Organizations and Users

SL1 version 12.2.1 (Document revision 2)

Table of Contents

Chapter 1

Introduction to Organizations and Users

Overview

This chapter explains organizations and their relationships to elements, users, and user policies.

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 Element?

An ***element*** is an object that can be managed by SL1. SL1 can create events about these objects. Users can create tickets about these objects. In SL1, elements include:

- Asset records
- Devices and their components, including network interfaces
- IP networks
- Network Interfaces
- Organizations
- User Accounts
- Vendor records

What is an Organization?

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

The basic characteristics of an organization are:

- A unique name (required).
- Users who are members of the organization.
- Elements (for example, devices) associated with the organization.

Organizations can be defined by geographic areas, departments, types of devices, or any structure that works best for your needs. For example, for a business with multiple locations, an administrator might create organizations named Boston, New York, and DC. Another administrator might create organizations named for departments, like Finance, Sales/Marketing, and Engineering.

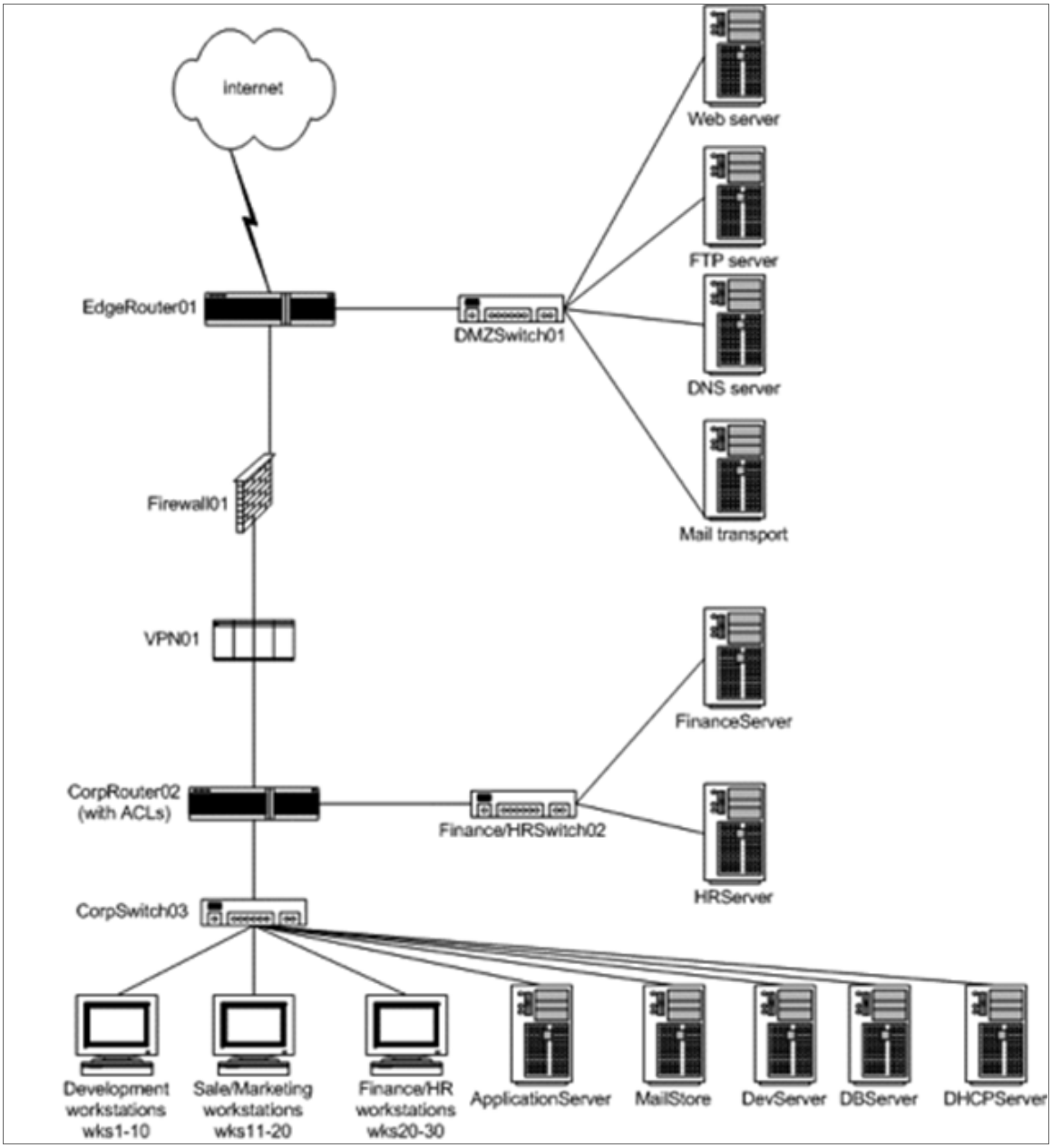
Organizations and Their Relationships

Organizations are the containers for user accounts and elements (and the associated policies and sub-elements). The following sections describe the relationships between organizations and elements and organizations and user accounts.

Organizations and Elements

After one or more organizations have been defined, administrators can associate elements with each organization.

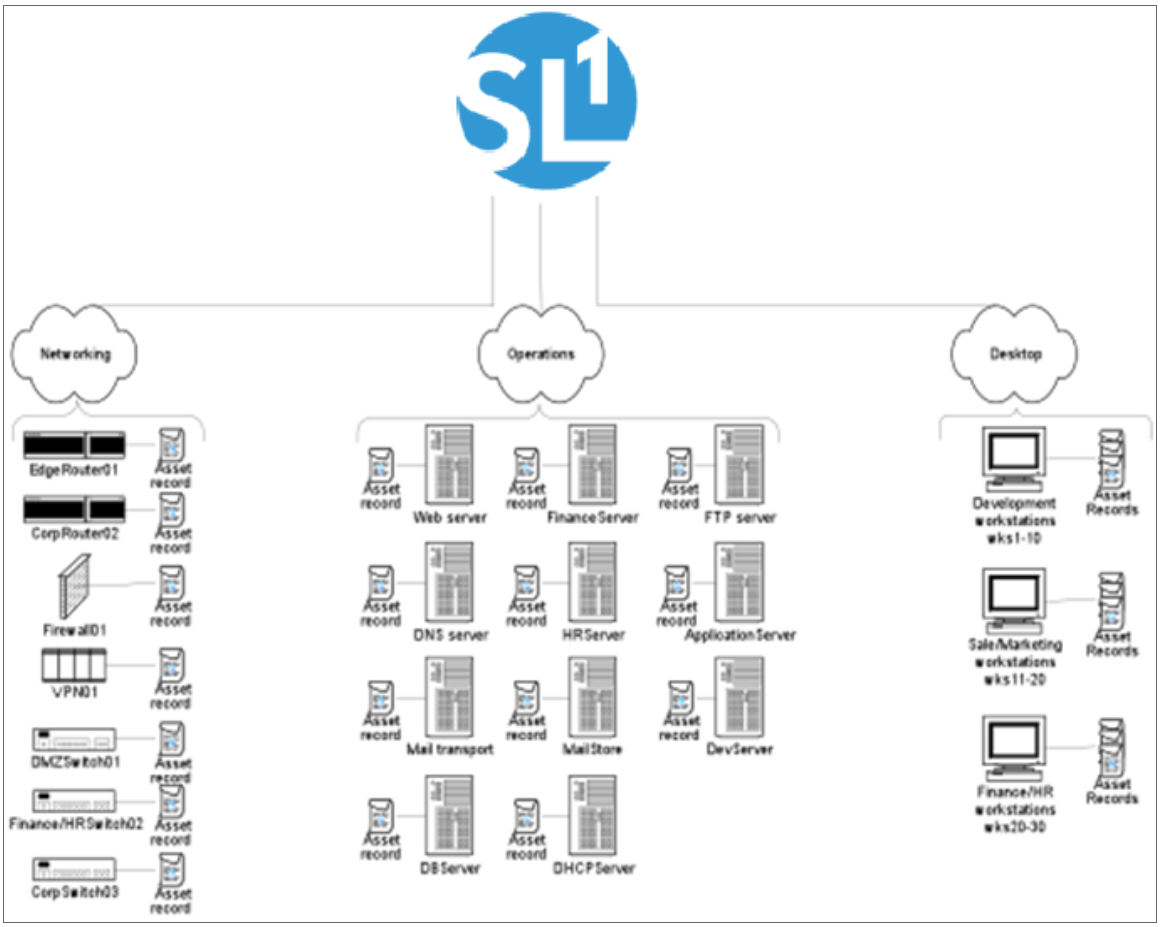
Suppose your network looked like this very simplified example:



Now suppose that the administrator had defined the following organizations:

- Network
- Operations
- Desktop

The administrator might assign elements like this:



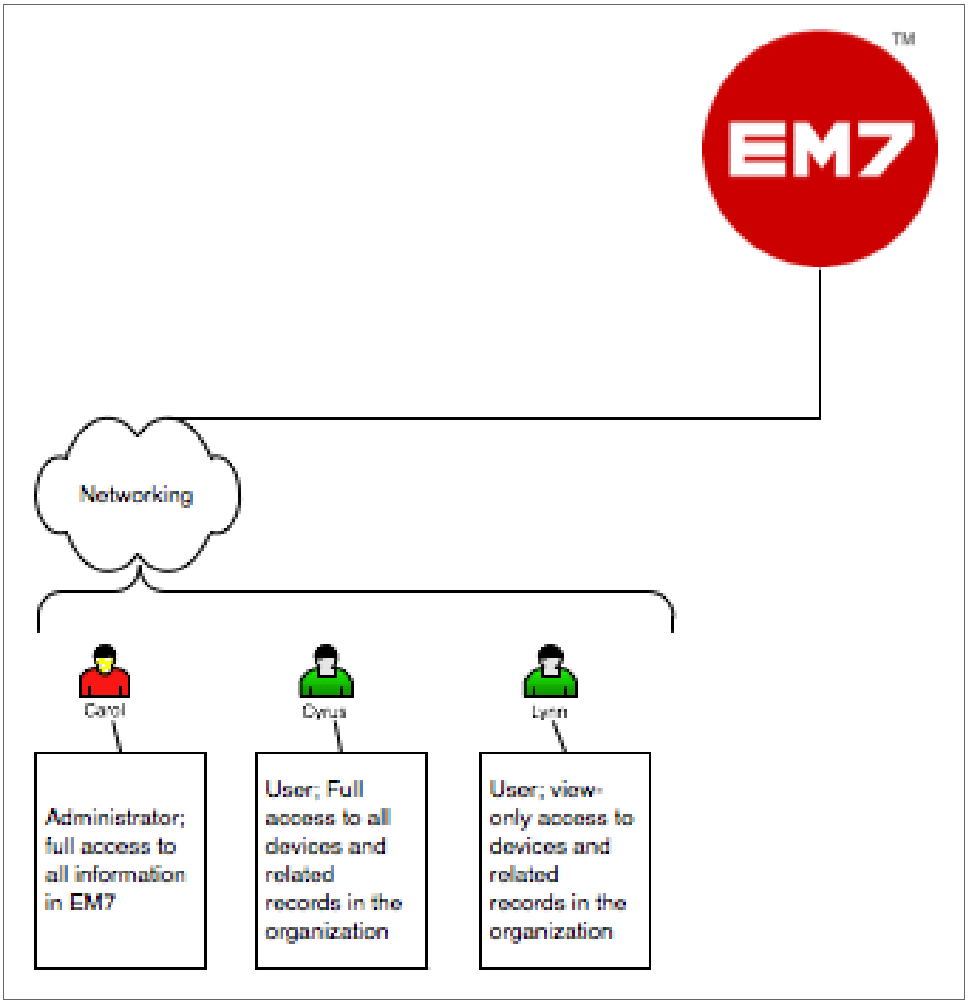
In this example:

- The Networking organization contains two routers, a firewall, a VPN device, three switches, and an asset record for each piece of hardware. All the network interfaces on the routers, firewall, VPN device, and switches also belong to the Networking organization.
- The Operations organization contains all 11 servers in the network, and an asset record for each piece of hardware. All the network interfaces on the eleven servers also belong to the Operations organization.
- The Desktop organization contains all 30 desktops in the network, and an asset record for each piece of hardware. All the network interfaces on the 30 desktops also belong to the Desktop organization.

Organizations and Users

Administrators can define user accounts and associate each user with a primary organization. For each organization, the administrator must determine which team members require access to SL1 and what access levels to assign to each team member.

Specifically, the administrator defines and adds users to organizations. For example, for the Networking organization, the administrator could define users like this:



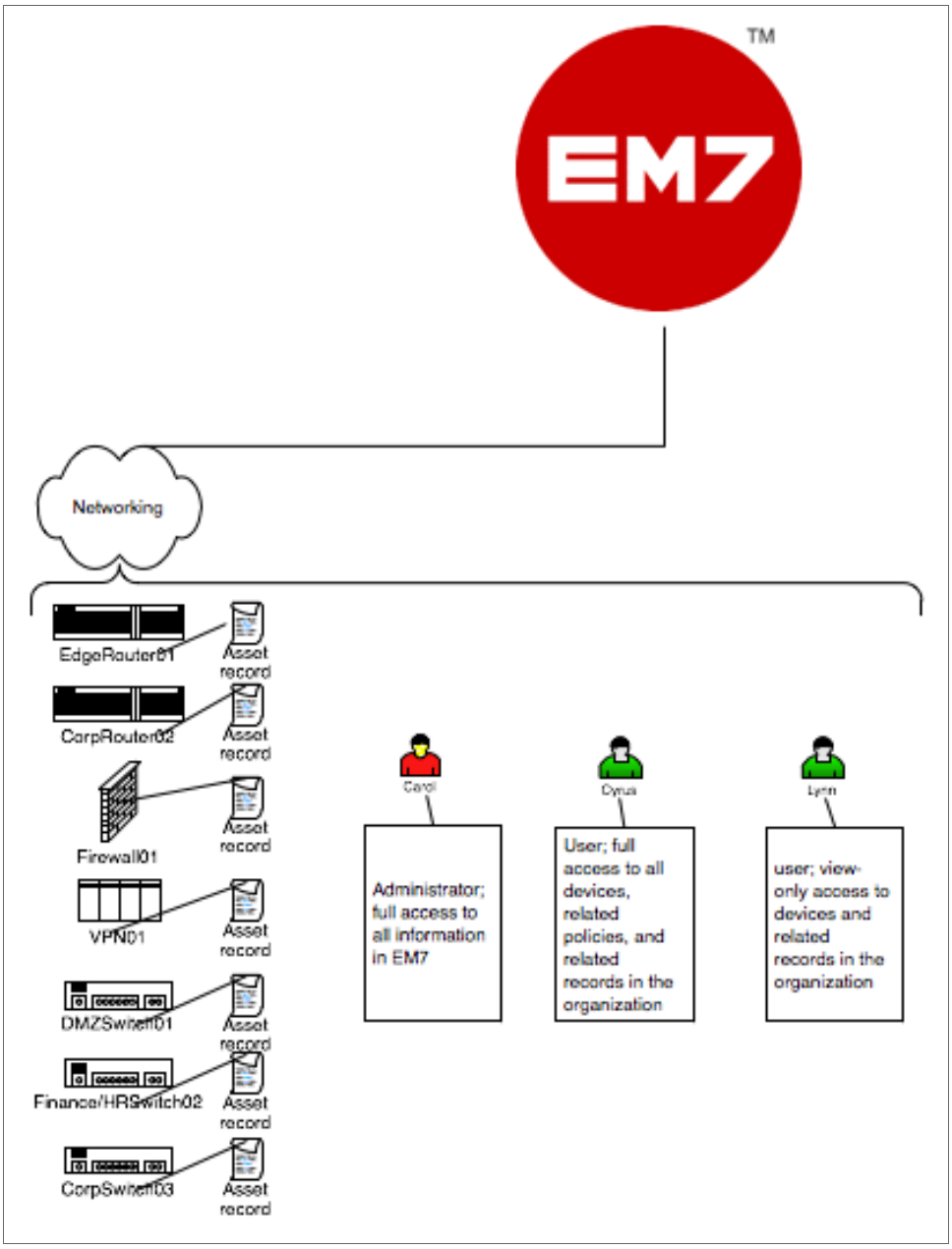
In this example:

- The Networking organization contains three users: Carol, Cyrus, and Lynn.
- Carol is the Director for Network Administration and is defined as an Administrator. She has unlimited access to all information in SL1.
- Cyrus and Lynn are defined as Users. Their access in SL1 is limited by the Access Keys associated with their accounts.
- Cyrus is the Manager for Network Administration and has full access to all devices and related records in the Networking organization. Cyrus can view information in SL1 to diagnose problems and also create and edit policies for the devices and components in his organization.
- Lynn is a Network Administrator and has read-only access to all devices and related records in the Networking organization. Lynn can view information in SL1 to diagnose network problems, but cannot make changes in SL1.

NOTE: The process of assigning users to organizations will be described in detail in this manual.

Example Organization and Its Relationships

Here's an illustration of the example organization, Networking, with both users and elements assigned:



Organizations and Their Policies and Reports

Some elements, policies, and reports are associated with an organization but are not associated with a device. These elements, policies, and reports can be accessed through the organization tools (they can also be accessed from the **[Registry]** tab and other places in SL1):

- User accounts
- Templates for creating customized access rights and access authorization
- Policies for bandwidth billing
- Product Subscription

Chapter 2

Creating and Editing Organizations

Overview

This chapter will show you how to create and edit an organization in SL1, and also how to view and filter a list of organizations.

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:

Before Deployment

Before deployment, an administrator must determine:

- How to best group devices in the network.
- Which organization to place each device in, so that device information is visible to those who need it and protected from other users.
- Which team members require access to SL1.
- What access levels to assign to each team member.
- Which organizations to place each team member in, so that each team member will have access to required device information.
- Remember that each discovered device and each user is associated with an organization.

Users with an account of type "administrator" have access to all pages and actions in SL1.

Users with an account of type "user" have custom-defined access levels. An administrator defines and assigns Access Keys to control the access level for each account of type "user". To learn more about Access Keys and how they affect users, see the ***Access Permissions*** manual.

Regardless of access keys, accounts of type "user" can access only pages and actions associated with their organization. For example:

- Suppose your organization includes three regional offices. Suppose you define three organizations: Northeast, Headquarters, and West Coast.
- Suppose each organization includes the hardware at the corresponding office.
- Now suppose the account "JohnDoe" is of type "user" and is a member of the organization "West Coast". User JohnDoe would be able to view and act upon only devices that are included in the organization "West Coast". User JohnDoe would not be able to view or act upon the hardware at the other offices.
- For this reasons, SL1 allows you to assign each user a primary organization and an optional additional organization.
- Now suppose that user "JohnDoe" needs to view the status of a device at headquarters. If you add a secondary organization to JohnDoe's account information, that user will now be able to view and act upon all the devices in the "Headquarters" organization.

> **NOTE**: You can use Access Keys to further limit the access of each user, even within his/her own organization.

Organizations also affect credentials. Credentials are access permissions that allow SL1 to retrieve information from external hardware and software. To support multi-tenancy, SL1 allows credentials to be aligned with organizations.

- For each credential that is aligned with an organization, only administrators and users who are members of the aligned organization will be able to see the credential in the **Credential Management** page.
- In SL1, in any field or column that displays the name of the credential, users who are not members of the aligned organization will not see the credential name. Instead, these users will see either a dash character (-) or the text "Restricted Credential".

In SL1, in any list from which users can select a credential, users who are not members of the aligned organization will not see the credential as an entry in the list.

To learn more about credentials, see the manual ***Discovery and Credentials***.

The System Organization

SL1 automatically creates a default organization, called System. This organization has the ID number "0" (zero). The System organization has some behavior that differs from user-defined organizations:

- If you do not specify an organization when creating a user account, the new account is assigned to the System organization.
- If you do not specify an organization when performing discovery, all devices (and their components), interfaces, and IP networks are assigned to the System organization.
- You cannot delete the system organization.
- You cannot bulk-edit the system organization with entries in the ***Select Actions*** menu.

Viewing the List of Organizations

The **Organizational Account Administration** page displays a list of all existing organizations in SL1. From the **Organizational Account Administration** page, you can view information about organizations, edit the properties of existing organizations, create new organizations, and generate reports for each organization, among other tasks.

To view a list of existing organizations:

1. Go to **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. The **Organizational Account Administration** page appears. This page displays information about each organization you are allowed to view.
3. For each organization, the **Organizational Account Administration** page displays:

    - ***Organization Name***. Name of the organization.
    - ***City***. City specified in the **Organization Properties** page.
    - ***State***. State specified in the **Organization Properties** page.
    - ***Contact***. First and last name of the contact specified in the **Organization Properties** page.
    - ***Phone***. Organization's main phone number specified in the **Organization Properties** page.
    - ***Email***. Email address for the organization specified in the **Organization Properties** page. Clicking the email icon () opens a new message in the local email client, with the organization's address in the ***To*** field.
    - ***Users***. Specifies the number of user accounts associated with the organization. Clicking the person icon () in this column leads to the **Finder** page, where you can view a list of all the user accounts in the organization.
    - ***Devices***. Specifies the number of devices associated with the organization. Clicking the devices icon () leads to the **Finder** page, where you can view a list of all the devices in the organization.

- ***Assets***. Specifies the number of asset records associated with the organization. Clicking the asset icon () leads to the **Finder** page, where you can view a list of all the asset records in the organization.
- ***Events***. Specifies the number of events associated with the organization. Clicking the events icon () leads to the **Finder** page, where you can view a list of all the user accounts in the organization.
- ***ID***. Unique numeric ID, assigned to each organization by SL1.
- ***Edited By***. User name of the user who created or last edited the organization.
- ***Last Edited***. Date and time the organization was created or last edited.

Filtering the List of Organizations

The following describes each filter on the **Organizational Account Administration** page:

- ***Organization Name***. You can enter a regular expression, including special characters, and the **Organizational Account Administration** page will display only organizations that have a matching organization name.
- ***City***. You can enter a regular expression, including special characters, and the **Organizational Account Administration** page will display only organizations that have a city.
- ***State***. You can enter a regular expression, including special characters, and the **Organizational Account Administration** page will display only organizations that have a matching state.
- ***Contact***. You can enter a regular expression, including special characters, and the **Organizational Account Administration** page will display only organizations that have a matching contact.
- ***Phone***. You can enter a regular expression, including special characters, and the **Organizational Account Administration** page will display only organizations that have a matching phone number.
- ***Email***. You can enter a regular expression, including special characters, and the **Organizational Account Administration** page will display only organizations that have a matching email address.
- ***Users***. You can enter a regular expression, including special characters, and the **Organizational Account Administration** page will display only organizations that have a matching number of users.
- ***Devices***. You can enter a regular expression, including special characters, and the **Organizational Account Administration** page will display only organizations that have a matching number of devices.
- ***Assets***. You can enter a regular expression, including special characters, and the **Organizational Account Administration** page will display only organizations that have a matching number of assets.
- ***Events***. You can enter a regular expression, including special characters, and the **Organizational Account Administration** page will display only organizations that have a matching number of events.
- ***ID***. You can enter a regular expression, including special characters, and the **Organizational Account Administration** page will display only organizations that have a matching organization ID.
- ***Edited By***. You can enter a regular expression, including special characters, and the **Organizational Account Administration** page will display only organizations that have a matching "edited by" value.
- ***Last Edited***. You can select from a list of time periods. The **Organizational Account Administration** page will display only organizations that have been edited within that time period.

Creating a New Organization

By default, SL1 includes a single organization, called System. To fully use the features of SL1, you must define organizations that suit your organization and business needs.

To create a new organization:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations) and click the **[Create]** button. The **Add Organizational Record** page appears.
2. On the **Add Organizational Record** page, supply values in each field:
    - ***Organization Name***. Name of the organization. Can be any combination of characters up to 128 characters in length. This field is required.
    - ***Street Address***. Street address of the organization. For easier viewing, ScienceLogic suggests that you limit the address to 5 lines, with up to 60 characters per line.
    - ***City***. City where the organization is located. Can be up to 64 characters in length.
    - ***State***. State where the organization is located. Select from the drop-down list.
    - ***Postal Code***. Zip code of the organization. Can be up to 15 characters in length.
    - ***Country***. Country where the organization is located. Select from the drop-down list.
    - ***Contact First Name***. First name of organization's contact. Can be up to 128 characters in length.
    - ***Contact Last Name***. Last name of organization's contact. Can be up to 64 characters in length.
    - ***Title***. Contact's title. Can be up to 64 characters in length.
    - ***Department***. Contact's department. Can be up to 64 characters in length.
    - ***Phone***. Business phone number for the organization. Can be up to 36 characters in length.
    - ***Email***. Organization's main email address. Can be up to 250 characters in length.
    - ***Billing ID***. Billing ID for the organization. Can be up to 24 characters in length.
    - ***CRM ID***. CRM ID for the organization. Can be up to 64 characters in length.
    - ***Email Notification Append Text***. The text entered in this field will appear at the bottom of all email messages sent from SL1 to members of this organization. This includes automated email messages and email messages that are sent manually either by clicking on an email icon or from the **Send Message** tab in the **Ticket Editor** page.

NOTE: On the **Behavior Settings** page (System > Settings > Behavior, if the field ***Automatic Ticketing Emails*** is set to *Disabled*, all assignees and watchers will not receive automatic email notifications about any tickets. By default, the field is set to *Enabled*.

3. Click the **[Save]** button to save the new organization. After saving the new organization, a new set of tabs appear in SL1 for the organization. These tabs allow you to further configure and manage the organization.

Editing an Existing Organization

You can edit the properties of an existing organization by accessing the **Organization Properties** page. The **Organization Properties** page includes the basic parameters of an organization such as organization name and address and contact information.

To access the **Organization Properties** page:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization you want to edit. Click its wrench icon ().
3. The **Organizational Summary** page appears. The **Organizational Summary** page displays read-only details about the organization and provides links to other pages associated with the organization.
4. To edit properties of the organization, click the **[Properties]** tab.
5. The **Organization Properties** page appears. In this page, you can edit one or more fields.

Organization Properties

The **Organization Properties** page contains the following fields:

- ***Organization Name***. Name of the organization. Can be any combination of characters up to 128 characters in length. This field is required.
- ***Street Address***. Street address of the organization. For easier viewing, ScienceLogic suggests that you limit the address to 5 lines, with up to 60 characters per line.
- ***City***. City where the organization is located. Can be up to 64 characters in length.
- ***State***. State where the organization is located. Select from the drop-down list.
- ***Postal Code***. Zip code of the organization. Can be up to 15 characters in length.
- ***Country***. Country where the organization is located. Select from the drop-down list.
- ***Contact First Name***. First name of organization contact. Can be up to 128 characters in length.
- ***Contact Last Name***. Last name of organization contact. Can be up to 64 characters in length.
- ***Title***. Contact's title. Can be up to 64 characters in length.
- ***Department***. Contact's department. Can be up to 64 characters in length.
- ***Phone***. Business phone number for the organization. Can be up to 36 characters in length.
- ***Fax Phone***. Fax number for the organization. Can be up to 36 characters in length.
- ***Toll Free***. Toll-free phone number for the organization. Can be up to 36 characters in length.
- ***Email***. Organization's main email address. Can be up to 250 characters in length.
- ***Billing ID***. Billing ID for organization. Can be up to 24 characters in length.
- ***CRM ID***. CRM ID for organization. Can be up to 64 characters in length.

- ***Email Notification Append Text***. The text entered in this field will appear at the bottom of all email messages sent from SL1 to members of this organization. This includes automated email messages and email messages that are sent manually either by clicking on an email icon or from the **Send Message** tab in the **Ticket Editor** page.
- ***Longitude***. Displays the longitude associated with the organization's address. To generate this field, click the **[Actions]** menu and then select ***Geolocate Coordinates***.
- ***Latitude***. Displays the latitude associated with the organization's address. To generate this field, click the **[Actions]** menu and then select ***Geolocate Coordinates***.
- ***Organizational Ticket Watchers***. You can select one or more users (in addition to the ticket's creator or assignee) who will be considered "watchers" for all tickets associated with the organization. Each organizational watcher will be notified when a ticket is created and aligned with the organization and when that ticket is assigned to a user or changes status. When that ticket is created, assigned, or updated, SL1 will automatically send email notifications to the list of watchers.

> **NOTE**: On the **Behavior Settings** page (System > Settings > Behavior, if the field ***Automatic Ticketing Emails*** is set to *Disabled*, all assignees and watchers will not receive automatic email notifications about any tickets. By default, the field is set to *Enabled*.

Critical Contact List

The **Critical Contact List** pane is useful when organization members must assign a task or contact a key team member.

A user appears in this pane if he/she was defined as a critical contact in the **Account Properties** page.

The **Critical Contact List** pane displays the following information about each critical contact:

- ***Name***. Name of person to contact.
- ***Role***. Description of the user's responsibilities in case of a critical situation. This description might differ from the user's actual title. For example, a contact's title might be Senior Engineer, but his/her role for the organization might be technical lead.
- ***Critical Contact***. Circumstance when person should be contacted. This description might differ from the user's department. For example, the user's department might be Operations, but his/her role for the organization might be Hardware Maintenance.
- ***Phone***. Person's phone number.
- ***Cell***. Person's cell phone number.
- ***Pager***. Person's pager number.
- ***Email***. Person's email address.
- ***Tools***. The following tools are available for each entry in the critical contact list:
    - *Manage User's Contact Information* (). Leads to the *Account Properties* page, where you can edit the person's contact information.

- *Send Email Message to this User* (). Opens an email client on the local desktop. The ***To*** field is populated with the email address of the selected user.

Product Usage List

The Product Usage List displays a list of SKUs associated with the organization. Usually, a SKU is associated with an organization because the organization is using that product or service.

To associate a SKU with the organization or change the list of SKUs associated with the organization, click the **[Actions]** menu and then select ***Product Catalog***. In the **Product Catalog** modal page, you can add and remove products from the organization.

For each product associated with the organization, the **Product Usage List** pane displays the following:

- ***SKU Class***. Description of the SKU. Can be up to 64 characters in length.
- ***SKU Number***. Numeric ID for the SKU. Can be up to 24 characters in length.
- ***SKU Name***. Name of the SKU. Can be up to 64 characters in length.
- ***Name***. The name of the element using the SKU. Clicking on the icon for the element leads to a page where you can view more information about the element.
- ***Type***. The type of element using the SKU. Choices are:
  - Organization
  - Device
  - Asset
  - Domain Name
  - Network
  - Interface
  - Other

Organizational Sub-Locations

If one or more alternate locations have already been defined for the Organization, the **Organizational Alternate Locations** pane appears at the bottom of the page.

To define an alternate location for an organization, click the **[Actions]** menu and select ***Alternate Locations***. In the **Alternate Locations** modal page, you can define a sub-location for the organization.

The **Organizational Alternate Locations** pane displays the following about each location:

- ***Location Name***. Name of the alternate organization.
- ***City***. City where the additional branch is located.
- ***State***. State where the additional branch is located.
- ***Zip Code***. Zip code of the additional location.
- ***Country***. Country where the additional branch is located.
- ***Primary Contact***. Name of the contact for the alternate location. To view detailed contact information, click on the contact icon ( ).
- ***Secondary Contact***. Name of the contact for alternate location. To view detailed contact information, click on the contact icon ( ).
- ***Tools***. For each location, you can use the following tools:
    - *View/edit properties of location* ( ). Leads to the **Location Editor** modal page, where you can edit the properties of an alternate location.
    - *Delete* ( ). Click this icon to delete the location.

Deleting an Existing Organization

Before you can delete an organization, you must first move all the user accounts and devices to another organization.

> **NOTE**: You cannot delete the System organization.

To move multiple devices from their current organization to another organization:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. In the **Device Manager** page, select the checkbox of each device to be moved to a new organization.
3. In the ***Select Action*** drop-down field (in the lower right), choose *Move to Organization* and select a new organization to associate with the devices.
4. Click the **[Go]** button.
5. Each selected device will now be associated with the new organization.

To move a user account from its current organization to another organization:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. In the **User Accounts** page, find the user account that you want to move. Click its wrench icon ( ).
3. Click the **[Permissions]** tab. In the **Account Permissions** page, select a new value in the ***Primary Organization*** field.

4. Click the **[Save]** button.
5. Repeat steps 2-4 for each user account you want to move to another organization.

To delete one or more organizations:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, select the checkbox (☑) for each organization you want to delete.
3. From the ***Select Actions*** menu in the lower right, select *DELETE*. Click the **[Go]** button.
4. The selected organizations will be deleted from SL1.

Performing Administrative Tasks for Multiple Organizations

The **Organizational Account Administration** page contains a drop-down field in the lower right called ***Select Action***. This field allows you to apply an action to multiple organizations at once.

To apply an action to multiple organizations:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. Select the checkbox (☑) for each organization that you want to apply the action to. To select all checkboxes for all organizations, select the big checkbox icon (☑) at the top of the page.
3. In the ***Select Action*** drop-down list, select one of the following actions:

    - ***DELETE***. Deletes all selected organizations from SL1. You must first move all devices and users to another organization. For details on how to do this, see the section on *Deleting an Organization*.
    - ***CLEAR Audit Logs***. Deletes data from the organization's log files. You can view an organization's log entries in the **Organizational Logs** page.
    - ***CREATE Google Earth Map***. Creates a .KML file that can be opened in Google Earth. The .KML file contains the location of each selected organization (based on the address(es) in each **Organization Properties** page). When you open the file in Google Earth, locations for each selected organization will be flagged.

To apply ***CREATE Google Earth Map*** to one or multiple organizations, you must first:

1. Make sure you have installed Google Earth on the local computer.
2. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
3. In the **Organizational Account Administration** page, find the organization that you want to view in Google Earth. Click the wrench icon (🔧) for that organization.
4. From the **Organizational Summary** page (or any page in the Organizational Administration tools), click the **[Actions]** menu.
5. From the **[Actions]** menu, select ***Geolocate Coordinates***.
6. Perform steps 3-5 for each organization that you want to view in Google Earth.

Example: Creating an Organization

The following example walks you through the steps for creating an organization.

- For this example, we'll use an imaginary company with three locations: a sales office in Boston, headquarters in Chicago, and an R&D office in California. The company has decided to create organizations based on geographical location.
- The company wants to create three organizations:
    - Northeast
    - Headquarters
    - West Coast
- Each organization will contain the local hardware and the local users. This plan will ensure that users can access information on local devices and local users. Administrators can define Access Keys to further limit or allow access.

In this example, we'll create the organization called "Northeast".

To create the "Northeast" organization:

1. Log in to SL1 as a system administrator. If you have not yet created organizations or user accounts, you can log in as "em7admin", using the password defined during initial configuration.
2. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
3. In the **Organizational Account Administration** page, click the **[Create]** button.
4. The **Add Organizational Record** page appears.
5. In the **Add Organizational Record** page, supply values in each field.
    - ***Organization Name***. We supplied the value "Northeast" as the name of the new organization.
    - ***Street Address***. We supplied the value "150 State Street" as the street address for the new organization.
    - ***City***. We supplied the value "Boston" as the city for the organization.
    - ***State***. We selected "Massachusetts" as the state for the organization.
    - ***Postal Code***. We supplied the value "02109" as the zip code for the organization.
    - ***Country***. We accepted the default value ("United States").
    - ***Contact First Name***. Our contact at the Boston office is named Paul Revere. So we supplied the value "Paul".
    - ***Contact Last Name***. Our contact at the Boston office is named Paul Revere. So we supplied the value "Revere".
    - ***Title***. We supplied the value "Vice President" as Paul Revere's title.
    - ***Department***. We supplied the value "Sales" as the department for Paul Revere.
    - ***Phone***. We supplied the value "(617) 552-1212" as the main phone number for the organization.

- ***Fax Phone***. We supplied the value "(617) 552-1111" as the fax phone number for the organization.
- ***Toll Free***. We supplied the value "(617) 552-3333" as the toll-free phone number for the organization.
- ***Email***. We supplied the value "prevere@company.com" as the organization's main email address.
- ***Billing ID***. This field is option. We supplied the value "abcs-1234" as the Billing ID for organization.
- ***CRM ID***. This field is optional. We supplied the value "wxyz-9876" as CRM ID for organization.
- ***Email Notification Append Text***. This field is optional. We did not enter a value in this field.
- ***Longitude***. This value is optional. We can't generate a longitude value until after we have saved the organization's definition.
- ***Latitude***. This value is optional. We can't generate a longitude value until after we have saved the organization's definition.
- ***Organizational Ticket Watchers***. This value is optional. We did not select a ticket watcher in this field.

6. Click the **[Save]** button to save the new organization policy.
7. When we perform discovery for the network in Boston, we must specify "Northeast" as the organization. This ensures that all discovered devices and components are included in the "Northeast" organization.
8. When we create user accounts for the users in the Boston office, we must specify "Northeast" as the primary organization. This ensures that the users in the Boston office will be able to view information about the devices and applications in their network and be able to manage the user accounts in the "Northeast" organization.

Chapter 3

Managing Organizations

Overview

This chapter covers many of the tasks that can be undertaken from the tabs in the **Organizational Administration** panel. These tasks include creating user accounts in the organization, viewing and adding organization devices, creating external contacts for the organization, creating tickets, viewing logs, associating products, and adding notes to the organization.

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:

Organizational Administration Panel

After saving a new organization, you can access the additional tabs in the **Organizational Administration** panel. These tabs allow you to further configure the organization and manage the organization. For example, these tabs allow you to add, edit, or view user accounts associated with the organization, view all devices and other elements associated with the organization, and view, create, or edit tickets about the organization, among other tasks.

The **Organizational Administration** panel for each organization includes the following tabs:

- ***Summary***. The **Organizational Summary** page displays read-only details about the organization and links to all elements associated with the organization.
- ***Properties***. The **Organization Properties** page displays the contact information for an organization and also lists all SKUs used by the organization and all additional locations for the organization.
- ***Logs***. The **Organizational Logs** page displays a record of all actions pertaining to the Organization, including all logins by organization members, all notifications sent to organization members, all events associated with an element in the organization or the organization itself, all create, edit, or delete actions in SL1 by organization members.
- ***Accounts***. The **Organizational Accounts** page displays a list of all user accounts associated with the organization. From this page, you can view and edit information about those user accounts.
- ***Contacts***. The **External Contact Accounts** page allows you to define users who can be sent email from within SL1. These external contacts can be sent messages from the **Service Notifier** page (Registry > Business Services > Service Notifier).
- ***Events***. The **Organizational Events** page displays a list of all active events associated with the organization. You can go the **[Actions]** menu and choose to view all cleared events associated with the organization.
- ***Tickets***. The **Organizational Tickets** page displays a list of all open, pending, and working tickets associated with the organization.
- ***Notes***. The **Organizational Notes** page displays all notes associated with the organization and created by selecting ***Notepad Editor*** from the **[Actions]** menu.

The Actions Menu

Each page in the **Organization Administration** panel (the set of tabs for each organization) includes the **[Actions]** menu. This menu allows you to perform many organization and account-related tasks, directly from the current page. The **[Actions]** menu looks like a button and is located in the upper right of the page.

The following entries in the **[Actions]** menu appear on each page in the **Organization Administration** panel.

- ***My Bookmarks***. Displays the **Administer Bookmarks** modal page, where you can access pre-defined bookmarks or save a new bookmark.
- ***Add New Account***. Leads to the *Create New Account* page, where you can define a new user account to include in the organization.

- ***Add New External Contact***. Leads to the *Create New External Contact* modal page, where you can define a new external contact to include in the organization.
- ***Alternate Locations***. Leads to the *Alternate Locations* modal page, where you can define an additional location, address, and contact information for the organization.
- ***Create a Ticket***. Leads to the *Ticket Editor* page, where you can define a new ticket about the organization.
- ***Custom Navigation***. Leads to the **Custom Navigation** modal page, where you can define a custom tab for the **Organization Administration** page for the current organization. The custom tab will contain a link to an outside URL.
- ***Organizational Finder***. Leads to the **Finder** page, where you can search SL1 for elements.
- ***Geolocate Coordinates***. *Generates latitude and longitude coordinates* for the organization's main location. The coordinates appear in the **Organization Properties** page and allow you to view the organization in the Google Earth application.
- ***Notepad Editor***. Leads to the *Notepad Editor* modal page, where you can enter a note to include with the organization. The note will appear in the **Organizational Notes** page for the organization.
- ***Product Catalog***. Leads to the *Product Catalog* modal page, where you can associate a product SKU with the organization or disassociate the organization from a product SKU.
- ***Report Creator***. Leads to the *Report Creator* modal page, where you can define an organization report, including the information to include in the report and the format in which to generate the report.

Shortcut Keys

You can access the **Organizational Account Administration** page from any place in SL1 by entering the following key combination:

- Ctrl + Alt + 0 (zero)

Viewing Details in the Organizational Summary Page

The **Organizational Summary** page provides an overview of an organization, information about the elements associated with the organization, and the current status of the organization.

To view the **Organizational Summary** page:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization you want to edit. Click its wrench icon ().
3. The **Organizational Summary** page appears.
4. The **Organizational Summary** page displays the following:

Events

The **Events** pane displays a list of active events associated with the organization. For each event, the **Events** pane displays the following:

- ***Date and time***. Date and time the event last occurred on the organization.
- ***Element***. Element associated with the event.
- ***Message***. The event message. The message is color-coded for severity.
    - Critical. Critical events are those that require immediate attention.
    - Major. Major events are those that require immediate investigation.
    - Minor. Minor events are those that need to be investigated before problems become sever.
    - Notice. Notice events are those that require attention but are not problem-related.
    - Healthy. Healthy events are those that are not urgent.

Clicking on an event displays the **Event Summary** modal page, where you can view details about the event.

Managed Entities

The **Managed Entities** pane displays the number of each type of element associated with the organization. This pane can contain entries for one or more of the following:

- ***Active Tickets (OWP)***. Specifies the number of active tickets associated with the organization. Clicking on the life ring icon () or the number of tickets leads to the *Organizational Tickets* page, where you can view details about the active tickets for the organization.
- ***Resolved Tickets***. Specifies the number of resolved tickets associated with the organization. Clicking on the life ring icon () or the number of tickets leads to the *Organizational Tickets* page, where you can view details about the resolved tickets for the organization.
- ***Active Events***. Specifies the number of active events associated with the organization. Clicking on the events icon () or the number of events leads to the *Organizational Events* page, where you can view details about the list of active events associated with the organization.
- ***Cleared Events***. Specifies the number of events that have been cleared or automatically resolved. Clicking on the events icon () or the number of events leads to the *Organizational Events* page, where you can view details about the list of active events associated with the organization.
- ***Accounts***. Displays the number of user accounts associated with the organization. Clicking on the accounts icon () leads to the *Organizational Accounts* page, where you can view details on the list of accounts.
- ***Product Services***. Specifies the number of product or service SKUs associated with the organization. Clicking on the barcode icon or the number of products displays the *Product Services* modal page. In this page, you can view details about the products associated with the organization.

- ***External Contacts***. Displays the number of external contacts associated with the organization. Clicking on the number or the contacts icon () leads to the *External Contact Accounts* page, where you can view details about the list of external contacts.
- ***Devices***. Displays the number of organizations associated with the organization. Clicking on the number or the devices icon () leads to the *Organizational Finder* page, where you can view details on the list of devices in the organization.
- ***Asset Records***. Displays the number of asset records associated with the organization. Clicking on the number or the asset icon () leads to the **Organizational Finder** page, where you can view details on the list of assets associated with the organization.
- ***IPv4 Networks***. Displays the number of asset records associated with the organization. Clicking on the number or the network icon () leads to the **Organizational Finder** page, where you can view details on the list of networks associated with the organization.
- ***Interfaces***. Displays the number of asset records associated with the organization. Clicking on the number or the interface icon () leads to the **Organizational Finder** page, where you can view details on the list of interfaces associated with the organization.
- ***Virtual Interfaces***. Displays the number of asset records associated with the organization. Clicking on the number or the virtual interface icon () leads to the **Organizational Finder** page, where you can view details on the list of virtual interfaces associated with the organization.

> **NOTE**: When a user assigns a network interface to a bandwidth policy, SL1 creates a virtual interface. The virtual interface represents the network interface, as monitored by the bandwidth policy. If multiple interfaces from a single organization are assigned to a bandwidth policy, the virtual interface represents the "sum" of the interfaces assigned to the policy. For example, suppose an organization has two network interfaces. Suppose both interfaces are assigned to a single bandwidth policy. The virtual interface for the organization will represent both network interfaces.

Tickets

The **Tickets** pane displays a list of open tickets associated with the organization. For each ticket, the following is displayed:

- ***Date and Time***. Date and time ticket was created or last edited.
- ***Element associated with the Ticket***. Element associated with the ticket.
- ***Ticket Message***. Message displayed by the ticket.

Clicking on a ticket message displays the **Ticket Summary** page for that ticket.

Contact List

The **Contact List** pane displays information about all the user accounts associated with the organization.

- ***Name***. Name of person to contact. Clicking on the name or the wrench icon () leads to the *Account Properties* page for the user account.

- ***Role***. Description of the user's responsibilities in case of a critical situation. The user's description might differ from the user's actual title. For example, a contact's title might be Senior Engineer, but his/her role for the organization might be technical lead.
- ***Critical Contact***. Circumstance when person should be contacted. This description might differ from the user's department. For example, the user's department might be Operations, but his/her role for the organization might be Hardware Maintenance.
- ***Phone***. Person's phone number.
- ***Cell***. Person's cell phone number.
- ***Pager***. Person's pager number.
- ***Email***. Person's email address. Clicking on this link opens an email client on the local computer and creates a new email message, with the contact's email address in the ***To*** field.

Organization Name

This pane displays the address, phone and Email information about the organization.

Editing Contact Information in the Organization Properties Page

The **Organization Properties** page displays the basic properties of the selected Organization and also additional information about critical contacts, product usage, and sub-locations.

In the **Organization Properties** page, you can view and edit the contact information for the organization.

To access the **Organization Properties** page:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization you want to edit. Click its wrench icon (). The **Organizational Summary** page appears.
3. Click the **[Properties]** tab. The **Organization Properties** page appears.

Organization Properties

The **Organization Properties** page contains the following fields:

- ***Organization Name***. Name of the organization. Can be any combination of characters up to 128 characters in length.
- ***Street Address***. Street address of the organization. For easier viewing, ScienceLogic suggests that you limit the address to 5 lines, with up to 60 characters per line.
- ***City***. City where the organization is located. Can be up to 64 characters in length.
- ***State***. State where the organization is located. Select from the drop-down list.
- ***Postal Code***. Zip code of the organization. Can be up to 15 characters in length.
- ***Country***. Country where the organization is located. Select from the drop-down list.

- ***Contact First Name***. First name of organization contact. Can be up to 128 characters in length.
- ***Contact Last Name***. Last name of organization contact. Can be up to 64 characters in length.
- ***Title***. Contact's title. Can be up to 64 characters in length.
- ***Department***. Contact's department. Can be up to 64 characters in length.
- ***Phone***. Business phone number for the organization. Can be up to 36 characters in length.
- ***Fax Phone***. Fax number for the organization. Can be up to 36 characters in length.
- ***Toll Free***. Toll-free phone number for the organization. Can be up to 36 characters in length.
- ***Email***. Organization's main email address. Can be up to 250 characters in length.
- ***Billing ID***. Billing ID for organization. Can be up to 24 characters in length.
- ***CRM ID***. CRM ID for organization. Can be up to 64 characters in length.
- ***Email Notification Append Text***. The text entered in this field will appear at the bottom of all email messages sent from SL1 to members of this organization. This includes automated email messages and email messages that are sent manually either by clicking on an email icon or from the **Send Message** tab in the **Ticket Editor** page.
- ***Longitude***. Displays the longitude associated with the organization's address. To generate this field, click the **[Actions]** menu and then select ***Geolocate Coordinates***.
- ***Latitude***. Displays the latitude associated with the organization's address. To generate this field, click the **[Actions]** menu and then select ***Geolocate Coordinates***.
- ***Organizational Ticket Watchers***. You can select one or more users (in addition to the ticket's creator or assignee) who will be considered "watchers" for all tickets associated with the organization. Each organizational watcher will be notified when a ticket is created and aligned with the organization and when that ticket is assigned to a user or changes status. When that ticket is created, assigned, or updated, SL1 will automatically send email notifications to the list of watchers.

NOTE: Users whose ***Login State*** is set to *Suspended* on the **Account Permissions** page will not display in the list of users in the ***Organizational Ticket Watchers*** field. For details about suspending user accounts, see the *Managing User Accounts* section.

NOTE: On the **Behavior Settings** page (System > Settings > Behavior, if the field ***Automatic Ticketing Emails*** is set to *Disabled*, all assignees and watchers will not receive automatic email notifications about any tickets. By default, the field is set to *Enabled*.

Critical Contact List

The **Critical Contact List** pane is useful when organization members must assign a task or contact a key team member.

A user appears in this pane if he/she was defined as a critical contact in the *Account Properties* page.

The **Critical Contact List** pane displays the following information about each critical contact:

- ***Name***. Name of person to contact.
- ***Role***. Description of the user's responsibilities in case of a critical situation. This description might differ from the user's actual title. For example, a contact's title might be Senior Engineer, but his/her role for the organization might be technical lead.
- ***Critical Contact***. Circumstance when person should be contacted. This description might differ from the user's department. For example, the user's department might be Operations, but his/her role for the organization might be Hardware Maintenance.
- ***Phone***. Person's phone number.
- ***Cell***. Person's cell phone number.
- ***Pager***. Person's pager number.
- ***Email***. Person's email address.
- ***Tools***. The following tools are available for each entry in the critical contact list:
    - *Manage User's Contact Information* (). Leads to the **Account Properties** page, where you can edit the person's contact information.
    - *Send Email Message to this User* (). Opens an email client on the local desktop. The ***To*** field is populated with the email address of the selected user.

Product Usage List

The Product Usage List displays a list of SKUs associated with the organization. Usually, a SKU is associated with an organization because the organization is using that product or service.

To associate a SKU with the organization or change the list of SKUs associated with the organization, click the **[Actions]** menu and then select ***Product Catalog***. In the **Product Catalog** modal page, you can add and remove products from the organization.

For each product associated with the organization, the **Product Usage List** pane displays the following:

- ***SKU Class***. Description of the SKU. Can be up to 64 characters in length.
- ***SKU Number***. Numeric ID for the SKU. Can be up to 24 characters in length.
- ***SKU Name***. Name of the SKU. Can be up to 64 characters in length.
- ***Name***. The name of the element using the SKU. Clicking on the icon for the element leads to a page where you can view more information about the element.
- ***Type***. The type of element using the SKU. Choices are:
    - Organization
    - Device
    - Asset
    - Domain Name
    - Network

- Interface
- Other

Organizational Alternate Locations

If one or more alternate locations have already been defined for the Organization, the **Organizational Alternate Locations** pane appears at the bottom of the page.

To define an alternate location for an organization, click the **[Actions]** menu and select ***Alternate Locations***. In the **Alternate Locations** modal page, you can define a sub-location for the organization.

The **Organizational Alternate Locations** pane displays the following about each location:

- ***Location Name***. Name of the alternate organization.
- ***City***. City where the additional branch is located.
- ***State***. State where the additional branch is located.
- ***Zip Code***. Zip code of the additional location.
- ***Country***. Country where the additional branch is located.
- ***Primary Contact***. Name of the contact for the alternate location. To view detailed contact information, click on the contact icon ( ).
- ***Secondary Contact***. Name of the contact for alternate location. To view detailed contact information, click on the contact icon ( ).
- ***Tools***. For each location, you can use the following tools:
  - *View/edit properties of location* ( ). Leads to the **Location Editor** modal page, where you can edit the properties of an alternate location.
  - *Delete* ( ). Click this icon to delete the location.

Viewing the User Accounts in an Organization

Each user account in SL1 is associated with an organization. Usually, each organization in SL1 will include at least one user account (although an organization is not required to include user accounts).

The Organization Administration tools allow you to view, create, and edit user accounts for an organization.

There are two ways you can view a list of user accounts associated with an organization. This section describes both ways.

To view a list of user accounts associated with an organization:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization you are interested in. Check if its *Users* column contains a value. If it does, you can click the user icon ( ). SL1 will display the **Finder** page with a list of each user in the organization. From this page, you can click the business card icon ( ) to edit an account's properties.

3. From the **Organizational Account Administration** page, you can also click the wrench icon () for an organization and then click the **[Accounts]** tab. The **Organizational Accounts** page will display a list of user accounts for the organization. From this page, you can click the wrench icon () to edit an account's properties.

Creating a User Account for an Organization

Each user account in SL1 is associated with an organization. Usually, each organization in SL1 will include at least one user account (although an organization is not required to include user accounts).

You can create a new user account from the Organizational Administration tools. The new account will automatically be associated with the organization from which you created the account.

To add a user account to an organization:

1. Go to **Organizational Account Administration** (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization where you want to add a new user account. Click the wrench icon () for that organization.
3. From the **Organizational Summary** page (or any page in the Organizational Administration tools), click the **[Actions]** menu.
4. From the **[Actions]** menu, select ***Add New Account***.
5. The **Create New Account** page appears. Supply a value in each field:
    - ***First Name***. User's first name. This value can be up to 24 characters in length.
    - ***Last Name***. User's last name. This value can be up to 24 characters in length.
    - ***Generate a unique name based on first and last name***. If you select this checkbox, SL1 will generate a login name for the user.
    - ***Password***. The user's password. This value must be at least six characters in length and can be up to 64 characters in length.
    - ***Confirm Password***. The user's password again. This value must be at least four characters in length and can be up to 64 characters in length.
    - ***Account Login Name***. User's login name. This field can be up to 32 characters in length.
    - ***Primary Email***. User's email address. This field can be up to 64 characters in length.
    - ***Organization***. The organization of which the new user account will be a member. Users can select from among all organizations in SL1.
    - ***Account Type***. Specifies whether the user is a member of a user policy. Choices are:

- *Individual*. User account is not a member of a user policy.
- *Policy Membership*. User will be defined with a user policy. When selected, the ***Policy Membership*** field becomes active.
  - When a user policy is applied to a user's account, the user inherits the Key Privileges specified in the user policy. Administrators cannot add additional Key Privileges or delete Key Privileges from the user's account.
  - When a user policy is edited, each user account that is a member of that policy will be dynamically updated.

- ***Account Type***. This drop-down contains an entry for each standard account type. These account types affect the list of Key Privileges for the user. The choices are:
  - *Administrator*. By default, administrators are granted all permissions available in SL1. Administrators can access all tabs and pages and perform all actions and tasks.
  - *User*. Accounts of type "user" are assigned key privileges. Key privileges are customizable by the administrator and grant users access to pages and tabs and permit users to view information and perform tasks in SL1. These key privileges are defined by the system administrator from the **Access Keys** page (System > Manage > Access Keys).
- ***Organization***. The organization of which the new user account will be a member. You can select from among all organizations in SL1.
- ***Login State***. Default login state for the user account. The choices are:
  - *Suspended*. Account is not active. User cannot log in to SL1.
  - *Active*. Account is active. User can log in to SL1.
- ***Authentication Method***. Specifies how the user will be authenticated. The choices are:
  - *EM7 Session*. User's username and password are authenticated by the Database Server.
  - *LDAP/Active Directory*. User's username and password are authenticated by an LDAP server or Active Directory server. For details on configuring SL1 to use LDAP or Active Directory authentication, see the manual on using ***LDAP or Active Directory***.

NOTE: For users who are authenticated with Single Sign-On (SSO), SL1 ignores the ***Authentication Method*** field. For details on configuring SL1 to use SSO authentication, see the manual on using ***Using Single Sign-On***.

- ***Restrict to IP***. The user will be allowed to access SL1 only from the specified IP. Specify the IP address in standard dotted-decimal notation.
- ***Time Zone***. Select the appropriate time zone to associate with the user account.

NOTE: If the user account is aligned with a user policy that specifies a time zone, the ***Time Zone*** field will be disabled. The user account will use the Time Zone specified in the user policy and the ***Time Zone*** field cannot be edited.

- ***Policy Membership***. If you selected *Policy Membership* in the ***Account Type*** field, the ***Policy Membership*** field is activated. In this field, you can select a user policy to apply to the new user account.

  - When a user policy is applied to a user's account, the user inherits the Key Privileges specified in the user policy. Administrators cannot add additional Key Privileges or delete Key Privileges from the user's account.
  - When a user policy is edited, each user account that is a member of that template will be dynamically updated.

6. Click the **[Save]** button to save the new account.
7. After saving, additional tabs (the Account tools) will appear for the account. You can then define additional parameters for the account. For details on the account tools, see the section on *Creating and Editing User Accounts*.
8. To later edit the user account from the **Organizational Accounts** page, click the wrench icon () for an account. The Account tools will appear for the account. For details on the account tools, see the section on *Creating and Editing User Accounts*.
9. You can also perform administrative tasks on multiple accounts from the **Organizational Accounts** page. To do so:

   - Select the checkbox for each account you want to edit.
   - In the ***Select Action*** drop-down list, select one of the following actions.

     - ***DELETE Accounts***. Deletes all selected user accounts.
     - ***Require LDAP/AD Authentication***. Each selected user must be authenticated on an LDAP server or an Active Directory server. User must have an existing account on an LDAP server or an Active Directory server. For details on configuring SL1 to use LDAP or Active Directory authentication, see the manual ***Using LDAP or Active Directory***.
     - ***Remove LDAP/AD Authentication***. Each selected user must be authenticated by a Compute Nodes.
     - ***Change Brand To***. Change the default theme (page layout, color, and graphics) for the user. Select from the list of existing themes.

   - Click the **[Go]** button to apply the selected action to each selected user account.

Viewing the Devices in an Organization

Each device in SL1 is associated with an organization. You can use the **Organizational Account Administration** page to view a list of devices associated with a specific organization.

To view a list of devices associated with a specific organization:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization you are interested in.
3. Check if its *Devices* column contains a value. If it does, you can click the devices icon ( ).
4. SL1 will display the **Finder** page with a list of each device in the organization.
5. From the **Finder** page, you can click the device icon ( ) to edit a device's properties.

Adding Devices to an Organization

There are two ways to add a device with an organization:

- Specifying the organization during discovery of the device.
- Moving a device from its current organization to another organization.

SL1's discovery tool automatically finds all the devices, hardware components, and software applications in your network. You must provide the discovery tool with a range of IP addresses, and SL1 finds all the devices, hardware components, and software applications in the range. For each discovered device, hardware component, or software application, SL1 gathers detailed data. This data is used throughout SL1.

To specify an organization during dynamic discovery:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. ***To edit an existing discovery session***, go to the Session Register and click the appropriate wrench icon ( ).
3. ***To create a new discovery session***, click the **[Create]** button.
4. In the **Discovery Session Editor** modal page, supply values the following field related to organization(s).

    - ***Organization***. This field contains a list of all organizations defined in SL1. Devices discovered during the discovery session will be assigned to the selected organization.

NOTE: Make sure you have the desired organization created and selected before running the discovery process. This field assigns all devices and networks in the specified IP range to a single organization. However, you can later assign individual devices and networks to different organizations.

5. In the ***Organization*** field, select a single organization from the list of all organizations in SL1. All devices discovered during this discovery session will be associated with the selected organization.

To move a discovered device from its current organization to another organization:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. In the **Device Manager** page, select the checkbox of each device to be moved to a new organization.
3. In the ***Select Action*** drop-down list, choose *Move to Organization* and select a new organization to associate with the devices.
4. Click the **[Go]** button.
5. Each selected organization will now be associated with the new organization.

Viewing the External Contacts in an Organization

An external contact is a user to whom you can send email messages from SL1 (from the **Service Notifier** page). However, external contacts do not have accounts and cannot log in to SL1. Like users, external contacts are associated with organizations. This section describes how to view a list of external contacts associated with an organization. To learn more about external contacts, see the *External Contacts* section.

To view the list of external contacts associated with an organization:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization you are interested in. Click its wrench icon ().
3. When the **Organizational Administration** panel appears, click the **[Contacts]** tab.
4. The **External Contact Accounts** page appears. This page displays a list of external contacts for the organization.
5. The **External Contact Accounts** page displays the following about each external contact:
    - ***Last Name | First Name***. Last name and first name of the external contact.
    - ***Title***. The external contact's work title.
    - ***Email Address***. Email address associated with the external contact account.
    - ***City***. City associated with the external contact account.
    - ***State***. State associated with the external contact account.
    - ***Postal Code***. Postal code associated with the external contact account.
    - ***Phone Number***. Phone number associated with the external contact account.
    - ***Subscriber ID***. Unique, numeric ID, automatically assigned to each external contact account by SL1.
    - ***Edit Date***. Date and time the external contact account was created or last edited.

Creating External Contacts for an Organization

External contacts can be created either from the **External Contacts** page or from the **Organizational Administration** tools. This section will describe how to create an external contact from the **Organizational**

Administration tools. To learn how to create an external contact from the **External Contacts** page, see the *External Contacts* section.

To create a new external contact account for the organization:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization where you want to add a new user account. Click the wrench icon () for that organization.
3. From the **Organizational Summary** page (or any page in the Organizational Administration tools), click the **[Actions]** menu.
4. From the **[Actions]** menu, select ***Add New External Contact***.
5. The **Create New External Contact** page appears.
6. To define a new external contact, supply a value in each field. (The organization field will already be populated with the name of the current organization)

    - ***First Name***. Contact's first name. This value can be up to 24 characters in length.
    - ***Last Name***. Contact's last name. This value can be up to 24 characters in length.
    - ***Title***. Contact's title. This field can be up to 32 characters in length.
    - ***Department***. Contact's department. This field can be up to 36 characters in length.
    - ***Phone***. Contact's phone number at work. This field can be up to 24 characters in length.
    - ***Fax***. Contact's fax number at work. This field can be up to 24 characters in length.
    - ***Mobile***. Contact's cell phone number. This field can be up to 24 characters in length.
    - ***Pager***. Any other phone numbers for contacting the person. This field can be up to 24 characters in length.
    - ***Primary Email***. Contact's primary email address. This field can be up to 64 characters in length.
    - ***Secondary Email***. Additional email address for contacting the person. This field can be up to 64 characters in length.
    - ***AlternateEmail***. Additional email address for contacting the person. This field can be up to 64 characters in length.
    - ***Street Address***. Contact's street address at work. This field can be up to 64 characters in length.
    - ***Suite/Building***. Suite/Building for the person at work. This field can be up to 64 characters in length.
    - ***City***. City where the person works. This field can be up to 64 characters in length.
    - ***State***. State where the person works.
    - ***Postal Code***. Zip code where the person works. This field can be up to 12 characters in length.
    - ***Country***. Country where the person works.

> **NOTE**: By default, the ***Country*** field will be set to the country specified in the **Behavior Settings** page (System > Settings > Behavior). You can override this setting for the current external contact. Editing the value in this field will not affect the system-wide default setting.

- ***Toll Free***. Toll-free phone number for the person. This field can be up to 24 characters in length.
- ***Organization***. Organization to associate with the person. Select from a list of all organizations in SL1.
- ***Key Role***. Description of the contact's responsibilities in case of a critical situation. This description might differ from the contact's actual title. For example, a contact's title might be Senior Engineer, but his/her role for the organization might be technical lead. Select from the drop-down list. (Administrators can go to the **Select Objects Editor** page to customize the entries that appear in this list.) If a value is supplied in this field, the contact will appear as a ***Critical Contact*** for the organization in the **Organization Properties** page.
- ***Critical Contact***. Circumstance when person should be contacted. This description might differ from the contact's department. For example, the contact's department might be Operations, but his/her role for the organization might be Hardware Maintenance. Select from the drop-down list. (Administrators can go to the **Select Objects Editor** page to customize the entries that appear in this list.) If a value is supplied in this field, the contact will appear as a ***Critical Contact*** for the organization in the **Organization Properties** page.
- ***Pass Phrase***. Questions that verify a contact who has forgotten his/her password. SL1 does not use this field.
    - What is your Mother's maiden name?
    - What is your favorite pet's name?
    - What is your favorite color?
- ***Answer***. This field contains the answer to the question selected in the ***Pass Phrase*** field. This field can be up to 64 characters in length.
- ***Time Zone***. Time zone associated with the contact's location. Select from a list of all time zones.
- ***Billing ID***. Billing ID associated with this contact. This field can be up to 24 characters in length.
- ***CRM ID***. CRM ID associated with this contact. This field can be up to 64 characters in length.
- ***Notes***. Any notes you want to include with the contact's profile information.

7. Click the **[Save]** button to save the new external contact account.
8. The new external contact account should now appear under the **[Contacts]** tab, in the **External Contact Accounts** page.

Viewing Events for an Organization

One of the easiest ways to monitor the health of your network is to look at events. Events are messages that are triggered when a specific condition is met. For example, an event can signal that a server has gone down, that a device's hard drives are getting too full, or simply display the status of a device.

Each instance of an event in SL1 is associated with an organization. Each occurrence of an event is grouped by organization (the organization associated with the device where the event occurred or the organization associated with the policy that generated the event).

In the **Organizational Administration** panel, you can view a list of events associated with a specific organization.

To view a list of events associated with a specific organization:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization with associated events that you want to view.
3. If a value appears in the *Events* column, click the event icon ().
4. The **Organizational Events** page appears for the organization.

   This page displays a list of all active events associated with the organization or the organization's elements. For each event, the page displays:

   - ***Name***. Name of the element associated with the event.
   - ***Event Message | Severity***. Message generated by event, as defined in the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit). The message is color-coded for severity.
   - ***Acknowledged***. Specifies whether a ScienceLogic user has acknowledged this event.
     - *Red check*. Event has not been acknowledged.
     - *Gray check with name*. Event has been acknowledged.
   - ***Age / Elapse***. Number of days, hours, and minutes since the first occurrence of the event.
   - ***Ticket***. Ticket ID associated with this event, if applicable.
   - ***Last Detected***. Date and time of last occurrence of the event.
   - ***EID***. Unique ID for the event, generated by SL1.

- ***Source***. Source of the log message that triggers the event, as defined in the **Event Policy Editor** page (Registry > Events > Event Manager > create or edit). Choices are:
    - *Syslog* . Event was generated from standard system log generated by device.
    - *Internal*. Event was generated by SL1.
    - *Trap*. Event was generated by an SNMP trap.
    - *Dynamic*. Event was generated by a dynamic application collecting data from the device.
    - *Email*. Event was generated by an email from an external agent; for example, Microsoft Operations Manager (MOM).
    - *API*. Event was generated by a snippet Run Book Action, a snippet Dynamic Application, a request to the ScienceLogic API, or by an external system.
- ***Count***. Number of times this event has occurred.
- ***View Notifications icon*** (). Leads to the **Event Actions Log**, where you can view details about each automation policy that has triggered for the event.
- ***Statistics icon*** (). Displays the **Event Statistics** page, where you can view historical statistics for the selected event.
- ***Information icon*** (). Displays the **Event Information** page, where you can view an overview of the selected event, suppress the selected event, or edit the definition of the selected event.

NOTE: To view a list of all cleared events for the organization, click the **[Actions]** menu and select ***View Cleared Events***. To return to the list of active events, click the **[Actions]** menu and select ***View Active Events***.

Viewing Tickets for an Organization

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 work required by your enterprise. A ticket can be created manually or be created based on an event.

Each ticket in SL1 is associated with an organization. That organization can either be the subject of the ticket or be associated with a device or policy that is the main subject of the ticket.

In the **Organizational Administration** panel, you can view a list of tickets associated with a specific organization.

To view a list of tickets associated with a specific organization:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization you are interested in. Click its wrench icon ().

3. Click the **[Tickets]** tab. The **Organizational Tickets** page appears, displaying a list of all open, pending, working, and resolved tickets associated with the organization and its elements.

Creating a Ticket for an Organization

You can create a ticket about an organization without having to leave the **Organizational Administration** tools. To do this:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization you are interested in. Click its wrench icon ()
3. From the **Organizational Summary** page (or any page in the Organizational Administration tools), click the **[Actions]** menu.
4. From the **[Actions]** menu, select ***Create a Ticket***.
5. The **Ticket Editor** page appears.
6. To create a new ticket, supply a value in each field.

    - ***Organization***. Select the organization with which the ticket will be associated. You can select from a list of all organizations that you are a member of. When creating a ticket from an organization's **Organizational Summary** page, that organization will already be selected.
    - ***Ticket Description***. Description of the problem or ticket. By default, this field will include the text "Ticket for Organization" and then the name of the organization. However, you can edit this description.
    - ***Sub-Organization***. Select a second organization with which the ticket will be associated.
    - ***Ticket State***. Custom parameter, defined in the **Ticket States** page (Registry > Ticketing > Custom States). Allows you to add additional workflow restrictions to a ticket.
    - ***Severity***. The severity of the problem. Choices are:

        - Severity 0/Healthy
        - Severity 1/Notice
        - Severity 2/Minor
        - Severity 3/Major
        - Severity 4/Critical

    - ***Category***. Descriptive category assigned to the ticket. You can use the **Select Objects Editor** page (System > Customize > Select Objects) to customize the list of possible categories.
    - ***Source***. Original source for the ticket. You can use the **Select Objects Editor** page (System > Customize > Select Objects) to customize the list of possible sources. The default choices are:

- *Automated*. Ticket was created automatically when an event occurred.
- *Email*. An Email about an issue prompted this ticket.
- *External*. An external source created this ticket.
- *Internal*. Ticket was created in SL1.
- *Phone*. A phone call about an issue prompted this ticket.

- ***Queue***. Ticket Queue to which the ticket will be assigned.
- ***Assigned User***. User who is responsible for resolving the ticket. This drop-down list contains entries for each user assigned to the specified Ticket Queue and who has a Login State of *Active*. When a ticket is assigned to a user, SL1 automatically sends the user an Email message as notification.
- ***Custom Fields***. If your SL1 system includes embedded custom fields for tickets, you can supply a value in those fields.
- ***Notes & Attachments***. The **Notes & Attachments** pane in the **Ticket Editor** page allows you to enter notes or comments about a ticket, insert content from a saved template, or to add images, videos, or attachments to the ticket.
  - To add a note to a ticket, click the **[New Note]** button in the **Ticket Editor** page. A new instance of the **Notepad Editor** will appear in the **Notes & Attachments** pane. To edit a note, click the wrench icon () for the note you want to edit.
  - To add an attachment to a note, click the paperclip icon (), and then click the **[Browse]** button to choose the file you want to attach to the note.

7. Click the **[Save]** button to save the new ticket.
   - The new ticket will appear in the **Ticket Console** page. The ***Element Name*** column will contain the name of the organization.
   - The new ticket will also appear in the **[Tickets]** tab, in the **Organizational Tickets** page of the **Organizational Administration** panel.

NOTE: After clicking the **[Save]** button, the **Ticket Editor** will appear. In this page, you can define additional fields for the ticket.

Viewing Logs for an Organization

SL1 creates a log for each organization. Each organization log displays a record of all actions pertaining to the organization. These actions include:

- All logins by organization members.
- All notifications sent to organization members.

- Organization member creating, editing, or deleting anything in SL1.
- All events associated with an entity managed by the organization.

The **Organizational Administration** panel includes an **Organizational Logs** page, where you can view the entries for a specific organization. The **Organizational Logs** page provides a complete audit trail for an organization.

To view the **Organizational Logs** page for an organization:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization you are interested in. Click its wrench icon ()
3. When the **Organizational Summary** page appears, click the **[Logs]** tab.
4. The **Organizational Logs** page appears. In this page, you can view the log entries for an organization. You can also search for log entries and flag log entries.
5. The **Organizational Logs** page displays the following for each log entry:

    - ***Date***. Date the action occurred and the log entry was created.
    - ***Source***. Source of the log entry.
    - ***Message***. Text of the log entry.
    - ***Flag***. Clicking on the flag checkmark changes the checkmark from red to black and appends the user's username to the checkmark. This aids in quickly finding the log entry.

Associating Products with an Organization

In SL1, products are associated with SKUs. A SKU is a unique identifier for each of the distinct products or services that can be ordered from a supplier. SKUs can be associated with both actual physical items for sale and also with billable services. For example, many providers use product SKUs to bill customers for services and bandwidth usage.

In SL1, you can define product SKUs in the **Product Catalog** (Registry > Business Services > Product Catalog). You can associate each new product SKU with an SL1 entity type. Those product SKUs that have a Type of "Organization" can be associated with organizations.

When you associate a product SKU with a specific organization, that association appears both in the **Organization Properties** page and in the **Product Subscription Manager** page (Registry > Business Services > Product Subscriptions). You can later use that association to define a billing policy for that organization.

To associate a product SKU with an organization:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization to which you want to assign a product SKU. Click the wrench icon () for that organization.
3. From the **Organizational Summary** page (or any page in the Organizational Administration tools), click the **[Actions]** menu.
4. From the **[Actions]** menu, select ***Product Catalog***.

5. The **Product Catalog** modal page appears. This page displays products that have already been associated with the organization and products that are available to be associated with the organization.
6. To associate an Available Product with the organization, select its checkbox. Click the **[Save]** button.

    - In the **Product Catalog** modal page, the selected product should now appear under the **Active Product Subscriptions** pane.
    - In the **Organization Properties** page, you should now see the product SKU listed under the **Product Usage List** pane.

Adding an Alternate Location to an Organization

If your organization has multiple offices or facilities, you might want to include information about those other locations in the **Organizational Administration** tools for the organization.

To add information about alternate locations for a specific organization:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization to which you want to add alternate locations. Click the wrench icon () for that organization.
3. From the **Organizational Summary** page (or any page in the Organizational Administration tools), click the **[Actions]** menu.
4. From the **[Actions]** menu, select ***Alternate Locations***.
5. The **Alternate Locations** modal page appears.
6. In the **Alternate Locations** modal page, you can enter the address and contact information about the alternate location. Click the **[Save]** button to save the alternate location.
7. Click the **[Properties]** tab. In the **Organization Properties** page, you should see the alternate location listed under **Organizational Alternate Locations** pane.

Adding a Note to an Organization

You can add notes to be stored in the Organizational Administration tools. These notes can include links, images, videos, and attachments. The **Notepad Editor** allows you to insert and edit content from saved templates, and format the paragraphs and fonts used in the note.

To create a note for an organization:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization where you want to add a note. Click the wrench icon () for that organization.
3. From the **Organizational Summary** page (or any page in the Organizational Administration tools), click the **[Actions]** menu.
4. From the **[Actions]** menu, select ***Notepad Editor***.
5. The **Notepad Editor** modal page appears.

6. Enter your note in the body of the editor. You can use the editor to include links, images, or videos in the message. You can also use the editor to insert content from a saved template and format the text of your note. You can use the field at the bottom of the editor to attach files to the note.
7. Click the **[Save]** button to save the note.
8. After saving, the note will appear in the **Organizational Notes** page for the organization.

Viewing an Organization in Google Earth

Google Earth allows you to view maps, satellite images, terrain, and photos of any location on earth.

The **Organizational Administration** tools allow you to view the address for an organization in the Google Earth application.

To configure your organization to be viewed with the Google Earth application:

1. Make sure you have installed Google Earth on the local computer.
2. Log in to SL1 and go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
3. In the **Organizational Account Administration** page, find the organization that you want to view in Google Earth. Click the wrench icon () for that organization.
4. Click the **[Properties]** tab.
5. Click the **[Actions]** menu. From the **[Actions]** menu, select ***Geolocate Coordinates***.
6. You should now see values in the *Longitude* and *Latitude* fields. Click the **[Save]** button to save the coordinates.
7. Click the **[Close]** tab to exit the **Organizational Administration** panel.
8. In the **Organizational Account Administration** page, click the earth icon () for the organization that you want to view in Google Earth.
9. SL1 generates a .KML file for the address for the organization. The .KML file contains the location of the organization, based on the address and the correlating latitude and longitude in the **Organization Properties** page.
10. You can save the .KML file to open later with Google Earth or you can select to open the file immediately.

Chapter 4

Customizing the Organization Administration Panel

Overview

This chapter shows you how to customize the **Organization Administration** panel by creating tabbed forms, defining custom tabs, and defining field entries in the Select Objects editor.

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:

Custom Navigation

You can define a custom tab to include in the **Organizational Administration** panel for a specific organization. This custom tab can include one or more links. Each link can lead to an internal page in SL1 or to an external URL or URI. For example, you could define a custom tab for your organization that leads to a SharePoint website for your group. Or you could include a custom tab for your organization that leads to a content management page for your enterprise.

The following sections will describe how to define and manage custom navigation for an organization.

Defining Custom Navigation

To define a custom tab for a selected organization:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization where you want to add a custom tab. Click the wrench icon () for that organization.
3. From the **Organizational Summary** page (or any page in the Organizational Administration tools), click the **[Actions]** menu.
4. In the **[Actions]** menu, select ***Custom Navigation***.
5. The **Custom Navigation** modal page appears.
6. In the **Custom Navigation** modal page, supply a value in the following fields:

    - ***Title (Shown on Tab)***. Enter a name for the tab. This name will appear on a new tab in the Organizational Administration tools for this organization.
    - ***Limit Access***. Users who will be allowed to access the custom tab, based on the type of user account. The choices are:

        - *Administrators*. Only users with account type "Administrator" are allowed to access this tab.
        - *Users*. Both users with account type "User" and users with account type "Administrator" are allowed to access this tab.

    - ***External URL / URI Link***. The URL of the page that is displayed when a user clicks the tab. The page can be an internal page in SL1 or an external web page. This field can contain any combination of alphanumeric characters, with a maximum length of 128 characters. Forward slash (/), underscore (_), and question mark (?) are allowed.

7. Click the **[Save]** button. The new tab appears in the **Organizational Administration** panel for the organization. Clicking the tab spawns a new browser page, opened to the URL associated with the tab.

Editing or Deleting Custom Navigation

After you have defined one or more custom tabs in the **Organizational Administration** panel for an organization, you can return to the **Custom Navigation** modal page to edit the custom tabs.

To edit a custom tab:

1. Go to **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization where you want to edit a custom tab. Click the wrench icon () for that organization.
3. From the **Organizational Summary** page (or any page in the Organizational Administration tools), click the **[Actions]** menu.
4. In the **[Actions]** menu, select ***Custom Navigation***.
5. The **Custom Navigation** modal page appears.
6. Go to the **Register** pane. Find the custom tab you want to edit. Click its wrench icon ().
7. The fields in the top pane will be populated with values from the selected custom tab.
8. You can edit the values in one or more fields. Click the **[Save]** button to save your changes to the custom tab.
9. To delete a custom tab, click its bomb icon ().

Tabbed Forms

Tabbed forms allow you to add a new page to the **Organizational Administration** panel for all organizations. The new page will have its own tab and can contain one or more custom fields.

The following sections describe how to define, edit, or delete a tabbed form.

Defining a Tabbed Form

To create a new tabbed page for the **Organizational Administration** panel:

1. Go to the **Application Forms** page (System > Customize > Form Fields).
2. In the **Application Forms** page, click the **[Create]** button.
3. The **Form Create** modal page appears.
4. Supply values in the following fields:
    - ***GUI Type***. Select *Tabbed*.
    - ***Form Type***. Select *Organization*.
    - ***Description***. Description of the custom form. This description is not displayed in the form.
    - **[Create]**. Click this button to create the new form
5. In the **Application Forms** page, click the **[Reset]** button to update the page.
6. In the **Tabbed Application Forms** pane, find the new tabbed form. Click its wrench icon ().
7. The **Form Creator** page appears.
8. The **Form Creator** page allows you to define the type and position of fields to include in the new tabbed

page and the guide text that will be associated with the new page.

9. To define or edit a tabbed form, perform the following:

    - ***Form Name/Description***. Contains the description you entered when you created the form in the **Form Create** modal page. You can edit this value.
    - ***Tab Label***. Enter the text you want to appear on the tab in the **Organizational Administration** panel.
    - Select the type of field to embed in the page. Double click on the field-type to add it to the pane to the right. The choices are:

        - ***VarChar32***. The field will accept up to 32 alphanumeric characters.
        - ***VarChar48***. The field will accept up to 48 alphanumeric characters.
        - ***VarChar64***. The field will accept up to 64 alphanumeric characters.
        - ***Float***. The field will accept numeric values with decimal points.
        - ***Drop-Down***. The field will be a drop-down list. You can populate the drop-down list in the **Select Objects Editor** page (System > Customize > Select Objects).
        - ***Checkbox***. The field will be a checkbox.
        - ***Textbox***. The field displays read-only text.
        - ***Password***. Data entered into this field will be represented as asterisks.
        - ***Phone Number***. The field will accept a phone number. Users can include parentheses around the area code, but cannot include spaces.
        - ***Email Address***. The field will accept a fully-qualified email address.
        - ***Web Address***. The field will accept a fully-qualified URL.
        - ***Date***. The field will allow users to select a date.
        - ***Date & Time***. This field allows the user to select a date and time.

10. Repeat step #9 for each field you want to embed in the new tabbed page.
11. You can define the following extra parameters for each field you want to embed:

    - ***Required***. The user must provide a value in this field.
    - ***Not Null***. The user most provide a non-null value in this field.

12. Use the Drag & Drop icon () to order the fields as you want them to appear in the page.
13. Use the Delete icon () to delete a field.
14. To restrict which users can edit a field, click the lock icon () for that field. The **Key Selection** pop-up will appear:

    - In the drop-down list, select an Access Key. To edit the field, a user must be granted the access key that you select.

- Click the **[Save]** button to save your changes.
- Click the **[Close]** button to close the **Key Selection** pop-up.

15. Click the **[Save]** button to save the tabbed page.
16. The new tabbed page now appears in the **Organizational Administration** panel for every organization.

Editing a Tabbed Form

To edit a form:

1. Go to the **Application Forms** page (System > Customize > Form Fields).
2. In the **Application Forms** page, find the application form you want to edit. Click its wrench icon ().
3. The **Form Creator** page appears.
4. In the **Form Creator** page, you can delete, edit, or add fields to the form or change the position of the fields.
5. In the **Form Creator** page, click the **[Save]** button to save your changes.

Deleting a Tabbed Form

1. Go to the **Application Forms** page (System > Customize > Form Fields).
2. In the **Application Forms** page, find the tabbed form you want to delete.
3. Click its bomb icon ().

Navigation Tab

You can define a custom tab to include in the Organizational Administration panel for all organizations (or you can select one or more organizations). This custom tab can include one or more links that would be useful for all organizations. Each link can lead to an internal page in SL1 or to an external URL or URI. For example, you could define a custom tab for your organization that leads to a content management page for your enterprise or to an external control panel.

The following sections describe how to define and manage a navigation tab for one, multiple, or all organizations.

Defining a Navigation Tab

To create a tab in the **Organization Administration** panel for one, multiple, or all organizations:

1. Go to the**Navigation Tab Editor** page (System > Customize > Navigation Tabs).
2. In the **Navigation Tab Editor** page, click the **[Reset]** button to clear any fields from the **Editor** pane.
3. In the **Editor** pane (at the top of the page), supply a value in each field:

    - ***Navigation Tab Location***. Specifies whether to display the new tab as a top-level tab in SL1 or as part of the **Organization Administration** panel. Select *Entity Page(s)*.

- ***Navigation Tab Title***. Tab's label. This is the text that users see on the tab.
- ***Link Type***. For future use. Select *standard*.
- ***Always Visible***. Specifies whether or not users who are not allowed to access the tab are able to view the tab in SL1. Choices are:
    - *No*. Tab does not appear in the product for users who do not have the appropriate permission keys to access the tab.
    - *Yes*. Tab always appears in the product and will be visible to users who do not have the appropriate permission keys to access the tab.
- ***Display For***. Specify the area in SL1 where you want to the tab to appear. Select *Organization*. The new tab appears in the **Organizational Administration** panel.
- ***Organizations***. Select which organizations display the new tab. You can choose to display the new tab in the **Organization Administration** panel for all organizations, for one organization, or for multiple organizations.
    - To select all organizations, select *All Organizations*.
    - To select a single organization, highlight it.
    - To select multiple organizations, left-click while holding down the **<Shift>** key.
- ***Access***. Specify which users are allowed to access the tab, based on the type of user account. Choices are:
    - *Administrators*. Only users with account type "administrator" are allowed to access this tab.
    - *Users*. Both users with account type "user" and users with account type "administrator" are allowed to access this tab.
- ***Permission Keys***. Select one or more Permission Keys in this field. To access the tab, a regular user must be granted at least one of the selected Permission Keys. Permission Keys define the tabs and pages users have access to and the actions that a user may perform. The SL1 system administrator defines these Permission Keys from the **Access Keys** page (System > Manage > Access Keys). Administrators always have access to the tab, regardless of the Permission Keys you select in this field.
- ***Target***. Specifies how the browser will open the URL. Choices are:
    - *_blank*. The browser opens the URL in a new window.
    - *_self*. The browser opens the URL in the current window.
    - *zoombox*. The browser opens the URL in a modal window.
    - *iframe*. The browser opens the URL in the pane below the header and top-level navigation tabs.
- ***URL/Link***. Full URL or link for the page that will be displayed in the tab. This field can contain any combination of alphanumeric characters, with a maximum length of 128 characters. Forward-slash (/), underscore (_), and question-mark (?) are allowed.

4. Click the **[Save]** button to save the new tab.
5. The new tab appears in the **Tab Registry** pane (at the bottom of the page).
6. The new tab also appears in the **Organizational Administration** panel for each selected organization. Click the tab to display the specified URL or link.

Editing a Navigation Tab

From the **Navigation Tab Editor** page, you can edit one or more parameters for a tab. To do this:

1. Go to the **Navigation Tab Editor** page (System > Customize > Navigation Tabs).
2. In the **Navigation Tab Editor** page, go to the **Tab Registry** pane (at the bottom of the page). Find the tab you want to edit. Click its wrench icon ( ).
3. The fields in the editor pane (at the top of the pane) are populated with values from the selected tab. You can edit the values in one or more fields:
4. Click the **[Save]** button to save your changes to the tab.

Deleting a Navigation Tab

In the **Navigation Tab Editor** page, you can delete a custom tab. To do this:

1. Go to the **Navigation Tab Editor** page (System > Customize > Navigation Tabs).
2. In the **Navigation Tab Editor** page, go to the **Tab Registry** pane (at the bottom of the page).
3. Find the tab you want to delete. Click its bomb icon ( ).

Select Objects

The **Select Objects Editor** page allows you to define and edit the entries that appear in drop-down lists throughout SL1. For example, you can define the list of entries that appear in the ***Cause*** field that appear when a user resolves a ticket. The user then selects one of the entries (for example, hardware failure) when resolving the ticket.

You can use the **Select Objects Editor** page to customize the following fields that appear in the **Organizational Administration** panel:

- ***Critical Contact*** field in the **Account Permissions** page.
- ***Key Role*** field in the **Account Permissions** page.

Both fields appear in the **Critical Contact** pane in the **Organization Properties** page.

The following sections describe how to define, edit, and delete select objects.

Defining an Entry for a Select Object

To create a new entry for the ***Critical Contact*** drop-down field or ***Key Role*** drop-down field:

1. Go to the **Select Objects Editor** page (System > Customize > Select Objects).
2. In the **Select Objects Editor** page, click the **[Reset]** button to clear any values from the **Editor** pane.
3. In the **[Filter]** drop-down list, select:
    - *Organization: Critical Contact*
    - *Organization: Role*
4. The **Registry** pane displays a list of all the existing entries in that drop-down field.
5. In the **Editor** pane, you can enter an additional value in the ***Definition/Value*** field. Click the **[Add]** button to save the new entry.
6. The new entry will now appear as an entry in that drop-down field for all users.

Editing an Entry for a Select Object

In the **Select Objects Editor** page, you can edit an entry in a drop-down list. To edit an entry in a drop-down list:

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 the page and drop-down field that you want to edit (either *Organization: Critical Contact* or *Organization:Role*).
3. The **Select Objects Registry** pane displays all the entries defined for the selected drop-down field. Find the entry you want to edit and click its wrench icon ().
4. The **Editor** pane (at the top of the page) is populated with values from the entry you selected. You can edit the following fields:
    - ***Definition/Value***. The entry that appears in the drop-down field.
    - ***Deprecate***. If you select this checkbox, the current entry will no longer appear in the drop-down list for its field. In instances of a page where this entry is already selected, the entry will still appear as the selected value for its field. In instances of a page where this entry is not selected, it will no longer appear in the drop-down list for its field.
5. Click the **[Save]** button to save your changes.

Deleting an Entry for a Select Object

In the **Select Objects Editor** page, you can delete an entry for a drop-down field. To delete an entry in a 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 field to select the page and drop-down field that you want to edit.
3. The **Select Objects Registry** pane displays all the entries defined for the selected drop-down field. Find the entry you want to delete and click its bomb icon ().

Chapter 5

Reports for Organizations

Overview

SL1 allows you to generate reports based on organizations. You can generate two types of reports about organizations:

- A report with overview information on multiple organizations in SL1.
- A report with detailed information on a single organization.

This chapter will describe how to generate each type of organization report.

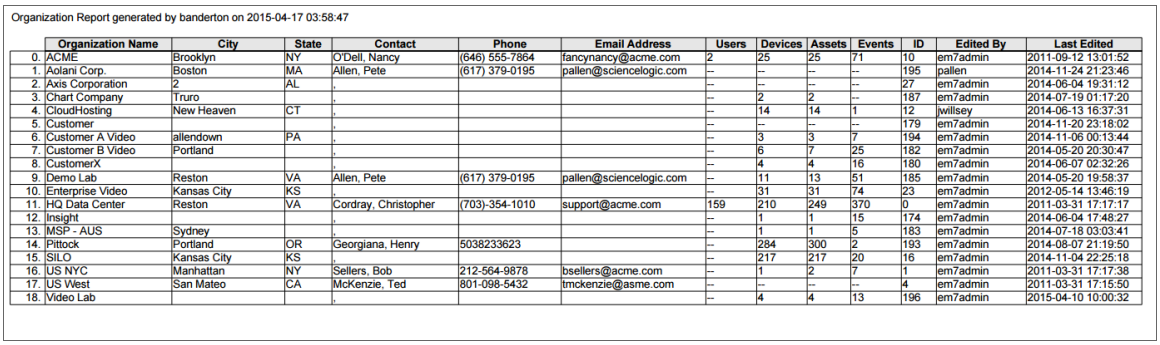
Use the following menu options to navigate the SL1 user interface:

- 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:

Generating a Report on Multiple Organizations in SL1

The **[Registry]** tab includes the **Organizational Account Administration** page (Registry > Accounts > Organizations). From the **Organizational Account Administration** page you can generate an Excel report that contains all the information in the **Organizational Account Administration** page, plus some additional information from the **Organization Properties** page for each organization.



Organization Report generated by banderton on 2015-04-17 03:58:47

	Organization Name	City	State	Contact	Phone	Email Address	Users	Devices	Assets	Events	ID	Edited By	Last Edited
0.	ACME	Brooklyn	NY	O'Dell, Nancy	(646) 555-7864	fancynancy@acme.com	2	25	25	71	10	em7admin	2011-09-12 13:01:52
1.	Aolani Corp.	Boston	MA	Allen, Pete	(617) 379-0195	pallen@sciencelogic.com	--	--	--	--	195	pallen	2014-11-24 21:23:46
2.	Axis Corporation	2	AL	.			--	--	--	--	27	em7admin	2014-06-04 19:31:12
3.	Chart Company	Truro		.			--	2	2	--	187	em7admin	2014-07-19 01:17:20
4.	CloudHosting	New Heaven	CT	.			--	14	14	1	12	jwillsey	2014-06-13 16:37:31
5.	Customer			.			--	--	--	--	179	em7admin	2014-11-20 23:18:02
6.	Customer A Video	allendown	PA	.			--	3	3	7	194	em7admin	2014-11-06 00:13:44
7.	Customer B Video	Portland		.			--	6	7	25	182	em7admin	2014-05-20 20:30:47
8.	CustomerX			.			--	4	4	16	180	em7admin	2014-06-07 02:32:26
9.	Demo Lab	Reston	VA	Allen, Pete	(617) 379-0195	pallen@sciencelogic.com	--	11	13	51	185	em7admin	2014-05-20 19:58:37
10.	Enterprise Video	Kansas City	KS	.			--	31	31	74	23	em7admin	2012-05-14 13:46:19
11.	HQ Data Center	Reston	VA	Cordray, Christopher	(703)-354-1010	support@acme.com	159	210	249	370	0	em7admin	2011-03-31 17:17:17
12.	Insight			.			--	1	1	15	174	em7admin	2014-06-04 17:48:27
13.	MSP - AUS	Sydney		.			--	1	1	5	183	em7admin	2014-07-18 03:03:41
14.	Pittock	Portland	OR	Georgiana, Henry	5038233623		--	284	300	2	193	em7admin	2014-08-07 21:19:50
15.	SILO	Kansas City	KS	.			--	217	217	20	16	em7admin	2014-11-04 22:25:18
16.	US NYC	Manhattan	NY	Sellers, Bob	212-564-9878	bsellers@acme.com	--	1	2	7	1	em7admin	2011-03-31 17:17:38
17.	US West	San Mateo	CA	McKenzie, Ted	801-098-5432	tmckenzie@asme.com	--	--	--	--	4	em7admin	2011-03-31 17:15:50
18.	Video Lab			.			--	4	4	13	196	em7admin	2015-04-10 10:00:32

To generate a report on all or multiple organizations in SL1:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. On the **Organizational Account Administration** page, click the **[Report]** button. The **Export current view as a report** modal page appears:

> **NOTE**: If you want to include only certain organizations in the report, use the "search as you type" fields at the top of each column. You can filter the list by one or more column headings. You can then click the **[Report]** button, and only the organizations displayed in the **Organizational Account Administration** page will appear in the report.

3. In the **Export current view as a report** page, you must select the format in which SL1 will generate the report. Your choices are:
   - Comma-separated values (.csv)
   - Web page (.html)
   - Open Document Spreadsheet (.ods)
   - Excel spreadsheet (.xlsx)
   - Acrobat document (.pdf)
4. Click the **[Generate]** button. The report will contain all the information displayed in the **Organizational Account Administration** page. You can immediately view the report or save it to a file for later viewing.

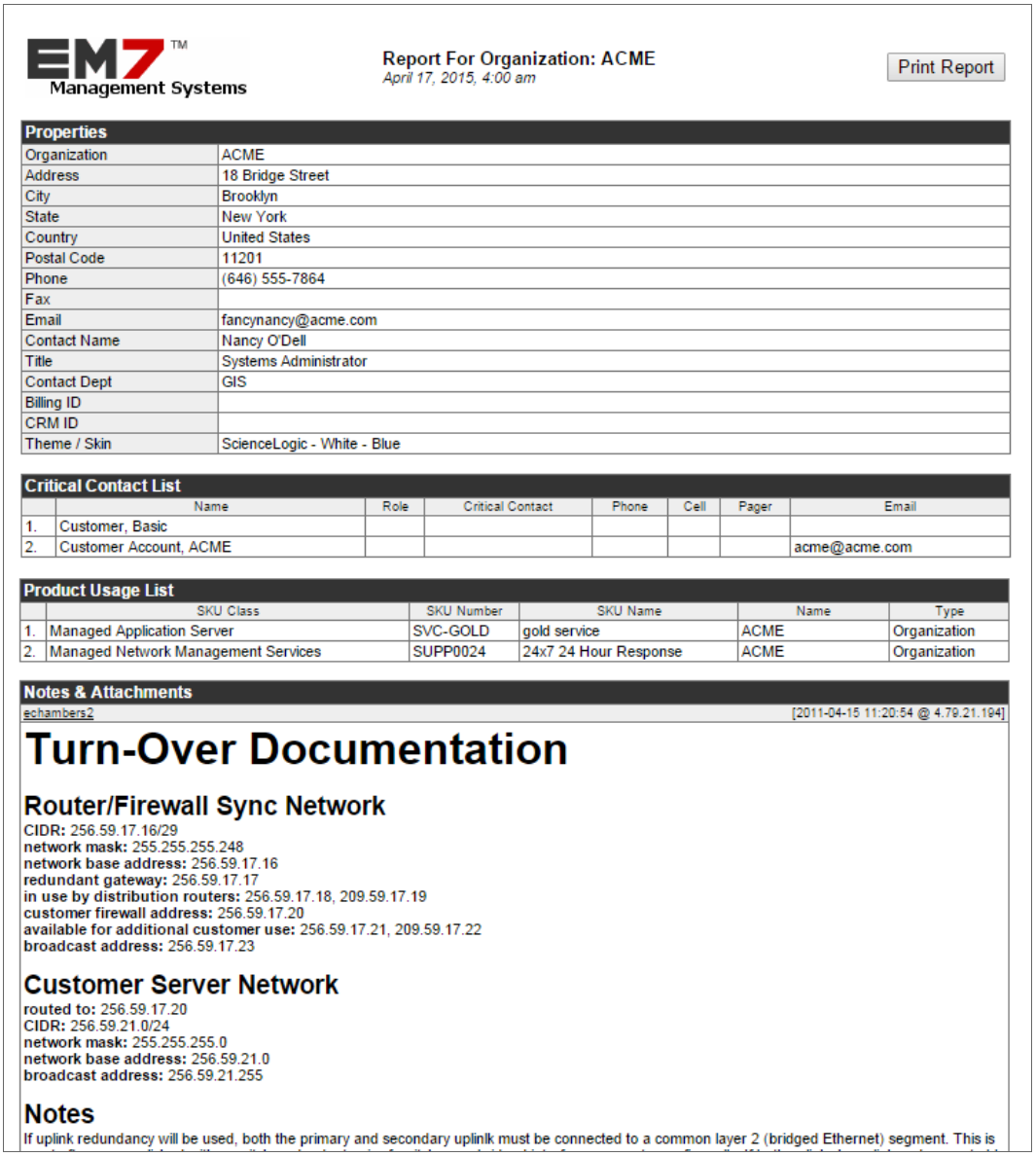
For each organization in SL1, this report displays:

- Organization ID

- Organization Name
- Address
- City
- State / Province
- Postal Code
- Country
- Contact's Last Name
- Contact's First Name
- Email
- Phone
- Fax
- Contact's Title
- Contact's Department
- Billing ID
- CRM ID
- Toll Free
- Number of User Accounts
- Number of Devices
- Number of Assets Records
- Number of Network Interfaces
- Date and Time of Last Edit

Detailed Report About a Single Organization

SL1 can generate a custom report about a single organization. You can specify the level or detail to include in the report and the output format for the report.



EM7 Management Systems

Report For Organization: ACME
April 17, 2015, 4:00 am

Print Report

Properties

Organization	ACME
Address	18 Bridge Street
City	Brooklyn
State	New York
Country	United States
Postal Code	11201
Phone	(646) 555-7864
Fax	
Email	fancynancy@acme.com
Contact Name	Nancy O'Dell
Title	Systems Administrator
Contact Dept	GIS
Billing ID	
CRM ID	
Theme / Skin	ScienceLogic - White - Blue

Critical Contact List

	Name	Role	Critical Contact	Phone	Cell	Pager	Email
1.	Customer, Basic						
2.	Customer Account, ACME						acme@acme.com

Product Usage List

	SKU Class	SKU Number	SKU Name	Name	Type
1.	Managed Application Server	SVC-GOLD	gold service	ACME	Organization
2.	Managed Network Management Services	SUPP0024	24x7 24 Hour Response	ACME	Organization

Notes & Attachments

echambers2 [2011-04-15 11:20:54 @ 4.79.21.194]

Turn-Over Documentation

Router/Firewall Sync Network

CIDR: 256.59.17.16/29
network mask: 255.255.255.248
network base address: 256.59.17.16
redundant gateway: 256.59.17.17
in use by distribution routers: 256.59.17.18, 209.59.17.19
customer firewall address: 256.59.17.20
available for additional customer use: 256.59.17.21, 209.59.17.22
broadcast address: 256.59.17.23

Customer Server Network

routed to: 256.59.17.20
CIDR: 256.59.21.0/24
network mask: 255.255.255.0
network base address: 256.59.21.0
broadcast address: 256.59.21.255

Notes

If uplink redundancy will be used, both the primary and secondary uplinlk must be connected to a common layer 2 (bridged Ethernet) segment. This is

To generate a detailed report about a single organization:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization you want to generate a report about.
3. Click its printer icon (). The **Report Creator** modal page appears. The **Report Creator** modal page allows you to generate an organization report. From the **Report Creator** modal page, you can specify which information to include in the report and the format in which the report will be generated.
4. You can select from the following list of formats in which the report can be generated:
    - Create Report as HTML Document
    - Create Report as PDF Document
    - Create Report as Open Document Spreadsheet
    - Create Report as MS Excel Document
5. You can select one of the following to specify the information to include in the report:
    - **[Full Report]**. Displays all the contact information (address, phone numbers, email, contact person) from the **Organization Properties** page plus any product SKUs associated with the organization and all notes and attachments for the organization, as displayed in the **Organizational Notes** page.
    - **[Partial]**. Displays all the contact information (address, phone numbers, email, contact person) plus any critical contact persons from the **Organization Properties** page.
    - **[Minimal]**. Displays only the address and contact information in the **Organization Properties** page.
    - **[Notes]**. Displays all notes and attachments for the organization from the **Organization Properties** page.
    - **[Contacts]**. Displays a list of all user accounts in the organization from the **Organization Properties** page.
    - **[Products]**. Displays a list of product SKUs associated with the organization from the **Organization Properties** page.
6. When you select the information to include the report, SL1 will generate the report. You can immediately view the report or save it to a file for later viewing.

Chapter 6

Understanding User Accounts

Overview

This chapter describes the types of user accounts, access keys and user policies, and how the latter two affect user accounts.

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 a User Account?

A user account allows you to access SL1 GUI. You access this GUI by opening a browser session and connecting to an Administration Portal. From the GUI, you can interact with SL1, view data, status, and reports, and define policies, as well as administer SL1.

Users and Organizations

For an overview of the relationship between an organization and its users, see the section on *Organizations and Their Relationships*.

Account Types

In SL1, there are two broad types of user accounts:

- ***Administrators***. By default, users of type "administrator" are granted all permissions available in SL1. Administrators can access all tabs and pages, and perform all actions and tasks on all entities, regardless of organization.
- ***Users***. Accounts of type "user" are assigned key privileges. Key privileges are customizable by the administrator and grant users access to pages and tabs and permit users to view information and perform tasks in SL1. These key privileges are defined by the SL1 system administrator from the **Access Keys** page (System > Manage > Access Keys).

To learn more about Access Keys and how they affect user accounts, see the ***Access Permissions*** manual.

An account of type "user" can be granted the privileges that allow him/her to create or modify other users' accounts. However, for accounts of type "user", certain restrictions apply:

- An account of type "user" cannot create or modify an account of type "administrator".
- An account of type "user" cannot change his/her own account to type "administrator" or change another user's account to type "administrator".
- An account of type "user" cannot add additional Access Keys to his/her own account.
- An account of type "user" cannot grant or remove Access Keys to other accounts that he/she has not also been granted.

Regardless of access keys, ***accounts of type "user" can access only pages and actions associated with their organization***. For example:

- Suppose your organization includes three regional offices. Suppose you define three organizations: Northeast, Headquarters, and West Coast.
- Suppose each organization includes the hardware located at the corresponding office.

- Now suppose the account "JohnDoe" is of type "user" and is a member of the organization "West Coast". User JohnDoe would be able to view and act upon only devices that are included in the organization "West Coast". User JohnDoe would not be able to view or act upon the hardware at the other offices.
- ***SL1 allows you to assign each user a primary organization and optional additional organizations***.
- Now suppose that user "JohnDoe" needs to view the status of a device at headquarters. If you add "Headquarters" as a secondary organization in JohnDoe's account information, that user will now be able to view and act upon all the devices in the "Headquarters" organization.

> **NOTE**: You can use Access Keys to further limit the access of each user, even within his/her own organization.

Organizations also affect credentials. To support multi-tenancy, SL1 allows credentials to be aligned with organizations.

- For each credential that is aligned with an organization, only administrators and users who are members of the aligned organization will be able to see the credential in the **Credential Management** page.
- In SL1, in any field or column that displays the name of the credential, users who are not members of the aligned organization will not see the credential name. Instead, these users will see either a dash character (-) or the text "Restricted Credential".
- In SL1, in any list from which users can select a credential, users who are not members of the aligned organization will not see the credential as an entry in the list.

To learn more about credentials, see the manual ***Discovery and Credentials***.

Understanding Access Keys

There are two broad types of user accounts: administrators and users.

By default, users of type "administrator" are granted all permissions available in SL1. Administrators can access all tabs and pages and perform all actions and tasks.

Accounts of type "user" are assigned privileges. These privileges are defined by the SL1 system administrator in the **Access Keys** page (System > Manage > Access Keys). ***Access Keys*** are customizable by the administrator, grant users access to pages and tabs, and permit users to view information and perform tasks in SL1.

Access Keys control the pages a user can navigate to and the actions the user can perform in each page. For details on access keys, see the manual entitled ***Access Permissions***.

Understanding User Policies

User Policies allow you to define a custom set of account properties and privileges (from the **Account Permissions** page) 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.

A user policy allows you to define:

- Login State
- Authentication Method
- Ticket Queue Memberships
- Primary Organization and Additional Organization Memberships
- Theme
- Time Zone
- Privilege Keys

User Policies have a dynamic relationship with their member user accounts. You can make a change to a user policy and SL1 will automatically update the account settings for each member account.

For example:

- Suppose you create a user account called "John Doe" on the first of the month and use the user policy named "NOC users" to create the user account.
- Suppose you create another user account called "Jane Smith" on the fifth of the month and again use the user policy "NOC users".
- Suppose on the 15th of the month, you add an additional Key Privilege to the "NOC users" policy.
- That additional Key Privilege will appear in the account for John Doe and Jane Smith as soon as the "NOC users" policy is saved.

If you create a user account with a user policy, the fields in the **Account Permissions** page for that user account are grayed out. If you want to manually edit fields in the **Account Permissions** page for the user account, you must disassociate the user account from the user policy. Any future changes made to the user policy will not appear in the disassociated user account.

If you want to automatically import user accounts from LDAP or Active Directory, you must create at least one user policy. To use user policies in this way, special configuration is required. This configuration is described in the manual ***Using LDAP or Active Directory***.

For details on creating a user policy, see the section on ***user policies***.

Understanding User Sessions

SL1 lets multiple users log into the same SL1 system at the same time. The time a user spends logged into SL1 is known as a ***user session***. You can end a user's session in SL1, and you can also limit the number of users that can be simultaneously logged into an SL1 system.

The **Access Sessions** page allows administrators to monitor user logins and logouts to the user interface.

From this page, you can also:

- End a user's session.
- View a list of accounts that are locked out of the user interface due to invalid username and password.
- Unlock accounts that are locked out of the user interface.

Viewing Information about Each Access Session

The **Access Sessions** page displays a list of recent logins to the user interface. To view the **Access Sessions** page:

1. Go to the **Access Sessions** page (System > Monitor > Access Logs).
2. For each session, the **Access Sessions** page displays:
    - ***User Account***. Username of person logging in to the user interface.
    - ***User Display Name***. The username, email address, or preferred display name. This value is determined by the user's authentication resource settings.
    - ***Last Address***. IP address from which the user accessed the user interface.
    - ***State***. Current status of the user. The choices are:
        - *Active*. User is currently logged in to the user interface.
        - *Expired*. User's session in the user interface was killed.
        - *Logged Out*. User logged out of the user interface.
        - *Never Used*. User logged in to the user interface and did not perform any tasks before the session was killed.
    - ***Login Time***. Date and time at which the user logged in.
    - ***Last-Hit Time***. Date and time at which the user last loaded a page in the user interface.
    - ***Logout Time***. Date and time at which the user logged out.
    - ***Session Duration***. Length of time between login and logout.

Deleting a User's Session

From the **Access Sessions** page, you can end a user's session in the user interface. The user must log in again to access the user interface. The status of the session will be "expired".

To end a user's session:

1. Go to the **Access Sessions** page (System > Monitor > Access Logs).
2. In the **Access Sessions** page, find the session you want to end. Click the checkbox (☑) for that session.
3. Click the ***Select Actions*** field (in the lower right of the page) and then select *Kill user session*. Click the **[Go]** button
4. Each selected session is ended. The user associated with each selected session is logged out of the user interface. The status of the session changes to "expired".

NOTE: After ending a user's session, that user can immediately log in to the user interface again. To prevent a user from logging in to the user interface, you must disable the user's account. For information on user accounts, see the manual ***Organizations and Users***.

Limiting the Number of Simultaneous User Sessions

If you get an "HTTP Response code was 429 (Too Many Requests)" error or a "User sessions at maximum" in SL1, you can adjust the **USER_MAX_SESSIONS** value in the **/opt/em7/nextui/nextui.conf** file:

1. SSH to the SL1 appliance and log in as user *em7admin*.
2. At the command line, open the nextui.conf file in the vi editor:

```
sudo vi /opt/em7/nextui/nextui.conf
```

3. In the NextUI configuration file, set a new value for **USER_MAX_SESSIONS**, such as **USER_MAX_SESSIONS=1000** for 1,000 concurrent user sessions.
4. Save your changes and restart the NextUI service:

```
sudo systemctl restart nextui
```

Viewing Lockouts and Unlocking Lockouts

If a user enters incorrect login information multiple times in a row, that username, the user's IP address, or both will be locked out of the user interface.

To view lockouts or restore login privileges to locked out users:

1. Go to the **Access Sessions** page (System > Monitor > Access Logs).
2. In the **Access Sessions** page, click the **[Lockouts]** button.
3. The **Account Lockouts** modal page allows administrators to view a list of locked-out accounts and to restore login privileges to locked out users.
4. The **Account Lockouts** modal page displays the following about each lockout:
   - ***Attempt Account***. Username that caused the lockout.
   - ***From Address***. IP address from which the failed login attempts originated.
   - ***Attempt Time***. Date and time at which lockout occurred.
   - ***Tries***. Number of times user tried to log in to the user interface.
5. ***To remove the lock for the user account*** and allow logins from the username and/or IP address, click the bomb icon ( ).

Global Settings for Lockouts

The platform includes global settings that define how lockouts behave. In the **Behavior Settings** page (System > Settings > Behavior), the following fields affect lock-outs:

- *Account Lockout Type*
- *Account Lockout Attempts*
- *Account Lockout Duration*
- *Lockout Contact Information*

Audit Logs

For additional information about users and their actions in the platform, you can view the **Audit Logs** page. The **Audit Logs** page provides a complete audit trail for the platform. The **Audit Logs** page displays a record of all actions in the platform that are generated by users or by managed elements. For details, see the section on *Audit Logs*.

Understanding Authentication

Authentication is the method by which SL1 determines if a user can access the SL1 system. There are three methods of authentication:

- *EM7 Session*. An administrator must define the user account in SL1. The user account has a username and password. During login, SL1 checks its own databases to make sure the username and password are legitimate and accurate.
- *LDAP/Active Directory*. If the user has an account in Active Directory or on an LDAP server, the user can log in to SL1 with the AD or LDAP username and password. SL1 will communicate with Active Directory or the LDAP server to determine if the username and password are legitimate and accurate.
- *SSO Authentication*. If the user has a Single Sign-On (SSO) account, the user can enter a URL to access SL1. A SAML IdP will authenticate the user with the user's browser acting as an intermediary. If the user is already logged in to the SAML IdP, SL1 will display the default page for the user. If the user is not yet logged in to the SAML IdP, the user will be prompted to log in to the SAML IdP and then redirected to the default page in SL1.

NOTE: To use Active Directory authentication or LDAP authentication, special configuration is required. For details, see the manual *Using LDAP or Active Directory*.

NOTE: To use SSO authentication, special configuration is required. For details on configuring SL1 to use SSO authentication, see the manual on using *Using Single Sign-On*.

Chapter 7

Creating and Editing User Accounts

Overview

This chapter will show you how to create and edit user accounts in SL1, and will also show you examples of user accounts created 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:

Before Deployment

Before deployment, an administrator must determine:

- Which team members require access to SL1.
- What access levels to assign to each team member.
- Which organization to place each team member in, so that each team member will have access to required device information.

After you have devised a plan, you can start adding user accounts to SL1.

Best Practices

When creating user accounts, ScienceLogic suggests you use the following best practices:

- Limit the number of user accounts of type "administrator" to those who absolutely require full access to SL1.
- Use care when assigning Access Keys to individual users and user policies. You should assign each user only the access that he/she requires to perform his/her job duties.
- Use care when updating user policies that have already been used to create user accounts. Remember that each change is dynamically added to each member's user account.
- Follow guidelines for creating a strong password, including:
    - Is at least eight characters long.
    - Does not contain your username, real name, or company name.
    - Cannot be found in a dictionary.
    - Is significantly different from previous passwords. Passwords that increment (Password1, Password2, Password3) are not strong.
    - Contains a mixture of uppercase and lowercase letters, numerals, and non-alphanumeric characters.

Viewing a List of User Accounts

From the **User Accounts** page, you can view a list of all existing user accounts in SL1. From this page, you can also define new user accounts and edit existing user accounts.

To access the **User Accounts** page:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. For each account, the **User Accounts** page displays:
    - ***Username***. The username used to log in to SL1.
    - ***User Display Name***. The user's name as it appears throughout SL1 and in logs. This value is determined by the user's authentication resource settings.

- ***Last Name, First Name***. The user's last name and first name. The icon to the left of the column specifies the account type.
- ***Account Type***. The user's account type. Choices are User or Administrator.
- ***User Policy***. *User policy* associated with the user's account, if applicable.
- ***Primary Organization***. The organization that the user belongs to.
- ***Email Address***. The user's email address.
- ***State***. Can be one of the following:
  - *Active*. User can log in.
  - *Suspended*. User cannot log in.
  - *Vacation*. User can log in, but SL1 will not send any automated email notifications to the user's email address(es).
- ***Auth Type***. Specifies how the account is authenticated:
  - *EM7*. Account is authenticated through account-definition on SL1.
  - *LDAP/AD*. Account is authenticated through an external LDAP or AD server.
  - *SSO*. Account is authenticated through an external SSO provider.
- ***User ID***. Unique numeric ID assigned to each user by SL1.
- ***Edited By***. User who created or last edited the user account.
- ***Last Edited***. The date and time the account was created or last edited.

TIP: You can filter the items on this page by typing filter text or selecting filter options in one or more of the filters found above the columns on the page.

Manually Creating a New User Account

There are four ways to create a new user account in SL1:

- Manually create the account and supply values in each field. This method is described in this section.
- Manually create the account and align the account with a user policy (instead of supplying values in each field).
- Automatically importing LDAP or Active Directory accounts into SL1. This is described in the ***Using LDAP or Active Directory*** manual.
- Automatically importing SSO accounts into SL1. This is described in the ***Using Single Sign-On (SSO)*** manual.

To manually create a new user account:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. In the **User Accounts** page, click the **[Create]** button. The **Create New Account** page appears.
3. In the **Create New Account** page, enter values in each field:
    - ***First Name***. User's first name. This value can be up to 24 characters in length.
    - ***Last Name***. User's last name. This value can be up to 24 characters in length.
    - ***Generate name based on first and last name***. If you select this checkbox, SL1 will generate a login name for the user. ScienceLogic recommends that you do not select this option.
    - ***Account Login Name***. User's login name. This field can be up to 32 characters in length.
    - ***Primary Email***. User's email address. This field can be up to 64 characters in length.
    - ***Password***. The user's password. This value must meet the requirements specified for the value you select in the ***Password Strength*** field set in the **Behavior Settings** page (System > Settings > Behavior).
    - ***Confirm Password***. The user's password again. This value must be identical to the value you specified in the ***Password*** field.
    - ***Password Strength***. When defining or editing a user account, the administrator can define the required password strength. The user must then always use a password that meets or exceeds that specified password strength. SL1 will not allow the user to save changes to his or her password that do not meet the password strength requirement. Choices are:
        - *Good*. Password must be at least eight characters long and contain at least one number or one symbol.
        - *Strong*. Password must be at least eight characters long and contain at least one number and at least one symbol.
        - *Very Strong*. Password must be at least 13 characters long, contain no repeated characters, and contain at least one number and at least one symbol. Recommended.
    - ***Password Expiration***. Specifies whether or not the password for this account will expire and if so, when the password will expire. Choices are:
        - *Disabled*. Password does not expire.
        - *30 Days*. When the current password is 30 days old, during login the user will be prompted to change the password.
        - *60 Days*. When the current password is 60 days old, during login the user will be prompted to change the password.
        - *90 Days*. When the current password is 90 days old, during login the user will be prompted to change the password. Recommended.
        - *180 Days*. When the current password is 180 days old, during login the user will be prompted to change the password.

If the password is set to expire, on the expiration date the user will be prompted to change the password at the Login page. The user will be required to enter his/her old password and then enter a new password twice. If the user incorrectly enters the previous password or enters an invalid new password, the user will not be allowed to log in to SL1.

The new password must meet the requirements of the ***Password Strength*** field and the ***Password Shadowing*** field. SL1 will prompt the user to meet these requirements and display a description of those requirements.

NOTE: The value in the ***Password Expiration*** field in this page (the **Account Permissions** page) overrides the value in the **Behavior Settings** page (System > Settings > Behavior).

- ***Password Shadowing***. Specifies requirements for password reuse. By default, when a user defines a new password, he/she cannot reuse any passwords that he/she has used in the last 12 months. The choices in this field are:
    - *Default - cannot reuse passwords from past year*
    - *1 - Cannot reuse last password*
    - *2 - Cannot reuse last 2 passwords*
    - *3 - Cannot reuse last 3 passwords*
    - *4 - Cannot reuse last 4 passwords*
    - *5 - Cannot reuse last 5 passwords*
    - *6 - Cannot reuse last 6 passwords*
    - *7 - Cannot reuse last 7 passwords*
    - *8 - Cannot reuse last 8 passwords*
    - *9 - Cannot reuse last 9 passwords*
    - *10 - Cannot reuse last 10 passwords*
- ***Require Password Reset***. If selected, the user will be prompted to change his or her password at the next login. When creating a new user account, this option is selected by default. After the user's first login, when he or she is prompted to change his or her password, this option is then unselected.
- ***Multi-Factor Auth (MFA) User***. If this user requires a different user name for Multi-factor authentication, enter the MFA user name in this field.

NOTE: For details on configuring multi-factor authentication, see the manual ***Using Multi-Factor Authentication***the section on using multi-factor authentication.

- ***Organization***. The organization of which the new user account will be a member. Users can select from among all organizations in SL1.
- ***Account Type***. Specifies whether the user is a member of a user policy. Choices are:
    - *Individual*. User account is not a member of a user policy.
    - *Policy Membership*. User will be defined with a user policy. When selected, the *Policy Membership* field becomes active.
        - When a user policy is applied to a user's account, the user inherits the Key Privileges specified in the user policy. Administrators cannot add additional Key Privileges or delete Key Privileges from the user's account.
        - When a user policy is edited, each user account that is a member of that template will be dynamically updated.

  The second drop-down list contains an entry for each standard account type. These account types affect the list of Key Privileges for the user. The choices are:

    - *Administrator*. By default, administrators are granted all permissions available in SL1. Administrators can access all tabs and pages and perform all actions and tasks.
    - *User*. Accounts of type "user" are assigned key privileges. Key privileges are customizable by the administrator and grant users access to pages and tabs and permit users to view information and perform tasks in SL1. These key privileges are defined by the SL1 system administrator from the **Access Keys** page (System > Manage > Access Keys).
- ***Login State***. Initial login state for the user account. The choices are:
    - *Suspended*. Account is not active. User cannot log in to SL1.
    - *Active*. Account is active. User can log in to SL1.
    - *Vacation*. Account is active and the user can log in to SL1, but SL1 does not send email messages to the user.
- ***Authentication Method***. Specifies how the user will be authenticated. The choices are:
    - *EM7 Session*. User's username and password are authenticated by the database.
    - *LDAP/Active Directory*. User's username and password are authenticated by an LDAP server or Active Directory server. For details on configuring SL1 to use LDAP or Active Directory authentication, see the manual ***Using LDAP or Active Directory***.see the section on Using LDAP or Active Directory.

NOTE: For users who are authenticated with Single Sign-On (SSO), SL1 ignores the ***Authentication Method*** field. For details on configuring SL1 to use SSO authentication, see the manual on using ***Using Single Sign-On***.For details on configuring SL1 to use SSO authentication, see the section on using Using Single Sign-On (SSO).

- ***Restrict to IP***. The user will be allowed to access SL1 only from the specified IP address. Specify the IP address in standard dotted-decimal notation.
- ***Country***. Select the appropriate country to associate with the user account.
- ***Time Zone***. Select the appropriate time zone to associate with the user account.

NOTE: : By default, the ***Country*** field and ***Time Zone*** field will be set to the system-wide defaults defined in the **Behavior Settings** page (System > Settings > Behavior). You can override these values for the current user. Changing the default country or time zone for the current user will not affect the system-wide default settings.

NOTE: If the user account is aligned with a user policy that specifies a time zone, the ***Time Zone*** field will be disabled. The user account will use the Time Zone specified in the user policy and the ***Time Zone*** field cannot be edited.

- ***Autosync Time Zone With Local Settings***. Specifies whether SL1 should always use the time zone specified in the ***Time Zone*** field or if SL1 should adopt the local time zone (when it differs from the value in the ***Time Zone*** field). This is helpful for users who travel and use SL1 "on the road". Choices are:
  - *Yes*. If the value in the ***Time Zone*** field differs from the local time zone, SL1 should use the local time zone.
  - *No*. SL1 will continue to use the time zone specified in the Time Zone field, even if the local time zone differs.
- ***Policy Membership***. If you selected *Policy Membership* in the ***Account Type*** field, the *Policy Membership* field is activated. In this field, you can select a user policy to apply to the new user account.
  - When a user policy is applied to a user's account, the user inherits the Key Privileges specified in the user policy. Administrators cannot add additional Key Privileges or delete Key Privileges from the user's account.
  - When a user policy is edited, each user account that is a member of that policy will be dynamically updated.

4. Click the **[Save]** button to save the new user account.
5. The **Account Permissions** page appears, with some of the fields already populated with values from the **Create New Account** page.
6. An additional set of tabs appears. These tabs are the Account Panel tools. These tabs are described in the section on *Managing User Accounts*.

Password Strength

When defining or editing a user account, the administrator can define the required password strength. The user must then always use a password that meets or exceeds that specified password strength.

To determine password strength, SL1 uses the following scoring system:

- ***Too short*** = password is less than eight characters
- ***Bad password*** = same password as username
- ***Bad password*** = score less than 34
- ***Good password*** = score greater than 34 and less than 68. Minimum requirements are that the password must be at least eight characters long and contain at least one number or one symbol.
- ***Strong password*** = score greater than 68 and less than 100. Minimum requirements are that the password must be at least eight characters long and contain at least one number and at least one symbol.
- ***Very Strong password*** = score equal to or greater than 100, where password length is greater than 13 characters. Minimum requirements are that the password must be at least 13 characters long, contain no repeated characters, and contain at least one number and at least one symbol.

To generate a score for a password, SL1 uses the following scoring parameters:

- Base score for password length (password must contain at least eight characters) = password length * 4
- If password contains at least three numbers = +5
- If password contains at least two symbols = +5
- If password contains both uppercase and lowercase letters = +10
- If password contains a least one number and letters = +15
- If password contains at least one number and at least one symbol = +15
- If password contains letters and at least one symbol = +15
- If password is only numbers = -10
- If password is only letters = -10
- One repeated character in password = (1 - password length) (a negative value)
- Two repeated characters in password = (2 - password length) (a negative value)
- Three repeated characters in password = (3 - password length) (a negative value)

Using LDAP or Active Directory for Authentication

If you have already created accounts for users in SL1, you can use Active Directory or LDAP to authenticate one or more of those users. Each time an Active Directory or LDAP user logs in to SL1 using his/her Active Directory or LDAP username and password, SL1 will use Active Directory or LDAP to authenticate that user.

For details on configuring SL1 to use LDAP or Active Directory authentication, see the manual on using ***LDAP or Active Directory***.

Importing Users from LDAP or Active Directory

If you have created Active Directory or LDAP accounts for users and do not want to manually create accounts again in SL1, you can configure SL1 to automatically create accounts for Active Directory users or LDAP users.

Each Active Directory or LDAP user logs in to SL1 using his or her Active Directory or LDAP username and password, and SL1 automatically creates an account for that user. Each subsequent time that user logs in to SL1, SL1 will use Active Directory or LDAP to authenticate that user.

For details on configuring SL1 to use LDAP or Active Directory authentication, see the manual on using ***LDAP or Active Directory***.

Using SSO for Authentication

If you have already created Single Sign-On (SSO) accounts for users, you can use SSO to authenticate one or more of those users. Each time an SSO user tries to access SL1, SL1 will use SSO (via SAML) to authenticate that user.

For details on configuring SL1 to use SSO authentication, see the manual on using ***Using Single Sign-On***.

Importing Users from SSO

If you have created Single Sign-On (SSO) accounts for users and do not want to manually create accounts again in SL1, you can configure SL1 to automatically create accounts for SSO users.

Each SSO user enters the URL to access SL1. SL1 automatically creates an account for that user. Each subsequent time that user logs in to SL1, SL1 will use SSO to authenticate that user.

For details on configuring SL1 to use SSO authentication, see the manual on using ***Using Single Sign-On***.

Editing an Existing User Account

The **Account Properties** page allows you to define contact information for a user or edit existing contact information for a user. From this page, you can also access the other tabs in the **Account Administration** panel.

To edit the contact information for a user account:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. In the **User Accounts** page, find the user account you want to edit. Click its business card icon ().
3. The **Account Properties** page appears.
4. In the **Account Properties** page, you can edit one or more contact fields. You can also click one of the additional tabs. After you save a new user account, an additional set of tabs appears. These tabs are the Account Panel tools. These tabs include the following:
    - ***Properties***. Displays the **Account Properties** page, where you can define contact information for a user or edit existing contact information.
    - ***Permissions***. Displays the**Account Permissions** page, where you can define or edit the account name, password, account type, state, authentication method, ticket queue membership, and privilege keys.
    - ***Preferences***. Displays the **Account Preferences** page, where you can customize some of the behavior and appearance of SL1. The customizations that you choose will appear each time the current user logs in to SL1. This will not affect how SL1 appears to other users.
    - ***Schedule***. Displays the **Account Scheduled** page, where you can view a calendar for the user and enter one-time and recurring appointments, meetings, and vacation leave for the user.
    - ***Report***. Generates an HTML report about the user account.
5. Each of the tabs is described in the section on *Managing User Accounts*.
6. Click the **[Save]** button to save your changes.

Deleting an Existing User Account

From the **User Accounts** page, you can delete one or more user accounts.

> CAUTION: If you delete an existing user account that has any shared dashboards, those dashboards will also be deleted.

To do so:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. In the **User Accounts** page, find the account or accounts you want to delete. Select its checkbox (☑).
3. In the ***Select Action*** drop-down field (in the lower right), choose *DELETE Accounts*.
4. Click the **[Go]** button.
5. The selected account(s) will be deleted from SL1.

Performing Administrative Tasks for One or More User Accounts

The **User Accounts Manager** page contains a drop-down field in the lower right called ***Select Action***. This field allows you to apply an action to multiple user accounts at once. You can delete, change authentication, or change the default brand for multiple user accounts, simultaneously.

To apply an action to multiple user accounts:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. In the **User Accounts** page, select the checkbox for each user account you want to apply the action to. To select all checkboxes for all user accounts, select the red checkbox at the top of the page.
3. In the ***Select Action*** drop-down list, select one of the following actions.
    - ***DELETE Accounts***. Deletes all selected user accounts fromSL1.
    - ***Require LDAP/AD Authentication***. Each selected user must be authenticated on an LDAP server or an Active Directory server. User must have an existing account on an LDAP server or an Active Directory server. For details on configuring SL1 to use LDAP or Active Directory authentication, see the manual ***Using LDAP or Active Directory with SL1***.
    - ***Remove LDAP/AD Authentication***. Each selected user must be authenticated by a Compute Nodes.
    - ***Change Brand To***. Change the default theme (page layout, color, and graphics) for the user(s). Select from the list of existing themes.
    - ***Change User Policy To***. Change the user policy associated with the user account(s). Select from the list of existing user policies.
4. Click the **[Go]** button to apply the selected action to each selected user account.

Examples of Manually Creating a User Account

The following example walks you through the steps for manually creating an organization.

- For this example, we'll use an imaginary company with three locations: a sales office in Boston, headquarters in Chicago, and an R&D office in California. The company has created organizations based on geographical location.
- The company has created three organizations: Northeast, Headquarters, West Coast.
- Each organization will contain the local hardware and the local users. This will ensure that users can access information on local devices and local users. Administrators can define Access Keys to further limit or allow access.

- We will manually create a user, Paul Revere, as a member of the organization called "Northeast". Paul Revere is the Administrator for his organization and requires full access to SL1. Therefore, he will have an account of type "administrator".
- We will manually create a user, Samuel Adams, as a member of the organization called "Northeast". Samuel Adams is the system administrator and will have an account of type "user". Samuel Adams needs to be able to manage the devices and user accounts in the organization "Northeast". We have already defined Access Keys that allow a user to perform these tasks.

Defining User "Paul Revere"

The user "Paul Revere" is an administrator who belongs to the organization "Northeast".

To manually create the user "Paul Revere":

1. Log in to SL1 as a system administrator. If you have not yet created organizations or user accounts, you can log in as "em7admin", using the password defined during initial configuration.
2. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
3. In the **User Accounts** page, click the **[Create]** button. The **Create New Account** page appears.
4. In the **Create New Account** page, supply the following values in each field:
    - ***First Name***. The user's name is Paul Revere, so we supplied "Paul" in this field.
    - ***Last Name***. We supplied the value "Revere" in this field.
    - ***Generate name based on first and last name***. We did not select this checkbox, because our corporate convention is to use first initial and last name as a user name. If we have duplicate names, we use first initial, middle initial, and last name as a user name.
    - ***Account Login Name***. We entered "prevere" as the user's account login name, as is our corporate convention.
    - ***Primary Email***. We entered "prevere@company.com" as the user's email address.
    - ***Password***. We entered "2IfByNight!" in this field, to follow best practices when creating a password. This password includes uppercase letters, lowercase letters, numerals, non-alphabetic characters, and cannot be found in a dictionary.
    - ***Confirm Password***. We entered the user's password again.
    - ***Password Strength***. We specified the user must have a Strong password.
    - ***Password Expiration***. We specified that the password will expire in 30 Days.
    - ***Password Shadowing***. We left this field at its default value - cannot reuse passwords from last year.
    - ***Require Password Reset***. We did not select this checkbox. The user will not be required to change their password when they first log in.
    - ***Multi-Factor Auth (MFA) User***. We entered "prevere1" in this field, because this user requires a different user name for Multi-factor authentication.

NOTE: For details on configuring multi-factor authentication, see the manual ***Using Multi-Factor Authentication***.

- ***Organization***. We selected the organization "System" as the user's primary organization.
- ***Account Type***. We selected "Individual", because this user is not a member of a user policy.
- ***Account Type***. We selected "Administrator", because this user requires full access to all tabs, pages, actions, and tasks in SL1.
- ***Login State***. We selected "Active" in this field, so this user can immediately begin using SL1.
- ***Authentication Method***. We selected *EM7 Session* in this field. We want to use the ScienceLogic database (as opposed to an LDAP or Active Directory database) to determine if the username and password are valid.
- ***Restrict to IP***. We did not enter a value in this field. Because this user is an administrator, we want to allow the user to access SL1 from multiple locations and multiple IP addresses, for diagnostic purposes.
- ***Country***. We selected "United States" as the country for this user.
- ***Time Zone***. We selected "America/New York" as the time zone for this user.
- ***Autosync Time Zone With Local Settings***. We selected *No*.
- ***Policy Membership***. Because this user was not created with a user policy, this field is grayed out.

5. Click the **[Save]** button to save the new user account.
6. The **Account Permissions** page appears, with some of the fields already populated with values from the **Create New Account** page
7. An additional set of tabs appears. These tabs are the Account Panel tools. These tabs are described in the section on *Managing User Accounts*.

Defining User "Samuel Adams"

The user "Samuel Adams" is a user who requires access to all the device features and account features for the devices and user accounts in his organization.

To manually create the user "Samuel Adams":

1. Log in to SL1 as a system administrator. If you have not yet created organizations or user accounts, you can log in as "em7admin", using the password defined during initial configuration.
2. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
3. In the **User Accounts** page, click the **[Create]**button.
4. The **Create New Account** page appears.
5. In the **Create New Account** page, supply the following values in each field:
    - ***First Name***. The user's name is Samuel Adams, so we supplied "Samuel" in this field.
    - ***Last Name***. We supplied the value "Adams" in this field.
    - ***Generate name based on first and last name***. We did not select this checkbox, because our corporate convention is to use first initial and last name as a user name. If we have duplicate names, we use first initial, middle initial, and last name as a user name.

- ***Account Login Name***. We entered "sadams" as the user's account login name, as is our corporate convention.
- ***Primary Email***. We entered "sadams@company.com" as the user's email address.
- ***Password***. We entered "TeaParty1216!" in this field, to follow best practices when creating a password. This password includes uppercase letters, lowercase letters, numerals, non-alphabetic characters, and cannot be found in a dictionary.
- ***Confirm Password***. We entered the user's password again.
- ***Password Strength***. We specified the user must have a Strong password.
- ***Password Expiration***. We specified that the password will expire in 30 Days.
- ***Password Shadowing***. We left this field at its default value—cannot reuse passwords from last year.
- ***Require Password Reset***. We did not select this checkbox. The user will not be required to change their password when they first log in.
- ***Multi-Factor Auth (MFA) User***. We entered "samadams1" in this field, because this user requires a different user name for Multi-factor authentication.

NOTE: For details on configuring multi-factor authentication, see the manual ***Using Multi-Factor Authentication***.

- ***Organization***. We selected the organization "System" as the user's primary organization.
- ***Account Type***. We selected *Individual*, because this user is not a member of a user policy.
- ***Account Type***. We selected *User*, because this user does not requires full access to all tabs, pages, actions, and tasks in SL1.
- ***Login State***. We selected *Active* in this field, so this user can immediately begin using SL1.
- ***Authentication Method***. We selected *EM7 Session* in this field. We want to use the ScienceLogic database (as opposed to an LDAP or Active Directory database) to determine if the user name and password are valid.
- ***Restrict to IP***. We did not enter a value in this field. Because this user is a system administrator, we want to allow the user to access SL1 from multiple locations and multiple IP addresses, for diagnostic purposes.
- ***Country***. We selected *United States* as the time zone for this user.
- ***Time Zone***. We selected *Anchorage* as the time zone for this user.
- ***Autosync Time Zone With Local Settings***. We selected *No*.
- ***Policy Membership***. Because this user was not created with a user policy, this field is grayed out.

6. Click the **[Save]** button to save the new user account.
7. The **Account Permissions** page appears, with some of the fields already populated with values from the **Create New Account** page:
8. In the **Account Permissions** page, we must now assign Access Keys to the user's account, so he can manage the devices and user accounts in his organization.

9. We have already created two Access Keys:

    - The Access key named ***Manage Devices*** allows a user full access to devices. For accounts of type "user", this access key allows a user full access to all the devices in his/her organization.
    - The Access key named ***Manage Accounts*** allows a user full access to user accounts. For accounts of type "user", this access key allows a user full access to all the user accounts in his/her organization.

10. We selected these Access Keys for the user Samuel Adams and clicked the **[Save]** button.
11. After creating the user account, an additional set of tabs appears. These tabs are the Account Panel tools. These tabs are described in the section on *Managing User Accounts*.

Chapter 8

User Policies

Overview

User Policies allow you to define a custom set of account properties and key privileges (from the **Account Permissions** page) 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. This chapter will show you how to create a user policy.

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 a User Policy?

In a user policy you can choose to define all the fields in the **Account Permissions** page or you can choose to define only one or more fields. When you apply the user policy to user accounts, only those fields you defined in the user policy will be applied to the user accounts. For the remaining fields, the user accounts will retain their previous values or use the default values.

User Policies have a dynamic relationship with their member user accounts. You can make a change to a user policy and SL1 will automatically update the account settings for each member account.

For example:

- Suppose you create a user account called "John Doe" on the first of the month and use the user policy named "NOC users" to create the user account.
- Suppose you create another user account called "Jane Smith" on the fifth of the month and again use the user policy "NOC users".
- Suppose on the 15th of the month, you add an additional Key Privilege to the "NOC users" policy.
- That additional Key Privilege will appear in the account for John Doe and Jane Smith as soon as the "NOC users" policy is saved.

If you create a user account with a user policy, the fields in the **Account Permissions** page for that user account are grayed out. If you want to manually edit fields in the **Account Permissions** page for the user account, you must disassociate the user account from the user policy. Any future changes made to the user policy will not appear in the disassociated user account.

If you want to automatically import user accounts from LDAP or Active Directory, you must create at least one user policy. To use user policies in this way, special configuration is required. This configuration is described in the manual ***Using LDAP or Active Directory***.

Creating a User Policy

User Policies allow you to define a custom set of account properties and privileges (from the **Account Permissions** page) 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 a new user policy:

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

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. In the **User Policy Properties Editor** page, supply a value in each field:

NOTE: If you don't want a field included in a User Policy, click on the field name. The field will become grayed out. SL1 does not apply the grayed-out fields to any aligned user accounts; the corresponding field in the user account retains its original value (either a default value or a custom value that was defined when the account was created).

- ***Policy Name***. Name of the user policy. Can be any combination of alphanumeric characters, up to 64 characters in length.
- ***Login State***. Specifies whether user accounts created with the policy can log in to SL1. Choices are:
    - *Active*. Means user accounts created with this policy are active and can log in to SL1.
    - *Suspended*. Means that user accounts created with this policy are not active and cannot log in to SL1.
- ***Account Type***. This drop-down contains an entry for each standard account type. These account types affect the list of Key Privileges for the user. The choices are:
    - *Administrator*. This type of user has unlimited permissions in SL1.
    - *User*. This type of user must be assigned permissions in SL1.
- ***Password Strength***. When defining or editing a user account, the administrator can define the required password strength. The user must then always use a password that meets or exceeds that specified password strength. SL1 will not allow the user to save changes to his/her password that do not meet the password strength requirement. Choices are:
    - *Good*. Password must be at least eight characters long and contain at least one number or one symbol.
    - *Strong*. Password must be at least eight characters long and contain at least one number and at least one symbol.
    - *Very Strong*. Password must be at least 13 characters long, contain no repeated characters, and contain at least one number and at least one symbol.
- ***Password Expiration***. Specifies whether or not the password for this account will expire and if so, when the password will expire. Choices are:
    - *Disabled*. Password does not expire.
    - *30 Days*. When the current password is 30 days old, during login the user will be prompted to change the password.
    - *60 Days*. When the current password is 60 days old, during login the user will be prompted to change the password.

- *90 Days*. When the current password is 90 days old, during login the user will be prompted to change the password.
- *180 Days*. When the current password is 180 days old, during login the user will be prompted to change the password.

If the password is set to expire, on the expiration date, the user will be prompted to change the password at the Login page. The user will be required to enter his/her old password and then enter a new password twice. If the user incorrectly enters the previous password or enters an invalid new password, the user will not be allowed to log in to SL1.

The new password must meet the requirements of the ***Password Strength*** field and the ***Password Shadowing*** field. SL1 will prompt the user to meet these requirements and display a description of those requirements.

NOTE: The value in the ***Password Expiration*** field in this page (the **Create New Account** page) overrides the value in the **Behavior Settings** page (System > Settings > Behavior).

- ***Password Shadowing***. Specifies requirements for password reuse. By default, when a user defines a new password, he/she cannot reuse any passwords that he/she has used in the last 12 months. The choices in this field are:
  - *Default - cannot reuse passwords from past year*
  - *1 - Cannot reuse last password*
  - *2 - Cannot reuse last 2 passwords*
  - *3 - Cannot reuse last 3 passwords*
  - *4 - Cannot reuse last 4 passwords*
  - *5 - Cannot reuse last 5 passwords*
  - *6 - Cannot reuse last 6 passwords*
  - *7 - Cannot reuse last 7 passwords*
  - *8 - Cannot reuse last 8 passwords*
  - *9 - Cannot reuse last 9 passwords*
  - *10 - Cannot reuse last 10 passwords*
- ***Require Password Reset***. If selected, the user will be prompted to change his/her password at the next login. When creating a new user account, this option is selected by default. After the user's first login, when he/she is prompted to change his/her password, this option is then unselected.

> **NOTE**: The ***Re-Apply All Settings to All Policy Members*** checkbox affects the behavior of the ***Require Password Reset*** field.

- ***Authentication Method***. Specifies how the user will be authenticated. The choices are:
  - *EM7 Session*. User's username and password are authenticated by the ScienceLogic database.
  - *LDAP/Active Directory*. User's username and password are authenticated by an LDAP server or Active Directory server. For details on configuring SL1 to use LDAP or Active Directory authentication, see the manual ***Using LDAP or Active Directory***.

> **NOTE**: For users who are authenticated with SSO, you must set the ***Authentication Method*** field to "LDAP/Active Directory" to support automatic user policy alignment updates in case attributes change. For details on configuring SL1 to use SSO authentication, see the manual on using ***Using Single Sign-On***.

- ***Restrict to IP***. The user will be allowed to access SL1 only from the specified IP. Specify the IP address in standard dotted-decimal notation.
- ***Ticket Queue Memberships***. Highlight one or more ticket queues of which users will be members.
- ***Primary Organization***. Specifies the primary organization. This will be the default organization for user accounts created with this policy. You can select from a list of all organizations in SL1.
- ***Theme***. Backgrounds, colors, fonts, and graphics that will appear when a user logs in. Themes are defined in the **Theme Management** page (System > Customize > Themes). You can select from a list of all themes in SL1.
- ***Time Zone***. The time zone to associate with each user account created with this user policy. Dates and times in SL1 will be displayed for the selected time zone.
- ***Additional Organization Memberships***. User accounts created with this user policy will be members of each selected organization. This allows users to view and access elements from multiple organizations. To select, highlight one or more organizations.
- ***Privilege Keys***. The **Privilege Keys** pane displays a list of Access Keys that can be assigned to the user's account. Access Keys define the tabs and pages users have access to and the actions that a user may perform. These key privileges are defined by the system administrator from the **Access Keys** page (System > Manage > Access Keys).
  - SL1 includes the default access key "Grant All". For accounts of type "user", this key always appears. The Grant All Key allows a user to access all pages and actions in SL1, except the user cannot create new access keys or edit existing access keys.
  - To assign an access key to a user, click the checkbox. A checkmark appears.

- To deny an access key to a user, do not select it.
- After clicking the **[Save]** button, all selected access keys will appear in red.

NOTE: Users of type "Administrator" automatically have access to all pages and actions in SL1. The **Privilege Keys** pane is grayed-out for "Administrator" policies.

- ***Re-Apply All Settings to All Policy Members***. When you save the policy and select this checkbox, all settings are reapplied to all policy members. If you have selected the ***Require Password Reset*** field, each user who is a member of this policy will have to reset their passwords on login, even if they have previously done so and toggled off that setting. Selecting this checkbox turns back on the ***Require Password Reset*** field again.

4. Click the **[Save]** button to save your new user policy.
5. You can now apply this user policy to new user accounts and existing user accounts. For details, see the following sections.

Creating a User Account with a User Policy

There are two ways to apply a user policy to a user account:

- When creating a new account, you can apply a user policy to simplify the creation process.
- You can apply a user policy to an existing user account. The previous settings will be deleted and the settings from the user policy will be applied.

To apply a user policy when manually creating a new account:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. In the **User Accounts** page, click the **[Create]** button. The **Create New Account** page appears.
3. In the **Create New Account** page, in the ***Account Type*** field, select *Policy Membership*.
4. In the ***Policy Membership*** pane, select a user policy.
5. Click the **[Save]** button to save the new 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.

NOTE: To remove the user from the user policy, in the ***Account Type*** field, select *Individual*.

To apply a user policy to an existing account:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. In the **User Accounts** page, find the user account you want to edit. Click its wrench icon ( ).

3. In the **Account Permissions** page, in the ***Account Type*** field, select *Policy Membership*.
4. A field appears below the ***Account Type*** field. From this new field, select the user policy to apply.
5. Click the **[Save]** button.
6. All permissions from the user policy are applied to the user account. All fields that are included in the user policy are now grayed out.

Applying a User Policy to Multiple User Accounts

To apply a user policy to multiple existing user accounts, perform the following:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. For each user account to which you want to apply a user policy, select the checkbox (☑) for the user account.
3. In the ***Select Action*** drop-down list (in the lower right), select a user policy (under *Change User Policy to*).
4. Click the **[Go]** button. The selected user policy is now applied to each selected user account.

Viewing Members of a User Policy

If you have created or edited user accounts using a user policy, those user accounts will appear as members of the user policy.

To view a list of members in a user policy:

1. Go to the **User Policy Membership** page (Registry > Accounts > User Policies).
2. Find the user policy for which you want to view members. Click its user icon (👤) in the *Members* column.
3. The **User Policy Membership** appears and displays the list of user accounts associated with the user policy.

Removing Members from a User Policy

You can disassociate one or more user accounts (members) from a user policy. When you do this, each disassociated user account will retain the settings in the **Account Permissions** page from the user policy, but the user account is no longer associated with the user policy. Any future changes made to the user policy will not appear in the disassociated user account.

For each disassociated user account, in the **Account Permissions** page, the ***Account Type*** field will contain the value "Individual" instead of "Policy Member" and none of the fields will be grayed-out. For each disassociated user account, you can now manually edit each field in the **Account Permissions** page.

To remove one or more members from a user policy:

1. Go to the **User Policy Membership** page (Registry > Accounts > User Policies).
2. Find the user policy for which you want to view members. Click its user icon (👤).
3. The **User Policy Membership** page displays the list of user accounts associated with the user policy.

4. Select the checkbox for each user account that you want to remove from the user policy.
5. In the ***Select Action*** field, select *REMOVE Policy Membership*. Click the **[Go]** button.
6. The selected user account(s) will now be "Individual" accounts, rather than members of the user policy.

Removing a Single User Account from a User Policy

You can remove a single user account from a user policy, directly from the **Account Permissions** page.

The user account will retain the current settings from the user policy in the **Account Permissions** page, but the user account is no longer associated with the user policy. Any future changes made to the user policy will not appear in the disassociated user account. None of the fields in the **Account Permissions** page will be grayed out anymore; you can now manually edit each field in the **Account Permissions** page.

To remove a single user account from a user policy:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. In the **User Accounts** page, find the user account you want to edit. Click its wrench icon ().
3. The **Account Permissions** page appears:
4. In the **Account Permissions** page:
    - In the ***Account Type*** field, select ***Individual*** (instead of *Policy Membership*).
    - When prompted, choose to remove the user account from the user policy.
5. Click the **[Save]** button to save your changes.

Deleting a User Policy

When you delete a user policy, the user accounts that are members of the user policy are not deleted. Each member user account will retain its previous settings, but in the **Account Permissions** page, the ***Account Type*** field will contain the value "Individual" instead of "Policy Member" and none of the fields will be grayed out.

To delete a user policy:

1. Go to the **User Policies** page (Registry > Accounts > User Policies).
2. In the **User Policies** page, find the user policy you want to delete. Select its checkbox (☑).
3. For each user policy you want to delete, select its checkbox.
4. In the ***Select Action*** drop-down field (in the lower right), choose *DELETE User Policies*.
5. Click the **[Go]** button.
6. Each selected user policy will be deleted. For each member account that was previously aligned with the deleted policies, in the **Account Permissions** page, SL1 sets the ***Account Type*** field to *Individual*.

Example of Creating a User Policy

Suppose we want to create all the user accounts for the people in the customer care department at our fictional company.

Suppose the customer care staff is located at headquarters of our fictional company and belong to the "Northeast" organization.

Suppose the customer care staff needs to be able to listen to complaints from customers and then record each complaint in a work ticket. So each member of the customer care staff needs to be able to create tickets and view the status of those tickets.

We could create a user policy that would allow us to "preset" many of these settings, so they can quickly be applied to multiple user accounts.

To create the user policy:

1. Log in to SL1 as a system administrator. If you have not yet created organizations or user accounts, you can log in as "em7admin", using the password defined during initial configuration.
2. Go to the **User Policies** page (Registry > Accounts > User Policies). Click the **[Create]** button.
3. In the **User Policy Properties Editor** page, enter a value in each of the following fields:

    - ***Policy Name***. For the name of the user policy, we entered "Customer_Care".
    - ***Login State***. We selected *Active*, so that user accounts created with this policy can immediately log in to SL1.
    - ***Account Type***. We selected *User*.
    - ***Password Strength***. We selected *Strong*.
    - ***Password Expiration***. We accepted the default setting of *Disabled*.
    - ***Password Shadowing***. We accepted the default setting of *Default - cannot reuse passwords from past year*.
    - ***Require Password Reset***. We did not select the *Next Login* checkbox.
    - ***Authentication Method***. We selected *EM7 Session*, so that the SL1 database will verify that each user's account name and password are legitimate.
    - ***Restrict to IP***. We did not supply a value in this field, because this policy will be applied to multiple users, each with his/her own IP address.
    - ***Event Console Default Display***. We accepted the default setting of *Flat events table*.
    - ***Ticket Queue Memberships***. We have left this set to *None*. If part of your user's responsibility is to file tickets, select all appropriate ticket queues in this field. This allows users created with the user policy to view and access all ticket queues in SL1.
    - ***Primary Organization***. We select *System* as the primary organization for all users created with this user policy.
    - ***Theme***. We accepted the default theme.

- ***Time Zone***. We selected the time zone for *America/New York*. User accounts created with this policy will see date and time values that match the New York time zone.
- ***Additional Organization Memberships***. We did not select any additional organizations. Customer care staff does not need to view devices or account information from other organizations in the company.
- ***Privilege Keys***. In this pane, we selected several Access Keys. These Access Keys allow users to have basic privileges and to create and view tickets and ticket reports. This allows the user to create tickets and track the status of those tickets.

4. Click the **[Save]** button to save your new user policy.
5. We can now apply this user policy to new user accounts and existing user accounts.

Example of Creating a User Account with a User Policy

In this example, we'll use the user policy we created previously (Customer_Care) to create a new user account.

The new user is Billy Corgan. He will be a member of the Customer Care group and requires the settings we saved in the user policy named "Customer_Care". Using the Customer_Care user policy will save us time when configuring the user account for Billy Corgan.

To create the new user account using the user policy:

1. Log in to SL1 as a system administrator. If you have not yet created organizations or user accounts, you can log in as "em7admin", using the password defined during initial configuration.
2. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
3. In the **User Accounts** page, click the **[Create]**button. The **Create New Account** page appears.
4. In the **Create New Account** page, supply the following values in each field:

   - ***First Name***. The user's name is Billy Corgan, so we supplied "Billy" in this field.
   - ***Last Name***. We supplied the value "Corgan" in this field.
   - ***Generate name based on first and last name***. We did not select this checkbox, because our corporate convention is to use first initial and last name as a username. If we have duplicate names, we use first initial, middle initial, and last name as a username.
   - ***Account Login Name***. We entered "bcorgan" as the user's account login name, as is our corporate convention.
   - ***Primary Email***. We entered "bcorgan@company.com" as the user's email address.
   - ***Password***. We entered "Pumpkins1979!!" in this field, to follow best practices when creating a password. This password includes uppercase letters, lowercase letters, numerals, non-alphabetic characters, and cannot be found in a dictionary.
   - ***Confirm Password***. We entered the user's password again.
   - ***Password Strength***. We specified the user must have a *Strong* password.
   - ***Password Expiration***. We specified that the password will expire in *30 Days*.
   - ***Password Shadowing***. We left this field at its default value - cannot reuse passwords from last year.

- ***Require Password Reset***. We did not select this checkbox. The user will not be required to change their password when they first login.
- ***Multi-Factor Auth (MFA) User***. We left this field blank, because this user has not enabled Multi-factor authentication.

> **NOTE**: For details on configuring multi-factor authentication, see the manual ***Using Multi-Factor Authentication***.

- ***Organization***. We selected the organization *SILO*.
- ***Autosync Time Zone With Local Settings***. We selected *No*.
- ***Account Type***. We selected *Policy Membership*, because we want to use the user policy named "Customer_Care" when creating this user account. After selecting *Policy Membership*, all the fields in the **Individual Properties** pane are grayed out, because these fields are among those that are defined in user policies. The fields in the **Policy Membership** pane became active.
- ***Policy Membership***. In this pane, we selected the policy *Customer_Care* to apply to the new user.

5. Click the **[Save]** button to save the new user account.
6. The **Account Permissions** page appears, with all the fields already populated with values from the **Create New Account** page and the Customer_Care user policy. The fields that are grayed out are those that are inherited from the user policy.

Chapter 9

Role-Based User Accounts

Overview

Remote support personnel or contractors sometimes require temporary or limited access to an SL1 appliance to perform maintenance tasks or to troubleshoot problems. For these situations, you can grant access to the SL1 appliance using one of the following limited access, role-based accounts:

- SL1User
- SL1Admin

This chapter will describe the role-based user accounts in SL1, and will show you how to use them.

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 are Role-Based User Accounts?

Remote support personnel or contractors sometimes require temporary or limited access to an SL1 appliance to perform maintenance tasks or to troubleshoot problems. For these situations, you can grant access to the SL1 appliance using one of the following limited access, role-based accounts:

- SL1User
- SL1Admin

> **NOTE:** Role-based accounts are supported on All-In-One Appliances and in the distributed SL1 architecture. These accounts are *not* currently supported for the extended SL1 architecture.

These role-based accounts are installed by default in SL1 version 11.1.0 and higher. No configuration is required to enable the accounts.

The sections that follow provide more details about these accounts.

Role-Based sl1admin Account

The *sl1admin* account enables the system owner to grant temporary access to support staff who perform maintenance and troubleshooting tasks.

- The sl1admin account does not appear in SL1 user interface. This account is available for SSH or console access to the command line of an SL1 appliance only.
- SL1 grants one-time passwords from a file of hash values. The initial file is generated upon install or upgrade of Sl1. This file is regenerated each time half the passwords in the file have been granted or when the file reaches 7-days old, whichever occurs first.
- Each time a one-time password is granted, SL1 creates a log entry in the **Audit Logs** page (System > Monitor > Audit Logs).
- The sl1admin user does not have full root access. The sl1admin user uses a tmux shell and has access to only a limited set of commands. The sl1admin user can restart services, shutdown and reboot SL1 appliances, and run sudo commands that do not require root access.
- All `sudo` actions by the sl1admin user are logged in the file /var/log/secure.
- Additionally, the SL1 administrator can attach to the session in read-only mode to watch the sl1admin session in progress or attach in read-write mode, which allows the SL1 administrator to take over the session, if necessary.

Using the sl1admin Account

To log into the sl1admin account:

1. In a console or command window, SSH to the SL1 appliance, as follows, using the IP address of the SL1 appliance.

```
ssh sl1admin@<ip_address>
```

2. The password prompt will display a 3- or 9-digit number. Make note of this number to use in the next step.

> **NOTE:** The numeric code is 3 digits unless you have canceled out in the middle of your most recent login or if another user is also logging in to the sl1admin user account at the same time. In either of those cases, you will be given a 9-digit numeric code such as `001/030/009`.

3. Open the SL1 user interface and go to the **Appliances** page (System > Settings > Appliances). Find the appliance you are logging in to in the list of appliances and click its padlock ( ) icon. The **One Time Password** modal appears.
4. Enter the numeric code that was displayed in step 3 into the One Time Password modal. Click **[Generate Password]**. The generated password appears.
5. Type the generated password into the console window at the password prompt. Press Enter. After authentication is complete, the sl1admin user session begins in a tmux shell. You will see a green status bar at the bottom of the screen.

Monitoring an sl1admin Session in Progress

You can monitor an sl1admin session that is in progress using the em7admin account. To monitor the session:

1. In a console or command window, SSH to the SL1 appliance where the sl1admin user session is in progress. Log in with an administrator account.
2. Obtain the unique identifier (UID) of the tmux session in progress by entering the following command.

```
file /tmp/tmux*/default
```

3. Note the UID returned by the command. In the following example, the UID is "1001"

```
/tmp/tmux-1001/default: socket
```

4. Use the UID to attach to the tmux session with the following command.

```
tmux -S /tmp/tmux-<uid>/default attach
```

> **NOTE:** The command above provides read/write access to the tmux session. If you want to attach as read-only, append "-r" to the command string.

5. Exit the attachment to the session by pressing Ctrl+b, and then "d".

Role-Based sl1user Account

The *sl1user* account allows a user to perform maintenance tasks from a set of menu options. This menu allows the sl1user account to administer a Data Collector.

- The sl1user account does not appear in SL1 user interface. This account is available for SSH or console access to the command line of an SL1 appliance only.
- The sl1user account can:
    - modify the IP address of a network interface
    - test DNS entries
    - modify and test NTP entries
    - view system status
    - view the message of the day
- Each action performed by the sl1user account is logged in /var/log/em7/slmenu.log.

Changing the Password for the sl1user Account

During installation or upgrade to SL1 version 11.1.0 or later, the password for the em7admin account is copied and set as the sl1user account password.

WARNING: ***SciencLogic strongly recommends that you change the initial default em7admin password before granting access to the sl1user account.*** Because the initial default password for the sl1user account is the same as the password for the em7admin account, you ***must*** change the password before the first use of the sl1user account.

To change the password for the sl1user account:

1. Log in to the console of the Database Server or SSH to the Database Server.
2. Enter the following command:

```
sudo passwd sl1user
```

3. When prompted, type and then re-type the new password.

Using the sl1user Account

To use the sl1user account:

1. In a console or command window, SSH to the SL1 appliance, as follows, using the IP address of the SL1 appliance and the sl1user password.

```
ssh sl1user@<ip_address>
```

2. At the sl1user main menu, make a selection using the number of the selection or the arrow keys. Click **[OK]**.
3. When you are finished, choose **[Exit]** from the main menu to close the session.

Menu Options for sl1user

The menu options available for the sl1user account are described below.

- ***Network Configuration***. The Network Configuration menu lets the sl1user select an interface from a list of interfaces and edit the configuration for that interface. For example, if the gateway or DNS entry was configured incorrectly during installation, the sl1user can choose this menu option to correct the configuration.
- ***NTP Configuration***. The NTP Configuration menu lets the sl1user perform basic NTP actions. Menu options are as follows:
    - ***Edit configuration***. Edit the existing NTP server entries.
    - ***Test configuration***. Check if the configured NTP servers are responsive.
    - ***Force Sync***. Force a sync with the NTP servers in case of clock drift, for example.
    - ***Restart Service***. Restarts the chronyd service.
- *DNS Configuration*.
    - ***Edit configuration***. Edit the existing DNS server entries.
    - ***Test configuration***. Check if the configured DNS servers are responsive.
- *System Status*.
    - ***View System Status Log***. Displays the contents of the last run of the system status script.
    - ***Run System Status***. Runs the system status script on demand.
    - ***Message of the Day***. Because the sl1user login is inside a shell, the message of the day is not displayed after the sl1user authenticates. This menu option provides a way for the sl1user to view the message of the day.

To move back to the previous menu, use the Exit option. If you are at the top-level menu, the Exit option ends the sl1user session.

Chapter 10

Managing User Accounts

Overview

This chapter covers many of the tasks that can be undertaken from the tabs in the **Account Administration** panel. These tasks include changing a user's organization and access keys, editing a user's contact information, editing a user account's schedule, and creating a ticket about a user account.

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:

Account Administration Panel

After you save a new user account, an additional set of tabs appears. These tabs are the **Account Administration** panel. These tabs include the following:

- ***Properties***. Displays the **Account Properties** page, where you can define contact information for a user or edit existing contact information.
- ***Permissions***. Displays the **Account Permissions** page, where you can define or edit the account name, password, account type, state, authentication method, ticket queue membership, and privilege keys.
- ***Preferences***. Displays the **Account Preferences** page, where you can customize some of the behavior and appearance of SL1. The customizations that you choose will appear each time the current user logs in to SL1. They will not affect how SL1 appears to other users.
- ***Schedule***. Displays the **Account Scheduled** page, where you can view a calendar for the user and enter one-time and recurring appointments, meetings, and vacation leave for the user.
- ***Report***. Generates an HTML report about the user account.

This chapter will describe how to use the **Account Administration** panel to manage each user account.

Changing a User's Organization

If you need to assign a user to a different primary organization than was originally defined or allow the user to access an additional organization:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. In the **User Accounts** page, find the user account you want to edit. Click its wrench icon ().
3. In the **Account Permissions** page, edit the following fields:
    - ***Primary Organization***. Specifies the primary organization. This will be the default organization for user accounts created with this policy. You can select from a list of all organizations in SL1. To change the primary organization, select a different organization from the list.
    - ***Additional Organization Memberships***. The user account will be members of each selected organization. This allows users to view and access elements from multiple organizations. To select, highlight one or more organizations.
4. Click the **[Save]** button to save your changes to the user account.

Changing a User's Access Keys

If you need to change the Privilege Keys that are assigned to a user:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. In the **User Accounts** page, find the user account you want to edit. Click its wrench icon ( ).
3. The **Account Permissions** page appears.
4. In the **Account Permissions** page, edit the following fields:
    - ***Privilege Keys***. The **Privilege Keys** pane displays a list of Access Keys that can be assigned to the user's account. Access Keys define the tabs and pages users have access to and the actions that a user may perform. These key privileges are defined by the SL1 system administrator from the **Access Keys** page (System > Manage > Access Keys).
        - To assign an access key to a user, click the checkbox. A checkmark appears.
        - To deny an access key to a user, do not select it.
        - To remove an access key from a user's account, select the checkmark. The key should now be unchecked.
        - After clicking the **[Save]** button, all selected access keys will appear in red.
5. Click the **[Save]** button to save your changes to the user account.

Editing Contact Information in the Account Properties Page

The **Account Properties** page allows you to define contact information for a user or edit existing contact information for a user.

To edit the contact information for a user account:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. In the **User Accounts** page, find the user account you want to edit. Click its business-card icon ( ). The **Account Properties** page appears.
3. In the **Account Properties** page, you can edit one or more contact fields.

NOTE: If the user's account was automatically created, using the user's LDAP or Active Directory account, SL1 can automatically populate many of the fields in the **Account Properties** page. You can also configure SL1 to dynamically update the corresponding LDAP or AD fields. If an administrator made changes to the account, SL1 will automatically write those changes to the user's account in LDAP or Active Directory. If an LDAP or AD administrator makes changes to an LDAP or AD account, SL1 will automatically retrieve those updates and apply them to the user's account in SL1 the next time the user logs in to SL1. For details, see the manual ***Using LDAP and Active Directory***.

- ***First Name***. User's first name. This value can be up to 24 characters in length.
- ***Last Name***. User's last name. This value can be up to 24 characters in length.
- ***Title***. User's title. This field can be up to 32 characters in length.

- ***Department***. User's department. This field can be up to 36 characters in length.
- ***Phone***. The user's phone number at work. This field can be up to 24 characters in length.
- ***Mobile***. The user's cell phone number. This field can be up to 24 characters in length.
- ***Pager***. Any other phone numbers for contacting the user. This field can be up to 24 characters in length.
- ***Primary Email***. The user's primary email address. This field can be up to 64 characters in length.
- ***Secondary Email***. Additional email address for contacting the user. This field can be up to 64 characters in length.
- ***Alternate Email***. Additional email address for contacting the user. This field can be up to 64 characters in length.
- ***Street Address***. User's street address at work. This field can be up to 64 characters in length.
- ***Suite/Building***. Suite/Building for the user at work. This field can be up to 64 characters in length.
- ***City***. City where the user works. This field can be up to 64 characters in length.
- ***State***. State where the user works.
- ***Postal Code***. Zip code where the user works. This field can be up to 12 characters in length.
- ***Country***. Country where the user works.
- ***Toll Free***. Toll-free phone number for the user. This field can be up to 24 characters in length.
- ***Key Role***. Description of the user's responsibilities in case of a critical situation. This description might differ from the user's actual title. For example, a contact's title might be Senior Engineer, but his/her role for the organization might be technical lead. Select from the drop-down list. (SL1 system administrators can go to the **Select Objects Editor** page to customize the entries that appear in this list.) If a value is supplied in this field, the user will appear as a ***Critical Contact*** for the organization in the **Organization Properties** page.
- ***Critical Contact***. Circumstance when person should be contacted. This description might differ from the user's department. For example, the user's department might be Operations, but his/her role for the organization might be Hardware Maintenance. Select from the drop-down list. (SL1 system administrators can go to the **Select Objects Editor** page to customize the entries that appear in this list.) If a value is supplied in this field, the user will appear as a ***Critical Contact*** for the organization in the **Organization Properties** page.
- ***Pass Phrase***. Questions that verifies a user who has forgotten his/her password. SL1 does not use this field.
    - What is your Mother's maiden name?
    - What is your favorite pet's name?
    - What is your favorite color?
- ***Answer***. This field contains the answer to the question selected in the ***Pass Phrase*** field. This field can be up to 64 characters in length.
- ***Time Zone***. Time zone associated with the user's location. Select from a list of all time zones.

NOTE: If the user account is aligned with a user policy that specifies a time zone, the ***Time Zone*** field will be disabled. The user account will use the Time Zone specified in the user policy and the ***Time Zone*** field cannot be edited.

- ***Billing ID***. Billing ID associated with this user. This field can be up to 24 characters in length.
- ***CRM ID***. CRM ID associated with this user. This field can be up to 64 characters in length.
- ***Notes***. Any notes you want to include with the user's profile information. You can also include a document template (System > Customize > Document Templates) in this field.

4. Click the **[Save]** button to save your changes.

Editing Access and Permissions in the Account Permissions Page

The **Account Permissions** page allows you to define permissions and access for the user account. In the **Account Permissions** page, you can define or edit the account name, password, user policy, state, authentication method, ticket queue membership, and privilege keys for a user account.

To edit the permissions and access for a user account:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. In the **User Accounts** page, find the user account you want to edit. Click its wrench icon ( ).
3. The **Account Permissions** page appears:
4. In the **Account Permissions** page, you can edit one or more of the following fields.

NOTE: If the user's account was created using a user policy, all the fields except ***Account Login Name*** and ***Password*** will be grayed out. To edit these fields, you must *remove the user from the user policy*.

NOTE: If the user's account was automatically created, using the user's LDAP or Active Directory account, SL1 can automatically populate many of the fields in the **Account Properties** page. You can also configure SL1 to dynamically update the corresponding LDAP or AD fields. If an administrator made changes to the account, SL1 will automatically write those changes to the user's account in LDAP or Active Directory. If an LDAP or AD administrator makes changes to an LDAP or AD account, SL1 will automatically retrieve those updates and apply them to the user's account in SL1 the next time the user logs in to SL1. For details, see the manual ***Using LDAP and Active Directory***.

- ***Account Login Name***. User's login name. This field can be up to 32 characters in length.
- ***User Display Name***. User's username, email address, or preferred display name. This value is determined by the user's authentication resource settings.
- ***Change Password***. The user's password. This value must be at least 8 characters in length and can be up to 64 characters in length. The password must meet the requirements that you set in the ***Password Strength*** field.
- ***Confirm Password***. The user's password again. This value must be at least 8 characters in length and can be up to 64 characters in length.
- ***Password Strength***. When defining or editing a user account, the administrator can define the required password strength. The user must then always use a password that meets or exceeds that specified password strength. SL1 will not allow the user to save changes to his or her password that do not meet the password-strength requirement. Choices are:

    - *Good*. Password must be at least eight characters long and contain at least one number or one symbol.
    - *Strong*. Password must be at least eight characters long and contain at least one number and at least one symbol.
    - *Very Strong*. Password must be at least 13 characters long, contain no repeated characters, and contain at least one number and at least one symbol.

- ***Account Type***. Specifies whether the user is a member of a user policy. Choices are:

    - *Individual*. User account is not a member of a user policy
    - *Policy Membership*. User will be defined with a user policy. When selected, the *Policy Membership* field becomes active.
        - When a user policy is applied to a user's account, the user inherits values for all fields specified in the user policy. When a user policy is selected, all fields inherited from the user policy will be grayed-out and cannot be modified.
        - When a user policy is edited, each user account that is a member of that template will be dynamically updated.

    The second drop-down list contains an entry for each standard account type. These account types affect the list of Key Privileges for the user. The choices are:

    - *Administrator*. This type of user has unlimited permissions in SL1.
    - *User*. This type of user must be assigned permissions in SL1.

- ***Login State***. Default login state for the user. The choices are:

    - *Suspended*. Account is not active. User cannot log in to SL1.
    - *Active*. Account is active. User can log in to SL1.

- *Vacation*. User can log in, but SL1 will not send any automated email notifications to the user's email address(es).

- ***Password Expiration***. Specifies whether or not the password for this account will expire and if so, when the password will expire. Choices are:

  - *Disabled*. Password does not expire.
  - *30 Days*. When the current password is 30 days old, during login the user will be prompted to change the password.
  - *60 Days*. When the current password is 60 days old, during login the user will be prompted to change the password.
  - *90 Days*. When the current password is 90 days old, during login the user will be prompted to change the password.
  - *180 Days*. When the current password is 180 days old, during login the user will be prompted to change the password.

If the password is set to expire, on the expiration date, the user will be prompted to change the password at the Login page. The user will be required to enter their old password and then enter a new password twice. If the user incorrectly enters the previous password or enters an invalid new password, the user will not be allowed to log in to SL1.

The new password must meet the requirements from the ***Password Strength*** field and the ***Password Shadowing*** field. SL1 will prompt the user to meet these requirements and display a description of those requirements.

NOTE: The value in the ***Password Expiration*** field in this page (the **Account Permissions** page) overrides the value in the **Behavior Settings** page (System > Settings > Behavior).

- ***Password Shadowing***. Specifies requirements for password reuse. By default, when a user defines a new password, he/she cannot reuse any passwords that he/she has used in the last 12 months. The choices in this field are:

    - *Default - cannot reuse passwords from past year*
    - *1 - Cannot reuse last password*
    - *2 - Cannot reuse last 2 passwords*
    - *3 - Cannot reuse last 3 passwords*
    - *4 - Cannot reuse last 4 passwords*
    - *5 - Cannot reuse last 5 passwords*
    - *6 - Cannot reuse last 6 passwords*
    - *7 - Cannot reuse last 7 passwords*
    - *8 - Cannot reuse last 8 passwords*
    - *9 - Cannot reuse last 9 passwords*
    - *10 - Cannot reuse last 10 passwords*

- ***Require Password Reset***. If selected, the user will be prompted to change his or her password at the next login. When creating a new user account, this option is selected by default. After the user's first login, when he or she is prompted to change his or her password, this option is then unselected.

NOTE: The ***Password Reset Interval*** option on the **Behavior Settings** page (System > Settings > Behavior controls the minimum amount of time that must pass before a user can change a password.

- ***Authentication Method***. Specifies how the user will be authenticated. The choices are:

    - *EM7 Session*. User's username and password are authenticated by the ScienceLogic database.
    - *LDAP/Active Directory*. User's username and password are authenticated by an LDAP server or Active Directory server. For details on configuring SL1 to use LDAP or Active Directory authentication, see the manual ***Using LDAP and Active Directory***.

NOTE: For users who are authenticated with Single Sign-On (SSO), EM7 ignores the ***Authentication Method*** field. For details on configuring SL1 to use Single Sign-On (SSO) authentication, see the manual on using ***Using Single Sign-On***.

- ***Restrict to IP***. The user will be allowed to access SL1 only from the specified IP address. Specify the IP address in standard dotted-decimal notation.

- ***Multi-Factor Auth (MFA) User***. If this user requires a different user name for Multi-factor authentication, enter the MFA user name in this field.

NOTE: For details on configuring multi-factor authentication, see the manual ***Using Multi-Factor Authentication***.

- ***Ticket Queue Membership***. Ticket Queues to which the user is assigned. When a user is assigned to a ticket queue and is granted an access hook that allows them to view tickets, he or she can view the tickets in that queue. Ticket queues are defined by SL1 system administrators.
- ***Primary Organization***. Specifies the primary organization. This will be the default organization for user accounts created with this policy. You can select from a list of all organizations in SL1.
- ***Theme***. Backgrounds, colors, fonts, and graphics that will appear when a user logs in. Themes are defined in the **Theme Management** page. You can select from a list of all themes in SL1.
- ***Time Zone***. The time zone to associate with each user account created with this user policy. Dates and times in SL1 will be displayed for the selected time zone.

NOTE: If the user account is aligned with a user policy that specifies a time zone, the ***Time Zone*** field will be disabled. The user account will use the time zone specified in the user policy and the ***Time Zone*** field cannot be edited for that account.

- ***Autosync Time Zone With Local Settings***. Specifies whether SL1 should always use the time zone specified in the ***Time Zone*** field or if SL1 should adopt the local time zone (when it differs from the value in the ***Time Zone*** field). This is helpful for users who travel and use SL1 "on the road". Choices are:
    - *Yes*. If the value in the ***Time Zone*** field differs from the local time zone, SL1 should use the local time zone.
    - *No*. SL1 will continue to use the time zone specified in the ***Time Zone*** field, even if the local time zone differs.
- ***Additional Organization Memberships***. Specifies additional organizations for the user. This allows users to view and access elements from multiple organizations. To select, highlight one or more organizations.
- ***Privilege Keys***. The Privilege Keys pane displays a list of access keys that can be assigned to the user's account. Privilege Keys define the tabs and pages users have access to and the actions that a user may perform. These key privileges are defined by the SL1 system administrator from the **Access Keys** page (System > Manage > Access Keys).
    - SL1 includes the default Access Key "Grant All". For accounts of type "user", this key always appears. The Grant All Key allows a user to access all pages and actions in SL1, except the user cannot create new Access Keys or edit existing Access Keys.

- To assign a Key Privilege to a user, click the checkbox. A checkmark appears.
- To deny a Key Privilege to a user, do not select it.
- After clicking the **[Save]** button, all selected Privilege Keys will appear in red.

NOTE: Users of type "Administrator" automatically have access to all pages and actions in SL1. The **Privilege Keys** pane is grayed-out for "Administrator" users.

5. Click the **[Save]** button to save your changes.

Password Reset Email Editor

The **Password Reset Email Editor** page (Password Reset Email Editor) allows ScienceLogic administrators to define the email message that is sent to ScienceLogic users who select the "I forgot my password" option from the **Login** page.

If the user enters a valid ScienceLogic username in the **Login** page and then selects the *I forgot my password* option, SL1 will check the account information for that user. If the user's account information includes an email address, SL1 will send the user an email message. The email message will include a link that allows the user to redefine their ScienceLogic password. The new password must meet the requirements defined in the ***Password Strength*** field and the ***Password Shadowing*** field for the user account. SL1 will prompt the user to meet these requirements and display a description of those requirements.

The user can select the *I forgot my password* option up to ten times without responding to the sent email (using the link in the email to reset the password). After ten times, SL1 will no longer send another email message to the user's email address. The user can continue to select the *I forgot my password* option, but SL1 will not resend an email.

If the user's account information does not include an email address, SL1 displays the message "Password recovery is not available for your account, please contact your system administrator".

If the user does not enter a valid ScienceLogic username in the **Login** page, the *I forgot my password* option is still displayed, but SL1 does not send an email. This prevents intruders from guessing ScienceLogic account names.

If the user exceeds the number of login tries (defined in the **Behavior Settings** page), the "I forgot my password" option is not displayed in the **Login** page.

Defining the Email Message for "I forgot my password"

In the **Password Reset Email Editor** page (System > Settings > Password Reset Email), you can define the email that is sent from SL1 when an end user selects the *I forgot my password* option from the **Login** page.

To define the email message sent by SL1:

1. Go to the **Password Reset Email Editor** page (System > Settings > Password Reset Email).
2. Supply a value in each of the following fields:

- ***Priority***. This will be the priority of the email message. Choices are:
    - *High*. Emails will be marked as high priority.
    - *Normal*. Emails will be marked as normal priority.
    - *Low*. Emails will be marked as low priority.
- ***Subject***. This will be the subject of the email message.
- ***Message***. This will be the body of the email message. ***The body must include the variable %L***. This variable inserts the link to the page that allows the user to reset their ScienceLogic password.

3. You can include the following variables in the ***Subject*** field and the ***Message*** field:
    - ***%L (uppercase "el")***. The link to the page that allows the user to reset their password.
    - ***%O (uppercase "oh")***. The user's primary organization, as defined in the **Account Permissions** page for the user.
    - ***%fn (lowercase "eff" "en")***. The user's first name, as defined in the **Account Permissions** page for the user.
    - ***%ln (lowercase "el "en"***. The user's last name, as defined in the **Account Permissions** page for the user.
4. Click the **[Save]** button to save the email template.
5. When a user follows the link in the email, SL1 displays the **Login** page, with the message "Your account has been reset. Please create a new password." The user must then enter their new password twice. The new password is recorded in SL1 and replaces the previous (forgotten) password.

For example, you could define the following:

Subject. ScienceLogic | %O (automated message)

Message. Hello %fn %ln,

Your password for account %A has been reset.

Please use the following link to log in and choose a new password:

%L.

For the user "Keyser Soze", who is a member of the System organization, the following email would be sent:

Subject: ScienceLogic | System (automated message).

Hello Keyser Soze,

Your password for account ksoze has been reset.

Please use the following link to login and choose a new password:

https://name_or_IP_of_EM7_Administration_Portal/login.em7?prs=hash

Editing GUI Appearance and Preferences in the Account Preferences Page

The **Account Preferences** page allows you to customize some of the behavior and appearance of SL1. The customizations are associated only with the selected user account and will appear each time the user logs in to SL1. They will not affect how SL1 appears to other users.

To edit account preferences:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. In the **User Accounts** page, find the user account you want to edit. Click its wrench icon ().
3. Click the **[Preferences]** tab. The **Account Preferences** page appears.
4. In the **Account Preferences** page, you can edit one or more of the following fields:

    - ***Default Page***. Displays a drop-down list of pages. The selected page will automatically appear when you log in.
    - ***Page Refresh Rate***. Specifies how often Event, Ticket, and Views pages in SL1 will be refreshed. The possible choices are from 10 seconds to 60 minutes.
    - ***Page Result Count***. Specifies the number of results to be displayed on each page. The choices are 25 to 500.
    - ***Table Row Height***. Affects the row height of all pages that display a table in the main content pane. You can also change this setting in the **Event Console Preferences** page and the **Ticket Console Preferences** page. Changing the setting for row height in this page, the **Event Console Preferences** page and the **Ticket Console Preferences** page affects the row height in all pages that display a table in the main content pane. Choices are:

        - *Small*. Sets row height to 17 px and font size to 11 px.
        - *Medium*. Sets row height to 27 px and font size to 12 px.
        - *Large*. Sets row height to 35 px and font size to 13 px.

    - ***Default Severity Filter***. When a severity is selected, you will see only events of the selected severity and greater in the **Event Console** page.

        - *Healthy*. Will display all events, including events with a severity of Healthy.
        - *Notice*. Will display all events with a severity of Notice, Major, Minor, and Critical.
        - *Minor*. Will display all events with a severity of Minor, Major, and Critical.
        - *Major*. Will display all events with a severity of Major and Critical.
        - *Critical*. Will display all events with a severity of Critical

- ***Preferred IF Label***. Specifies how interfaces will be labeled in all pages and reports that reference network interfaces.

    - *Interface Alias*. Easy-to-remember, human-readable name for the network interface.
    - *Interface Name*. The name of the network interface.

- ***Default Interface Graph Display***. Specifies the default unit of measure for the Hourly Interface Usage graph in the **Device Summary** page. Choices are:

    - *Interface Default*. The Hourly Interface Usage graph displays the amount traffic in the unit of measure specified in the ***Measurement*** field in the **Interface Properties** page for the interface.
    - *% Utilization*. The Hourly Interface Usage graph displays utilization in percent.

- ***Default Date Format***. Specifies the default date format that will be used throughout SL1. You can select from a list of possible formats.
- ***Date Format String.*** Specifies a user-defined date format that will be used throughout SL1. If defined, this date format overrides the default date format. Any date variables supported by the PHP date function can be used.
- ***Disable NavBar Auto-hide***. If you select this checkbox, the NavBar pane persists after you click a link. This option is selected by default.
- ***View Assigned Tickets Only***. If you select this checkbox, by default, only tickets assigned to you are displayed in the **Ticket Console** page.
- ***Show Masked Events***. If you select this checkbox, all events that have been grouped together under a single event description will be displayed in the **Event Console** page. The default behavior of SL1 is to roll up related events under a single description.
- ***Organizational Grouping Events***. If you select this checkbox, events will be grouped by organization in the **Event Console** page. The filter-while-you-type fields and the advanced filter tool will appear for each organization grouping and will act only on the events in that organization grouping. You will not be able to apply a single filter to events in multiple organizations.
- ***Collapse Organization Events***. If you select this checkbox, all organizations with assigned events will be displayed but will be contracted; the **Event Console** page will display only a list of contracted organizations, which can be expanded by clicking on the plus sign (+). The default behavior of SL1 is to expand each organization and display the list of events for each organization.
- ***Show Severity Badges***. If you select this checkbox:

    - The value in the ***Severity*** column will be displayed as a color-coded badge in the **Event Console** page and the **Ticket Console** page.
    - The value in the ***Current State*** column will be displayed as a color-coded badge in the **Device Manager** page.

    If you do not select the ***Show Severity Badges*** checkbox:

- In the **Event Console** page, the value in the ***Event Message*** column and the value in the ***Severity*** column will be painted with the severity color.
- In the **Ticket Console** page, the value in the ***Description*** column and the ***Severity*** column will be painted with the severity color.
- In the **Device Manager** page, the value in the ***Device Name*** column and the value in the ***Current State*** column will be painted with the severity color.

- ***Ticket Comment Reverse Sort***. In the Notes section of a ticket, sort notes by newest first. If you do not select this checkbox, the user interface displays ticket notes from oldest to newest, with oldest displayed first.
- ***Disabled Ticket Comment Cloaking***. When you add comments to a ticket, by default the comments are viewable by all (not cloaked).
- ***Scale Percent Graphs to 100%***. Graphs that display percentage on the y-axis will display from 0% to 100%, regardless of the highest actual value. Default behavior is to display from 0% to highest actual value.
- ***Code Highlighting***. If selected, enables syntax highlighting in areas of SL1 that display HTML, PHP, Python, and SQL code. If selected, syntax highlighting appears in:
  - The **Snippet Editor & Registry** page for Dynamic Applications of type "snippet" (System > Manage > Applications > create/edit > Snippets).
  - The **Dashboard Widget Editor** page (System > Customize > Dashboards > Widgets > create/edit).
  - The **Database Tool** page (System > Tools > DB Tool).

    NOTE: The **Database Tool** page is available only in versions of SL1 prior to 12.2.1 and displays only for users that have sufficient permissions to access the page.

  - The **Action Policy Editor** page for actions of type "Snippet" and "SQL Query" (Registry > Run Book > Actions > create/edit).
  - The **Report Template Editor** page (Reports > Management > Report Manager > create/edit).
- ***Hide Empty Networks***. If you select this checkbox, the **IPv4 Networks** page hides networks that do not include any devices or interfaces.
- ***Event Console Columns***. In this list, the you can select the default columns to be displayed in the **Event Console** page.
- ***Ticket Manager Columns***. In this list, you can select the default columns to be displayed in the **Ticket Console** page. You can still override these default columns by specifying Console Preferences while in the **Ticket Console** page.
- ***Device Manager Columns***. In this list, you can select the default columns to be displayed in the

Device Manager page.

> **NOTE:** Hidden field values do not change when you make changes to the fields on this page.

5. Click the **[Save]** button to save your changes.

Editing the User's Work Schedule

The **Schedule Manager** page (Registry > Accounts > User Accounts > wrench icon > Schedule) allows you to enter one-time and recurring appointments, meetings, and vacation leave for the user.

You can use the **Schedule Manager** page to specify the following:

- Normal work schedule for the user (for example, in the office on Monday – Friday, but out of the office on Saturday and Sunday)
- Vacation time for the user
- Recurring meetings and appointments (for example, a weekly status meeting that occurs every Tuesday)
- One-time meetings and appointments (for example, a doctor's appointment)

> **NOTE:** You can also view and manage all scheduled processes from the **Schedule Manager** page (Registry > Schedules > Schedule Manager). For more information, see the ***System Administration*** manual.

Viewing the Schedule Manager

The **Schedule Manager** page (Registry > Accounts > User Accounts > wrench icon > Schedule) displays the following information about one-time and recurring appointments, meetings, and vacation leave for the user:

- ***Schedule Summary***. Displays the name assigned to the scheduled process.
- ***Schedule Description***. Displays a description of the scheduled process.
- ***Event ID***. Displays a unique, numeric ID for the scheduled process. SL1 automatically creates this ID for each scheduled process.
- ***sch id***. Displays a unique, numeric ID for the schedule. SL1 automatically creates this ID for each schedule.
- ***Context***. Displays the area of SL1 upon which the schedule works.
- ***Timezone***. Displays the time zone associated with the scheduled process.
- ***Start Time***. Displays the date and time at which the scheduled process will begin.
- ***Duration***. Displays the duration, in minutes, which the scheduled process occurs.
- ***Recurrence Interval***. If applicable, displays the interval at which the scheduled process recurs.
- ***End Date***. If applicable, displays the date and time on which the scheduled process will recur.

- ***Last Run***. If applicable, displays the date and time the scheduled process most recently ran.
- ***Owner***. Displays the username of the owner of the scheduled process.
- ***Organization***. Displays the organization to which the scheduled process is assigned.
- ***Visibility***. Displays the visibility level for the scheduled process. Possible values are "Private", "Organization", or "World".
- ***Enabled***. Specifies if the scheduled process is enabled. Possible values are "Yes" or "No".

To edit scheduled or recurring appointments, meetings, and vacation leave for the user, click its wrench icon () and update the item as needed on the **Schedule Editor** modal page. (For more information, see the section *Defining a Scheduled or Recurring Calendar Item*.)

Defining a Scheduled or Recurring Calendar Item

You can add a scheduled or recurring meeting, appointment, or vacation for the user in the **Schedule Manager** page.

To define a scheduled or recurring meeting, appointment, or vacation:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. In the **User Accounts** page, find the user account you want to edit. Click its wrench icon().
3. Click the **[Schedule]** tab. The **Schedule Manager** modal page appears.
4. Click **[Create]**. The **Schedule Editor** modal page appears.
5. On the **Schedule Editor** modal page, make entries in the following fields:

Basic Settings

- ***Schedule Name***. Type a name for the scheduled process.
- ***Schedule Type***. Indicates the scheduled process type (such as Tickets, Reports, or Devices).
- ***Visibility***. Select the visibility for the scheduled process. You can select one of the following:
    - *Private*. The scheduled process is visible only to the owner selected in the ***Owner*** field.
    - *Organization*. The scheduled process is visible only to the organization selected in the ***Organization*** field.
    - *World*. The scheduled process is visible to all users.
- ***Organization***. Select the organization to which you want to assign the scheduled process.
- ***Owner***. Select the owner of the scheduled process. The default value is the username of the user who created the scheduled process.
- ***Preserve Schedule***. Select this checkbox to exclude this schedule from being pruned after expiration.
- ***Description***. Type a description of the scheduled process.

Time Settings

- ***Start Time***. Click in the field and select the date and time you want the scheduled process to start.
- ***End Time***. Click in the field and select the date and time you want the scheduled process to end.
- ***Time Zone***. Select the region or time zone for the scheduled start time.

> **NOTE:** If you want SL1 to automatically adjust for daylight savings time (if applicable), then you must select a named region (such as *America/New York*) in the ***Time Zone*** field. If you select a specific time zone (such as *EST*) or a specific time offset (such as *GMT-5*), then SL1 will not automatically adjust for daylight savings time. In addition, if you select a specific time zone, such as *EST*, that does not exist during daylight savings time observance, your schedules will be saved and execute at unexpected times.

- ***All Day***. Select this checkbox if the scheduled process occurs all day rather than during a specific period of time. If you do so, the ***End Time*** field becomes disabled.
- ***Recurrence***. Select whether you want the scheduled process to occur once or on a recurring basis. You can select one of the following:
    - *None*. The scheduled process occurs only once.
    - *By Interval*. The scheduled process recurs at a specific interval.
    - *Every Xth day of the Week*. The scheduled process occurs at a monthly interval based on a day of the week. The day of the week displayed in this option matched the day selected in the ***Start Time*** field. For example, if you set the ***Start Time*** to Thursday, August 5th and that day is the first Thursday of the month, then the recurrence option will be *Every 1st Thursday*, and the scheduled process will occur monthly on the first Thursday of the month.

If you select *By Interval*, the following additional fields appear:

- ***Interval***. In the first field, enter a number representing the frequency of the scheduled process, then select the time interval in the second field. Choices are *Minutes*, *Hours*, *Days*, *Weeks*, or *Months*. For example:
    - If you specify "6 Hours", then the scheduled process recurs every six hours from the time listed in the ***Start Time*** field.
    - If you specify "10 Days", then the scheduled process recurs every 10 days from the date listed in the ***Start Time*** field.
    - If you specify "2 Weeks", then the scheduled process recurs every two weeks, on the same day of the week as the ***Start Time***.
    - If you specify "3 Months" the ticket recurs every three months, on the same day of the month as the ***Start Time***.

- ***Recur Until***. Specifies when the scheduled process stops recurring. You can select one of the following:

  - *No Limit*. The scheduled process recurs indefinitely until it is disabled.
  - *Specified Date*. The scheduled process recurs until a specific date and time. If you select *Specified Date*, you must select a date and time in the ***Last Recurrence*** field.

- ***Last Recurrence***. Click in the field and select the date and time you want the scheduled process to stop recurring.

6. Click **[Save]**.

Enabling or Disabling One or More Scheduled Calendar Items

You can enable or disable one or more scheduled or recurring meetings, appointments, or vacations from the **Schedule Manager** page (Registry > Accounts > User Accounts > wrench icon > Schedule). To do this:

1. Go to the **Schedule Manager** page (Registry > Accounts > User Accounts > wrench icon > Schedule).
2. Select the checkbox icon for each scheduled process you want to enable or disable.
3. Click the ***Select Action*** menu and choose *Enable Schedules* or *Disable Schedules*.
4. Click the **[Go]** button.

Deleting One or More Scheduled Calendar Items

You can delete one or more scheduled or recurring meetings, appointments, or vacations from the **Schedule Manager** page (Registry > Accounts > User Accounts > wrench icon > Schedule). To do this:

1. Go to the **Schedule Manager** page (Registry > Accounts > User Accounts > wrench icon > Schedule).
2. Select the checkbox icon for each scheduled process you want to delete.
3. Click the ***Select Action*** menu and choose *Delete Schedules*.
4. Click the **[Go]** button.

Creating a Ticket about a User Account

A ***ticket*** is a request for work. Tickets allow you to monitor required work-tasks associated with your network.

You can create a ticket about a user account. For example, to delete an old account or to change the parameters of a current account.

To create a ticket about a user account:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. In the **User Accounts** page, find the account for which you want to generate a report. Click its ticket icon ( ).

3. The **Ticket Editor** page appears.
4. In the **Ticket Editor** page, supply a value in each field.

    - ***Organization***. Select the organization with which the ticket will be associated. You can select from a list of all organizations that you are a member of.
    - ***Ticket Description***. Description of the problem or ticket. If you create a ticket from an event in the **Event Console**, this field is populated automatically by SL1.
    - ***Sub-Organization***. Select a second organization with which the ticket will be associated.
    - ***Ticket State***. Custom parameter, defined in the **Ticket States** page (Registry > Ticketing > Custom States). Allows you to add additional workflow restrictions to a ticket.
    - ***Severity***. The severity of the problem. If you create a ticket from an event in the **Event Console**, this field is populated automatically by SL1 with the event's severity. The choices are:

        - Severity 0/Healthy
        - Severity 1/Notice
        - Severity 2/Minor
        - Severity 3/Major
        - Severity 4/Critical

    - ***Category***. Descriptive category assigned to the ticket. You can use the **Select Objects Editor** page (System > Customize > Select Objects) to customize the list of possible categories.
    - ***Source***. Original source for the ticket. You can use the **Select Objects Editor** page (System > Customize > Select Objects) to customize the list of possible sources. Choices are:

        - *Automated*. Ticket was created automatically when an event occurred.
        - *Email*. An email about an issue prompted this ticket.
        - *External*. An external source created this ticket.
        - *Internal*. Ticket created in SL1.
        - *Phone*. A phone call about an issue prompted this ticket.

    - ***Queue***. Ticket Queue to which the ticket will be assigned.
    - ***Assigned User***. User who is responsible for resolving the ticket. This drop-down list contains entries for each user assigned to the specified Ticket Queue and who has a Login State of *Active*. When a ticket is assigned to a user, SL1 automatically sends the user an email message as notification.
    - ***Custom Fields***. If your SL1 system includes embedded custom fields for tickets, you can supply a value in those fields.
    - ***Notes & Attachments***. The **Notes & Attachments** pane in the **Ticket Editor** page allows you to enter notes or comments about a ticket, insert content from a saved template, or to add images, videos, or attachments to the ticket.

- To add a note to a ticket, click the **[New Note]** button in the **Ticket Editor** page. A new instance of the **Notepad Editor** will appear in the **Notes & Attachments** pane. To edit a note, click the wrench icon () for the note you want to edit.
- To add an attachment to a note, click the paperclip icon (), and then click the **[Browse]** button to choose the file you want to attach to the note.

5. Click the **[Save]** button to save the new ticket.

Chapter 11

External Contacts

Overview

An external contact is a user to whom SL1 can send email messages (service notifications and ticket notifications) from SL1. External contacts do not have ScienceLogic accounts and cannot login to SL1. Like ScienceLogic users, external contacts are associated with organizations.

Each external contact can be included in distribution lists, service notifications, and in the list of possible ticket watchers for either the external contact's organization, or for individual tickets in the external contact's organization.

The **External Contacts** page allows you to view a list of existing external contact accounts, edit their properties, and define new external contact accounts.

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:

Viewing the List of External Contacts

The **External Contacts** page allows you to view a list of existing external contact accounts.

To view external contacts:

1. Go to the **External Contacts** page (Registry > Accounts > External Contacts).
2. The **External Contacts** page displays the following about each external contact account:

> **TIP:** To sort the list of external contacts, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again. The ***Last Edited*** column sorts by descending order on the first click; to sort by ascending order, click the column heading again.

- ***Last Name | First Name***. Last name and first name of the external contact.
- ***Organization***. Organization associated with the external contact account.
- ***Email Address***. Email address associated with the external contact account.
- ***City***. City associated with the external contact account.
- ***State***. State associated with the external contact account.
- ***Postal Code***. Postal code associated with the external contact account.
- ***Phone Number***. Phone number associated with the external contact account.
- ***Contact ID***. Unique, numeric ID, automatically assigned to each external contact account by SL1.
- ***Last Edited***. Date and time the external contact account was created or last edited.

Filtering the List of External Contacts

The **External Contacts** page includes nine filters, at the top of the registry. You can filter the list of external contacts by one or multiple of the following parameters: last name | first name, primary organization, email address, city, state, postal code, phone number, contact ID, and last edited. You can specify one or more parameters to filter the display of external contacts. Only external contacts that meet all the filter criteria will be displayed in the **External Contacts** page.

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

- For each filter except ***Last Edited***, you must enter text to match against. SL1 will search for external contacts that match the text, including partial matches. Text matches are not case-sensitive. You can use the following special characters in each filter:

  - , (comma). Specifies an "or" operation. For example:

    dell, micro

    would match all values that contain the string "dell" OR the string "micro".

  - ! (exclamation mark). Specifies a "not" operation. For example:

    !dell

would match all values that do not contain the string "dell".

- ***Last Name | First Name***. You can enter text to match, including special characters, and the **External Contacts** page will display only external contacts that have a matching last name or a first name, or both.
- ***Organization***. You can enter text to match, including special characters, and the **External Contacts** page will display only external contacts that have a matching primary organization.
- ***Email Address***. You can enter text to match, including special characters, and the **External Contacts** page will display only external contacts that have a matching email address.
- ***City***. You can enter text to match, including special characters, and the **External Contacts** page will display only external contacts that have a matching city in their addresses.
- ***State***. You can enter text to match, including special characters, and the **External Contacts** page will display only external contacts that have a matching state in their addresses (for example, California, Massachusetts, Virginia, etc.).
- ***Postal Code***. You can enter text to match, including special characters, and the **External Contacts** page will display only external contacts that have a matching postal code in their addresses.
- ***Contact ID***. You can enter text to match, including special characters, and the **External Contacts** page will display only external contacts that have a matching ID.
- ***Last Edited***. You can select from a list of time periods. The **External Contacts** page will display only external contacts that have been created or edited within that time period.

Creating and Editing an External Contact

You can create an external contact from the **External Contacts** page. To create an external contact:

1. Go to the**External Contacts** page (Registry > Accounts > External Contacts).
2. In the **External Contacts** page, click the **[Create]** button.
3. The **Create New External Contact** page appears, where you can define values in the following fields:
    - ***First Name***. Contact's first name. This value can be up to 24 characters in length.
    - ***Last Name***. Contact's last name. This value can be up to 24 characters in length.
    - ***Title***. Contact's title. This field can be up to 32 characters in length.
    - ***Department***. Contact's department. This field can be up to 36 characters in length.
    - ***Phone***. Contact's phone number at work. This field can be up to 24 characters in length.
    - ***Fax***. Contact's fax number at work. This field can be up to 24 characters in length.
    - ***Mobile***. Contact's cell phone number. This field can be up to 24 characters in length.
    - ***Pager***. Any other phone numbers for contacting the person. This field can be up to 24 characters in length.
    - ***Primary Email***. Contact's primary email address. This field can be up to 64 characters in length.

- ***Secondary Email***. Additional email address for contacting the person. This field can be up to 64 characters in length.
- ***Alternate Email***. Additional email address for contacting the person. This field can be up to 64 characters in length.
- ***Street Address***. Contact's street address at work. This field can be up to 64 characters in length.
- ***Suite/Building***. Suite/Building for the person at work. This field can be up to 64 characters in length.
- ***City***. City where the person works. This field can be up to 64 characters in length.
- ***State***. State where the person works.
- ***Postal Code***. Zip code where the person works. This field can be up to 12 characters in length.
- ***Country***. Country where the person works.

> NOTE: By default, the ***Country*** field will be set to the country specified in the **Behavior Settings** page (System > Settings > Behavior). You can override this setting for the current external contact. Editing the value in this field will not affect the system-wide default setting.

- ***Toll Free***. Toll-free phone number for the person. This field can be up to 24 characters in length.
- ***Organization***. Organization to associate with the person. Select from a list of all organizations in SL1.
- ***Key Role***. Description of the Contact's responsibilities in case of a critical situation. This description might differ from the Contact's actual title. For example, a contact's title might be Senior Engineer, but his/her role for the organization might be technical lead. Select from the drop-down list. (SL1 system administrators can go to the System > Customize > Select Objects page to customize the entries that appear in this list) If a value is supplied in this field, the contact will appear as a Critical Contact for the Organization in the **Organization Properties** page.
- ***Critical Contact***. Circumstance when person should be contacted. This description might differ from the Contact's department. For example, the Contact's department might be Operations, but his/her role for the organization might be Hardware Maintenance. Select from the drop-down list. (SL1 system administrators can go to the System > Customize > Select Objects page to customize the entries that appear in this list) If a value is supplied in this field, the contact will appear as a Critical Contact for the Organization in the **Organization Properties** page.
- ***Pass Phrase***. Questions that verifies a contact who has forgotten his/her password. SL1 does not use this field.
    - What is your Mother's maiden name?
    - What is your favorite pet's name?
    - What is your favorite color?
- ***Answer***. This field contains the answer to the question selected in the ***Pass Phrase*** field. This field can be up to 64 characters in length.

- ***Time Zone***. Time zone associated with the Contact's location. Select from a list of all time zones.
- ***Billing ID***. Billing ID associated with this contact. This field can be up to 24 characters in length.
- ***CRM ID***. CRM ID associated with this contact. This field can be up to 64 characters in length.
- ***Notes***. Any notes you want to include with the contact's profile information.

4. After you have defined fields in the **Create New External Contact** modal page, click the **[Save]** button to save the external contact.

Editing an External Contact

You can edit an external contact from the **External Contacts** page. To edit an external contact:

1. Go to the **External Contacts** page (Registry > Accounts > External Contacts).
2. In the **External Contacts** page, find the external contact you want to edit. Click its wrench icon ().
3. The **External Contact Information** page appears. You can edit any of the fields described above.
4. Click the **[Save]** button to save your edits.

Deleting One or More External Contacts

You can delete one or more external contact accounts from the **External Contacts** page. To delete one or more external contact accounts:

1. Go to the **External Contacts** page (Registry > Accounts > External Contacts).
2. In the **External Contacts** page, select the checkbox for each external contact account that you want to delete. To select all checkboxes for all organizations, select the checkbox icon (☑) at the top of the page.
3. In the ***Select Action*** drop-down list, select *DELETE External Contacts*.
4. Click the **[Go]** button to delete the contact(s).

Adding External Contacts to a Distribution List

A distribution list is a list of users, external contacts, and/or vendors to whom you want to send email messages from SL1. The list can include both rules and manually added accounts. The rules allow the distribution list to be dynamically updated. For example, suppose one of the rules for a distribution list is "include all external contact accounts in the organization named Central NOC." You could then add or remove external contacts from the organization, and the distribution list would include only the current external contact accounts in the organization.

Distribution lists are used in the **Service Notifier** page. The **Service Notifier** page allows you to send a message from SL1. The message can include text, screen captures, and attached files. The message can be sent to manually entered email addresses, distribution lists, and manually selected users, external contact accounts, and vendors.

To learn more about adding an external contact to a distribution list, see the manual ***Business Services***.

Adding External Contacts to a Service Notification

The **Service Notifier** page allows you to send a message from SL1. The message can include text, screen captures, and attached files. The message can be sent to manually entered email addresses, distribution lists, and manually selected users, external contact accounts, and vendors.

If you include an external contact account in a distribution list, you can send a service notification to the external contact by sending a service notification to that distribution list.

To learn more about adding an external contact to a service notification, see the manual ***Business Services***.

Chapter 12

Lockouts

Overview

A lockout is a security measure, to prevent the SL1 user interface from being hacked.

If a user enters incorrect login information multiple times in a row, that username, the user's IP address, or both will be locked out of SL1. Until an administrator removes the lockout, that user will not be able to log in to 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:

System Settings that Define Lockouts

You can define how lockouts behave in your specific ScienceLogic environment.

You can define global settings that control when a lockout is triggered, how long the lockout will last, and if the offending user is locked out by name, by IP address, or by both.

To define lockout behavior:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).
2. The **Behavior Settings** page appears.
3. Supply values in these fields:
    - ***Account Lockout Type***. If a user enters incorrect login information multiple times in a row, that user will be locked out of SL1. In this field, you can select how the lockout will be applied. Choices are:
        - *Lockout by IP Address (default)*. All login attempts from the IP address will be denied.
        - *Lockout by Username and IP Address*. All login attempts by the username from the IP address will be denied.
        - *Lockout by Username*. All login attempts by the username will be denied.
        - *Disabled*. Lockouts are disabled.
    - ***Account Lockout Attempts***. Number of times a user can enter incorrect login information before the lockout occurs. Choices are 1 time through 10 times.
    - ***Account Lockout Duration***. Specifies how long a user will be locked out of SL1. Choices are from 1 hour to 24 hours, in 1 hour increments.
    - ***Lockout Contact Information***. This contact information will be displayed when a user is locked out of SL1. Can be any combination of alphanumeric characters, up to 255 characters in length. This information should allow the user to contact his/her administrator to unlock the account.
4. Click the **[Save]** button to save your changes to the lockout settings.

Viewing a List of Lockouts and Removing a Lockout

You can view a list of user accounts that are currently locked out of SL1.

To view the list of current lockouts:

1. Go to the **Access Sessions** page (System > Monitor > Access Logs).
2. In the **Access Sessions** page, click the **[Lockouts]** button.
3. The **Access Lockouts** page appears, displaying a list of user accounts that are currently locked out of SL1.

Removing a Lockout

You can view a list of user accounts that are currently locked out of SL1 and remove one or more users from lockout mode. This allows the user account to once again log in to SL1.

To view the list of current lockouts and remove one or more users from lockout mode:

1. Go to the **Access Sessions** page (System > Monitor > Access Logs).
2. In the **Access Sessions** page, click the **[Lockouts]** button.
3. The **Access Lockouts** page appears, displaying a list of user accounts that are currently locked out of SL1.
4. Find the lockout you want to remove. Click its bomb icon ().
5. The user account will now be able to log in to SL1 again.

Chapter 13

Reports for User Accounts

Overview

SL1 allows you to generate reports based on user accounts. You can generate two type of reports based on user accounts:

- A report based on all or multiple user accounts.
- A report based on a single user account.

This chapter describes how to generate each type of report.

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:

Generating a Report for Multiple User Accounts

From the **User Accounts** page you can generate a report that displays information for all or multiple user accounts in SL1. The report will contain all the information displayed in the **User Accounts** page.

To generate a report on all or multiple user accounts:

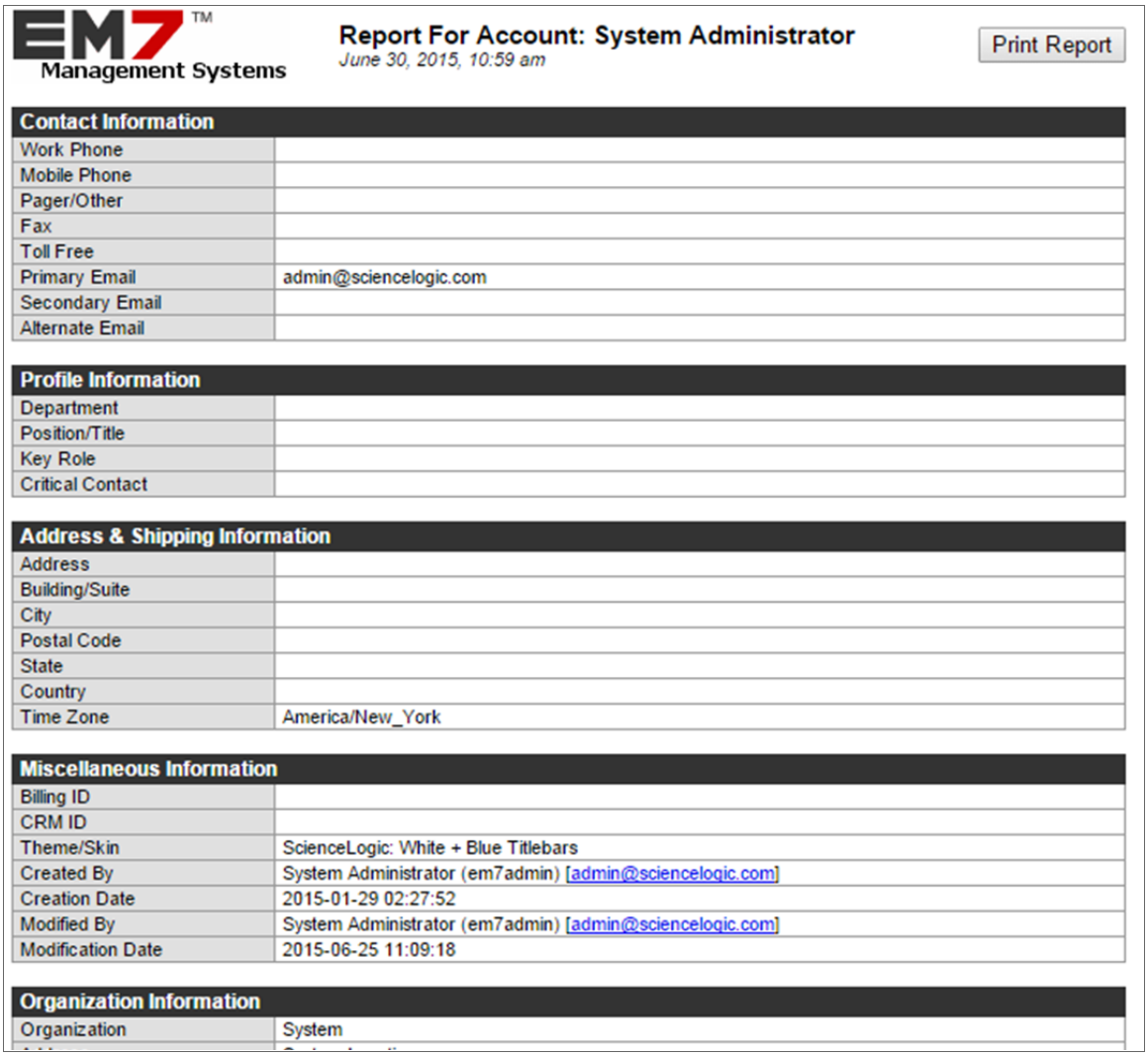
1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. In the **User Accounts** page, click the **[Report]** button. The **Export current view as a report** modal page appears.

> **NOTE**: If you want to include only certain interfaces in the report, use the "search as you type" fields at the top of each column. You can filter the list by one or more column headings. You can then click the **[Report]** button, and only the user accounts displayed in the **User Accounts** page will appear in the report.

3. In the **Export current view as a report** modal page, you must select the format in which SL1 will generate the report. Your choices are:
   - Comma-separated values (.csv)
   - Web page (.html)
   - Open Document Spreadsheet (.ods)
   - Excel spreadsheet (.xlsx)
   - Acrobat document (.pdf)
4. Click the **[Generate]** button. The report will contain all the information displayed in the **User Accounts** page. You can immediately view the report or save it to a file for later viewing.

Generating a Report for a Single User Account

You can also generate a report that displays information for a single user account in SL1.



EM7 Management Systems

Report For Account: System Administrator

June 30, 2015, 10:59 am

Print Report

Contact Information	
Work Phone	
Mobile Phone	
Pager/Other	
Fax	
Toll Free	
Primary Email	admin@sciencelogic.com
Secondary Email	
Alternate Email	

Profile Information	
Department	
Position/Title	
Key Role	
Critical Contact	

Address & Shipping Information	
Address	
Building/Suite	
City	
Postal Code	
State	
Country	
Time Zone	America/New_York

Miscellaneous Information	
Billing ID	
CRM ID	
Theme/Skin	ScienceLogic: White + Blue Titlebars
Created By	System Administrator (em7admin) [admin@sciencelogic.com]
Creation Date	2015-01-29 02:27:52
Modified By	System Administrator (em7admin) [admin@sciencelogic.com]
Modification Date	2015-06-25 11:09:18

Organization Information	
Organization	System

To generate a report on a single user account:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. In the **User Accounts** page, find the account for which you want to generate a report. Click the account's wrench icon () or its business card icon ().
3. Click the **[Report]** tab:
4. An HTML report appears, populated with data from the selected user account. You can print the report or right-click to save the HTML page.

Chapter 14

Logs

Overview

SL1 creates a log for each organization that displays a record of all actions pertaining to the organization. This chapter will demonstrate how to view logs and access logs for organizations.

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:

Viewing Logs for an Organization

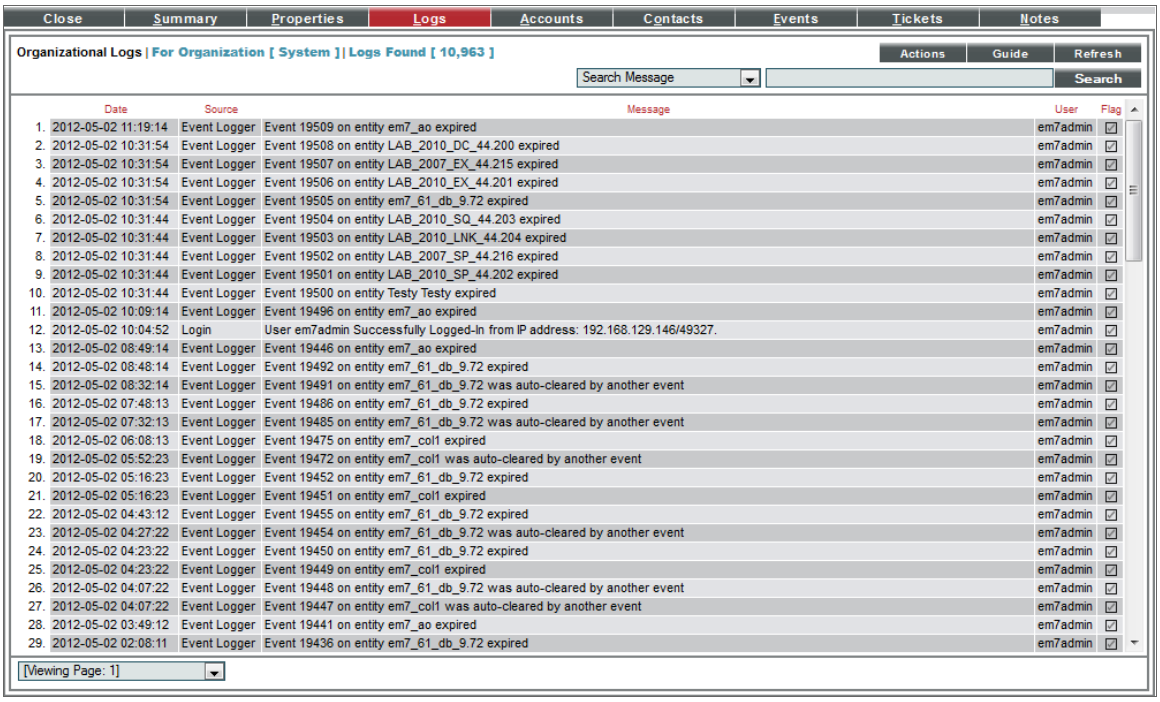
SL1 creates a log for each organization. Each organization log displays a record of all actions pertaining to the organization. These actions include:

- All logins by organization members.
- All notifications sent to organization members.
- Organization member creating, editing, or deleting anything in SL1.
- All events associated with an entity managed by the organization.

The **Organizational Administration** panel includes an **Organizational Logs** page, where you can view the entries for a specific organization. The **Organizational Logs** page provides a complete audit trail for an organization.

To view the **Organizational Logs** page for an organization:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. In the **Organizational Account Administration** page, find the organization you are interested in. Click its wrench icon ( ).
3. When the **Organizational Summary** page appears, click the **[Logs]** tab.
4. The **Organizational Logs** page appears. In this page, you can view the log entries for an organization. You can also search for log entries and flag log entries.



5. The **Organizational Logs** page displays the following for each log entry:
    - ***Date***. Date the action occurred and the log entry was created.
    - ***Source***. Source of the log entry.
    - ***Message***. Text of the log entry.
    - ***Flag***. Clicking on the flag checkmark changes the checkmark from red to black and appends the user's username to the checkmark. This aids in quickly finding the log entry.

Viewing Access Logs

SL1 allows you to monitor user logins and logouts to SL1. You can view:

- Which user accounts are currently logged in.
- From which IP address a user is/was logged in to SL1.
- The current status of each session (active, logged out, expired).
- How long each user was logged in to SL1.
- When each user logged out of SL1.

To view this information:

1. Go to the **Access Sessions** page (System > Monitor > Access Logs).
2. The **Access Sessions** page appears:
3. The **Access Sessions** page displays a list of recent logins to SL1. For each sessions, the **Access Sessions** page displays:
    - ***User Account***. User name of person logging in to SL1.
    - ***User Display Name***. User's username, email address, or preferred display name. This value is determined by the user's authentication resource settings.
    - ***Last Address***. IP address from which user accessed SL1.
    - ***State***. Current status of user in SL1. The possible states are:
        - *Active*. User is currently logged in to SL1.
        - *Expired*. User's session in SL1 was killed.
        - *Logged Out*. User logged out of SL1.
        - *Never Used*. User logged in to SL1 and did not perform any tasks before the session was killed.
    - ***Login Time***. Date and time at which the user logged in.
    - ***Last-Hit Time***. Date and time at which the user last loaded a page in SL1.

- ***Logout Time***. Date and time at which the user logged out.
- ***Session Duration***. Length of time between login and logout.

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.

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

International: +1-703-354-1010