see the manual on ***Ticketing***.

Run Book Automation

Run Book Automation is a powerful tool that allows you to define automatic actions that SL1 performs in response to events and additional event conditions.

Using Run Book Automation, you can have SL1 automatically send emails, create a new ticket, update an existing ticket, or run a custom Python script (among other actions). You can use Run Book Automation to automate your workflow and ensure uniformity.

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

Select Objects and Form Fields

You can use *Select Objects* to customize the entries that appear in drop-down lists throughout SL1. You can use Select Objects to customize the ticketing interface and other interfaces in your workflow.

You can use *Form Fields* to add custom fields and custom tabbed pages. You can use Form Fields to customize the ticketing interface and other interfaces in your workflow.

For details on Select Objects and Form Fields, see the manual on **Customizing User Experience**.

Appendix

A

Data for Escalation Policies

Overview

The *section on escalation policies* explained how to create a single escalation policy. This appendix includes the data for the remaining 33 escalation policies for Super Service Provider.

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:

Escalation Policies for Member of NOC Organization

From the *section on escalation policies*, perform steps 2- 5 for each of the remaining three escalation policies for the NOC organization. Use the values in the table below. If a field is not specified in the table below, accept the default value for the field.

For Ticket Queue	Policy Name	State	Ticket Status	Ticket Severity	Age Type	Minutes	Hours	Days	User Action	Notify Action	Members	Add Message
Triage	NEW ACKNOWLE DGMENT SLA VIOLATION HAS OCCURRED	Enabled	When ticket state is open	and severity is >="Sev 5/Heal thy"	and ticket create age is	15	None	None	and ticket is not updated	and notify select ed queue memb ers	Mill, Griffin	NEW ACKNOWLED GMENT SLA VIOLATION HAS OCCURRED.
Triage	NEW ASSIGNMENT SLA VIOLATION IMMINENT	Enabled	When ticket state is pending	and severity is >="Sev 5/Heal thy"	and ticket create age is	25	None	None	and ticket is not assigned	and notify select ed queue memb ers	All Queue Memb ers	NEW ASSIGNMENT SLA VIOLATION IMMINENT. Assign ticket immediately.
Triage	NEW ASSIGNMENT SLA VIOLATION HAS OCCURRED	Enabled	When ticket state is pending	and severity is >="Sev 5/Heal thy"	and ticket create age is	30	None	None	and ticket is not assigned	and notify select ed queue memb ers	Mill, Griffin	NEW ASSIGNMENT SLA VIOLATION HAS OCCURRED.

Escalation Policies for Linux Engineering Ticket Queue

From the *section on escalation policies*, perform steps 2- 5 for each of the remaining ten escalation policies for the Linux Engineering ticket queue. Use the values in the table below. If a field is not specified in the table below, accept the default value for the field.

For Ticket Queue	Policy Name	State	Ticket Status	Ticket Severity	Age Type	Minutes	Hours	Days	User Action	Notify Action	Members	Add Message
Linux Engineering	CRITICAL UPDATE SLA VIOLATION IS IMMINENT	Enabled	When ticket state is pending	and severity is >="Sev 1/Critical"	and ticket's last update age is	30	None	None	and ticket is not updated	and notify selected queue members	Dean Keaton, Roger Kint	CRITICAL UPDATE SLA VIOLATION IS IMMINENT. Attend to ticket immediately.
Linux Engineering	CRITICAL UPDATE SLA VIOLATION HAS OCCURRED	Enabled	When ticket state is pending	and severity is >="Sev 1/Critical"	and ticket's last update age is	35	None	None	and ticket is not updated	and notify selected queue members	Roger Kint	CRITICAL UPDATE SLA VIOLATION HAS OCCURRED
Linux Engineering	MAJOR UPDATE SLA VIOLATION IS IMMINENT	Enabled	When ticket state is pending	and severity is >="Sev 2/Major"	and ticket's last update age is	55	None	None	and ticket is not updated	and notify selected queue members	Dean Keaton, Roger Kint	MAJOR UPDATE SLA VIOLATION IS IMMINENT. Attend to ticket immediately.
Linux Engineering	MAJOR UPDATE SLA VIOLATION HAS OCCURRED	Enabled	When ticket state is pending	and severity is >="Sev 2/Major"	and ticket's last update age is	None	1	None	and ticket is not updated	and notify selected queue members	Roger Kint	MAJOR UPDATE SLA VIOLATION HAS OCCURRED
Linux Engineering	MINOR UPDATE SLA VIOLATION IS IMMINENT	Enabled	When ticket state is pending	and severity is >="Sev 3/Minor"	and ticket's last update age is	55	3	None	and ticket is not updated	and notify selected queue members	Dean Keaton, Roger Kint	MINOR UPDATE SLA VIOLATION IS IMMINENT. Attend to ticket immediately.

For Ticket Queue	Policy Name	State	Ticket Status	Ticket Severity	Age Type	Minutes	Hours	Days	User Action	Notify Action	Members	Add Message
Linux Engineering	MINOR UPDATE SLA VIOLATION HAS OCCURRED	Enabled	When ticket state is pending	and severity is >="Sev 3/Minor"	and ticket's last update age is	None	4	None	and ticket is not updated	and notify selected queue members	Roger Kint	MINOR UPDATE SLA VIOLATION HAS OCCURRED
Linux Engineering	NOTICE UPDATE SLA VIOLATION IS IMMINENT	Enabled	When ticket state is pending	and severity is >="Sev 4/Notice"	and ticket's last update age is	55	23	None	and ticket is not updated	and notify selected queue members	Dean Keaton, Roger Kint	NOTICE UPDATE SLA VIOLATION IS IMMINENT. Attend to ticket immediately.
Linux Engineering	NOTICE UPDATE SLA VIOLATION HAS OCCURRED	Enabled	When ticket state is pending	and severity is >="Sev 4/Notice"	and ticket's last update age is	None	None	1	and ticket is not updated	and notify selected queue members	Roger Kint	NOTICE UPDATE SLA VIOLATION HAS OCCURRED
Linux Engineering	HEALTHY UPDATE SLA VIOLATION IS IMMINENT	Enabled	When ticket state is pending	and severity is >="Sev 5/Healthy"	and ticket's last update age is	55	23	2	and ticket is not updated	and notify selected queue members	Dean Keaton, Roger Kint	HEALTHY UPDATE SLA VIOLATION IS IMMINENT. Attend to ticket immediately.
Linux Engineering	HEALTHY UPDATE SLA VIOLATION HAS OCCURRED	Enabled	When ticket state is pending	and severity is >="Sev 5/Healthy"	and ticket's last update age is	None	None	3	and ticket is not updated	and notify selected queue members	Roger Kint	HEALTHY UPDATE SLA VIOLATION HAS OCCURRED

Escalation Policies for Network Engineering Ticket Queue

From the *section on escalation policies*, perform steps 2- 5 for each of the remaining ten escalation policies for the Network Engineering ticket queue. Use the values in the table below. If a field is not specified in the table below, accept the default value for the field.

For Ticket Queue	Policy Name	State	Ticket Status	Ticket Severity	Age Type	Minutes	Hours	Days	User Action	Notify Action	Members	Add Message
Network Engineering	CRITICAL UPDATE SLA VIOLATION IS IMMINENT	Enabled	When ticket state is pending	and severity is >="Sev 1/Critical"	and ticket's last update age is	30	None	None	and ticket is not updated	and notify selected queue members	Roger Kint, Dave Kahane, Jeff Rabin	CRITICAL UPDATE SLA VIOLATION IS IMMINENT. Attend to ticket immediately.
Network Engineering	CRITICAL UPDATE SLA VIOLATION HAS OCCURRED	Enabled	When ticket state is pending	and severity is >="Sev 1/Critical"	and ticket's last update age is	35	None	None	and ticket is not updated	and notify selected queue members	Roger Kint	CRITICAL UPDATE SLA VIOLATION HAS OCCURRED
Network Engineering	MAJOR UPDATE SLA VIOLATION IS IMMINENT	Enabled	When ticket state is pending	and severity is >="Sev 2/Major"	and ticket's last update age is	55	None	None	and ticket is not updated	and notify selected queue members	Roger Kint, Dave Kahane, Jeff Rabin	MAJOR UPDATE SLA VIOLATION IS IMMINENT. Attend to ticket immediately.
Network Engineering	MAJOR UPDATE SLA VIOLATION HAS OCCURRED	Enabled	When ticket state is pending	and severity is >="Sev 2/Major"	and ticket's last update age is	None	1	None	and ticket is not updated	and notify selected queue members	Roger Kint	MAJOR UPDATE SLA VIOLATION HAS OCCURRED

For Ticket Queue	Policy Name	State	Ticket Status	Ticket Severity	Age Type	Minutes	Hours	Days	User Action	Notify Action	Members	Add Message
Network Engineering	MINOR UPDATE SLA VIOLATION IS IMMINENT	Enabled	When ticket state is pending	and severity is >="Sev 3/Minor"	and ticket's last update age is	55	3	None	and ticket is not updated	and notify selected queue members	Roger Kint, Dave Kahane, Jeff Rabin	MINOR UPDATE SLA VIOLATION IS IMMINENT. Attend to ticket immediately.
Network Engineering	MINOR UPDATE SLA VIOLATION HAS OCCURRED	Enabled	When ticket state is pending	and severity is >="Sev 3/Minor"	and ticket's last update age is	None	4	None	and ticket is not updated	and notify selected queue members	Roger Kint	MINOR UPDATE SLA VIOLATION HAS OCCURRED
Network Engineering	NOTICE UPDATE SLA VIOLATION IS IMMINENT	Enabled	When ticket state is pending	and severity is >="Sev 4/Notice"	and ticket's last update age is	55	23	None	and ticket is not updated	and notify selected queue members	Roger Kint, Dave Kahane, Jeff Rabin	NOTICE UPDATE SLA VIOLATION IS IMMINENT. Attend to ticket immediately.
Network Engineering	NOTICE UPDATE SLA VIOLATION HAS OCCURRED	Enabled	When ticket state is pending	and severity is >="Sev 4/Notice"	and ticket's last update age is	None	None	1	and ticket is not updated	and notify selected queue members	Roger Kint	NOTICE UPDATE SLA VIOLATION HAS OCCURRED
Network Engineering	HEALTHY UPDATE SLA VIOLATION IS IMMINENT	Enabled	When ticket state is pending	and severity is >="Sev 5/Healthy"	and ticket's last update age is	55	23	2	and ticket is not updated	and notify selected queue members	Roger Kint, Dave Kahane, Jeff Rabin	HEALTHY UPDATE SLA VIOLATION IS IMMINENT. Attend to ticket immediately.

For Ticket Queue	Policy Name	State	Ticket Status	Ticket Severity	Age Type	Minutes	Hours	Days	User Action	Notify Action	Members	Add Message
Network Engineering	HEALTHY UPDATE SLA VIOLATION HAS OCCURRED	Enabled	When ticket state is pending	and severity is >="Sev 5/Healthy"	and ticket's last update age is	None	None	3	and ticket is not updated	and notify selected queue members	Roger Kint	HEALTHY UPDATE SLA VIOLATION HAS OCCURRED

Escalation Policies for Windows Engineering Ticket Queue

From the *section on escalation policies*, perform steps 2- 5 for each of the remaining ten escalation policies for the Windows Engineering ticket queue. Use the values in the table below. If a field is not specified in the table below, accept the default value for the field.

For Ticket Queue	Policy Name	State	Ticket Status	Ticket Severity	Age Type	Minutes	Hours	Days	User Action	Notify Action	Members	Add Message
Windows Engineering	CRITICAL UPDATE SLA VIOLATION IS IMMINENT	Enabled	When ticket state is pending	and severity is >="Sev 1/Critical"	and ticket's last update age is	30	None	None	and ticket is not updated	and notify selected queue members	Fred Fenster, Roger Kint	CRITICAL UPDATE SLA VIOLATION IS IMMINENT. Attend to ticket immediately.
Windows Engineering	CRITICAL UPDATE SLA VIOLATION HAS OCCURRED	Enabled	When ticket state is pending	and severity is >="Sev 1/Critical"	and ticket's last update age is	35	None	None	and ticket is not updated	and notify selected queue members	Roger Kint	CRITICAL UPDATE SLA VIOLATION HAS OCCURRED
Windows Engineering	MAJOR UPDATE SLA VIOLATION IS IMMINENT	Enabled	When ticket state is pending	and severity is >="Sev 2/Major"	and ticket's last update age is	55	None	None	and ticket is not updated	and notify selected queue members	Fred Fenster, Roger Kint	MAJOR UPDATE SLA VIOLATION IS IMMINENT. Attend to ticket immediately.

For Ticket Queue	Policy Name	State	Ticket Status	Ticket Severity	Age Type	Minutes	Hours	Days	User Action	Notify Action	Members	Add Message
Windows Engineering	MAJOR UPDATE SLA VIOLATION HAS OCCURRED	Enabled	When ticket state is pending	and severity is >="Sev 2/Major"	and ticket's last update age is	None	1	None	and ticket is not updated	and notify selected queue members	Roger Kint	MAJOR UPDATE SLA VIOLATION HAS OCCURRED
Windows Engineering	MINOR UPDATE SLA VIOLATION IS IMMINENT	Enabled	When ticket state is pending	and severity is >="Sev 3/Minor"	and ticket's last update age is	55	3	None	and ticket is not updated	and notify selected queue members	Fred Fenster, Roger Kint	MINOR UPDATE SLA VIOLATION IS IMMINENT. Attend to ticket immediately.
Windows Engineering	MINOR UPDATE SLA VIOLATION HAS OCCURRED	Enabled	When ticket state is pending	and severity is >="Sev 3/Minor"	and ticket's last update age is	None	4	None	and ticket is not updated	and notify selected queue members	Roger Kint	MINOR UPDATE SLA VIOLATION HAS OCCURRED
Windows Engineering	NOTICE UPDATE SLA VIOLATION IS IMMINENT	Enabled	When ticket state is pending	and severity is >="Sev 4/Notice"	and ticket's last update age is	55	23	None	and ticket is not updated	and notify selected queue members	Fred Fenster, Roger Kint	NOTICE UPDATE SLA VIOLATION IS IMMINENT. Attend to ticket immediately.
Windows Engineering	NOTICE UPDATE SLA VIOLATION HAS OCCURRED	Enabled	When ticket state is pending	and severity is >="Sev 4/Notice"	and ticket's last update age is	None	None	1	and ticket is not updated	and notify selected queue members	Roger Kint	NOTICE UPDATE SLA VIOLATION HAS OCCURRED

For Ticket Queue	Policy Name	State	Ticket Status	Ticket Severity	Age Type	Minutes	Hours	Days	User Action	Notify Action	Members	Add Message
Windows Engineering	HEALTHY UPDATE SLA VIOLATION IS IMMINENT	Enabled	When ticket state is pending	and severity is >="Sev 5/Healthy"	and ticket's last update age is	55	23	2	and ticket is not updated	and notify selected queue members	Fred Fenster, Roger Kint	HEALTHY UPDATE SLA VIOLATION IS IMMINENT. Attend to ticket immediately.
Windows Engineering	HEALTHY UPDATE SLA VIOLATION HAS OCCURRED	Enabled	When ticket state is pending	and severity is >="Sev 5/Healthy"	and ticket's last update age is	None	None	3	and ticket is not updated	and notify selected queue members	Roger Kint	HEALTHY UPDATE SLA VIOLATION HAS OCCURRED

ScienceLogic

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

International: +1-703-354-1010