



---

# Creating a Tiered Service Offering

ScienceLogic version 8.4.2

---

# Table of Contents

<b>Creating a Tiered Service Offering</b> .....	<b>3</b>
Levels of Service .....	4
Steps to Configure the Tiered Service .....	4
<b>Configuring Product SKUs</b> .....	<b>6</b>
Creating a Product SKU .....	7
Example Product SKU Definitions .....	7
<b>Configuring Device Templates</b> .....	<b>8</b>
Device Templates for a Monitoring Service .....	9
Example Silver-Level Net SNMP Template .....	9
Example Gold-Level Apache/Linux Web Server Template .....	12
<b>Configuring User Policies</b> .....	<b>16</b>
Using the Default User Policies .....	17
Editing a User Policy .....	18
Editing an Access Key .....	19
<b>Provisioning a New Customer</b> .....	<b>21</b>
Creating an Organization and Aligning Product SKUs .....	22
Creating a Discovery Session for Pingable Devices .....	24
Creating a Discovery Session that includes a Device Template .....	25
Creating a User Account .....	26

---

# Chapter

# 1

## Creating a Tiered Service Offering

---

### Overview



This manual describes how a service provider might configure SL1 to offer their customers a managed service for the devices that are hosted by the provider or on a customer site. In this example, there are three initial configuration steps:

1. Creating Product SKUs
2. Creating Device Templates
3. Creating User Policies

After performing the initial configuration, you can provision a new customer by:

1. Creating an Organization record.
2. Aligning Product SKUs to the Organization record.
3. Creating and running a Discovery Session that includes the appropriate device template.
4. Creating a user account for the customer.

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:

<a href="#">Levels of Service</a> .....	4
<a href="#">Steps to Configure the Tiered Service</a> .....	4

---

## Levels of Service

In this example, customers will be offered three tiers of service:

- Bronze, which includes the availability and latency monitoring that SL1 automatically performs for every device.
- Silver, which includes additional monitoring capabilities, including CPU, physical memory, file system and interface statistics collection.
- Gold, which includes more frequent Interface statistics collection and additional, device/application specific, collection. For example, gold-level monitoring for an Apache Web Server might include:
  - Port monitoring policies for ports 80 and 443.
  - A web content verification policy.
  - A system process monitoring policy for the "httpd" process.

---

## Steps to Configure the Tiered Service

This manual describes the following steps for creating and offering the example service:

1. **Creating Product SKUs.** In SL1, product SKUs are used to track the products and services that are associated with the devices, organizations, interfaces, and assets in the system. In this example, a product SKU is created for each type of device for each level of service. For example, this example includes a product SKU for "Gold Level Apache/Linux Server Monitoring". When a new customer is provisioned, the product SKUs for the services that they subscribed to are manually aligned with that customer's organization record.
2. **Creating Device Templates.** In SL1, device templates are used to save a set of parameters for monitoring a device. For example, a device template can specify the availability protocol, interface monitoring settings, and device/application-specific monitoring settings for a device. The device template can then be used to reconfigure multiple devices or device groups, or to specify the initial configuration for all devices discovered using a specific discovery session. In this example, a device template is configured for each type of device for each level of service. For example, this example includes a device template for "Gold Level Apache/Linux Web Servers". When a new customer is provisioned, the appropriate device template is selected in the discovery session(s) that will discover that customer's devices. If you select a device template in a discovery session, all monitoring settings in the device template are automatically applied to each discovered device.
3. **Creating User Policies.** In SL1, user policies allow you to define a set of user account properties and permissions to re-use for multiple user accounts. When you create a user account, you can use a user policy to quickly apply settings to the new user account. User policies have a dynamic relationship with their member user accounts. When you make a change to a user policy, the user accounts associated with that user policy are automatically updated. In this example, a single user policy is defined that grants customer-level access to the system. When a new customer is provisioned, the user policy is used to create a user account for the new customer.
4. **Provisioning a New Customer.** The following provisioning process is used in this example:

- An organization is created for the customer.
- The product SKUs for the services the customer subscribed to are aligned with the organization. Because each product SKU in this example specifies a service level and a type of device, a customer could subscribe to a different service level for each type of device. For example, a customer might subscribe to gold service for their MySQL Database Servers and silver service for their Apache/Linux Web Servers.
- A discovery session is created for each type of customer device. For example, one discovery session that includes all the customer's Apache Web Servers, one discovery session that includes all the customer's MySQL Database Servers, etc. The appropriate device template is selected based on the product SKU's listed in the customer's organization record.
- A user account is created for the customer. The pre-configured user policy is used to create the user account.

**NOTE:** This manual describes how to provision devices manually. You could configure an automatic provisioning process using the ScienceLogic API.

---

# Chapter

# 2



## Configuring Product SKUs

---

### Overview

In SL1, product SKUs are used to track the products and services that are associated with the devices, organizations, interfaces, and assets in the system. In this example, a product SKU is created for each type of device for each level of service. For example, this example includes a product SKU for "Gold Level Apache/Linux Server Monitoring". When a new customer is provisioned, the product SKUs for the services that they subscribed to are manually aligned with that customer's organization record.

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:

<i>Creating a Product SKU</i> .....	7
<i>Example Product SKU Definitions</i> .....	7

---

## Creating a Product SKU

To create a product SKU for this example, perform the following steps:

1. Go to the **Product Catalog** page (Registry > Business Services > Product Catalog).
2. Select the **[Create]** button in the top right of the page.
2. The **Add Product** page appears.
3. In the **Add Product** page, enter values in the following fields. See the [Example Product SKU Definitions](#) for section for a list of example values:
  - **Product Name**. Name of the product. For example, "Bronze Level Apache Web Server Monitoring".
  - **SKU Identifier**. A numeric identifier for the product based on your business requirements and processes.
  - **Product Class**. Description of the type of product. System administrators can select the plus icon or use the **Select Objects Editor** page (System > Customize > Select Objects) to customize the list of possible choices in this field.
  - **Addendum/Description**. Additional identification for the SKU. Can be up to 24 characters in length.
  - **For Entity Type**. The element for which you are creating a product. In this example, product SKUs are associated with customer organizations. Select *Organizations* in this field.
4. Select the **[Save]** button to save the new product SKU.
5. Optionally, you can track the cost for each service by entering values in the following fields and then selecting the **[Save]** button again:
  - **Non-Recurring Cost**. Any initial, non-recurring cost associated with the product. Can be up to 12 characters in length.
  - **Monthly Recurring Cost**. Monthly recurring cost associated with the product.

---

## Example Product SKU Definitions

The following table lists example values for product SKUs that match the device templates described in [Configuring Device Templates](#):

Product Name	Product Class	SKU Identifier	Addendum/Description
Bronze-Level Monitoring	Managed Network Management Services	BRNZ-ALL	Bronze: All Devices
Silver-Level Net-SNMP Monitoring	Managed Network Management Services	SILV-NETSNMP	Silver: Net-SNMP
Gold-Level Apache/Net-SNMP Monitoring	Managed Network Management Services	GOLD-APACHE	Gold: Apache/Net-SNMP

---

# Chapter

# 3

## Configuring Device Templates



---

### Overview

In SL1, device templates are used to save a set of parameters for monitoring a device. For example, a device template can specify the availability protocol, interface monitoring settings, and device/application-specific monitoring settings for a device. The device template can then be used to reconfigure multiple devices or device groups, or to specify the initial configuration for all devices discovered using a specific discovery session.

In this example, a device template is configured for each type of device for each level of service. For example, this example includes a device template for "Gold Level Apache/Linux Web Servers". When a new customer is provisioned, the appropriate device template is selected in the discovery session(s) that will discover that customer's devices. If you select a device template in a discovery session, all monitoring settings in the device template are automatically applied to each discovered device.

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

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

This chapter covers the following topics:

<a href="#">Device Templates for a Monitoring Service</a> .....	9
<a href="#">Example Silver-Level Net SNMP Template</a> .....	9
<a href="#">Example Gold-Level Apache/Linux Web Server Template</a> .....	12



---

## Device Templates for a Monitoring Service

To create device templates for your monitoring service, you need to determine:

- The levels of service that you want to offer and the monitoring capabilities that you want to include at each level.
- The types of devices that will be monitored. For a level of service, you might need to create a device template for each type of device. For example, if you include TCP/IP port monitoring with a particular level of service, you would need to create a device template for web servers (ports 80 and 443), mail servers (port 25), MySQL servers (port 3306), etc.

**TIP:** Try discovering some test devices to determine which Dynamic Applications, TCP/IP ports, system processes, Windows services, and other monitoring options are applicable for each type of device.

For the bronze level of service in this example, which includes availability and latency monitoring, no device template is required. To monitor availability and latency without collecting other statistics, e.g. interface, file system, CPU, and physical memory utilization, you can discover a device using only the ICMP (ping) protocol. For an example of how to create a discovery session that discovers devices using only the ICMP protocol ("pingable" devices), see [Provisioning a New Customer](#).

The following sections describe how to configure the silver level and gold level templates for this example.

---

## Example Silver-Level Net SNMP Template

In this example, the following monitors are included in the silver-level service:

- Availability and Latency statistics. SL1 will automatically perform these collections for all devices.
- File system utilization statistics. If an applicable device is discovered using SNMP, SL1 will automatically perform file system collection every 5 minutes.
- Interface utilization statistics. If an applicable device is discovered using SNMP, SL1 will automatically perform interface collection every 15 minutes.
- CPU utilization statistics. In SL1 systems, this collection is performed using Dynamic Applications. Dynamic Applications are customizable policies that tell the system what data to collect from devices, how to present that data, and when to generate alerts based on the data.
- Memory utilization statistics. In SL1 systems, this collection is performed using Dynamic Applications.

For a tiered service, you will want to limit what is monitored on each device; therefore, this example disables automatic alignment of Dynamic Applications during initial discovery. Instead, the Dynamic Applications for CPU and Memory utilization statistics are applied using a device template. This section describes how to configure a silver-level device template for devices that support Net-SNMP, which includes most Linux and Solaris devices.

To configure the example silver-level device template for Net-SNMP devices, perform the following steps:

1. Go to the **Configuration Templates** page (Registry > Devices > Templates) page.
2. Select the **[Create]** button. The **Device Template Editor** page is displayed:

The screenshot displays the 'Device Template Editor | Config Template Settings' interface. At the top, there are 'New' and 'Reset' buttons. Below is a 'Template Name' input field. A navigation bar includes tabs for 'Config', 'Interface', 'CV Policies', 'Port Policies', 'Svc Policies', 'Proc Policies', 'Dyn Apps', and 'Logs'. The 'Config' tab is active, showing three main sections: 'Access & Monitoring', 'Device Retention & Basic Thresholds', and 'Interface Inventory Settings'. 'Access & Monitoring' includes settings for Device Organization (AWS), SNMP Read (c0sm0s), Availability Protocol (TCP), Latency Protocol (TCP), Avail+Latency Alert (Disabled), Collection (Enabled), Coll. Type (Standard), Critical Ping (Disabled), and Event Mask (Disabled). 'Device Retention & Basic Thresholds' features sliders for System Latency (100 ms), Availability Packet Size (56 bytes), Availability Ping Count (1 pings), and rollup data retention periods (Daily Rollup Bandwidth Data: 730 days, Hourly Rollup Bandwidth Data: 120 days, Raw Performance Data: 7 days, Daily Rollup Performance Data: 730 days). 'Interface Inventory Settings' includes Interface Inventory Timeout (600000 ms) and Maximum Allowed Interfaces (10000). A 'Device Preferences' sidebar on the right contains checkboxes for Auto-Clear Events, Scan All IPs, Accept All Logs, Dynamic Discovery, Daily Port Scans, Preserve Hostname, Auto-Update, Disable Asset Update, and Bypass Interface Inventory. 'Save' and 'Save As' buttons are at the bottom.

By default, all fields in the **[Config]** tab are disabled and will not be modified for the devices to which the template is applied.

3. For a tiered service, you will want to limit what is monitored on each device. By default, the system will automatically attempt to align Dynamic Applications with each discovered device during nightly auto-discovery. To disable nightly auto-discovery for the devices to which this template is aligned, enable the following fields by selecting the field name:
  - **Dynamic Discovery**
  - **Auto-Update**

When you enable each field, they are unchecked by default. Un-checking these checkboxes for a device disables nightly auto-discovery for that device.

For this example, all the other fields in the **[Config]** tab are left disabled. During discovery, SL1 will supply appropriate default settings in these fields.

- To configure the Dynamic Applications that will be aligned to the devices to which this template is applied, select the **[Dyn Apps]** tab.

The screenshot shows the 'Device Template Editor' interface with the 'Dyn Apps' tab selected. The interface includes a 'Template Name' field at the top, a navigation bar with tabs for 'Config', 'Interface', 'CV Policies', 'Port Policies', 'Svc Policies', 'Proc Policies', 'Dyn Apps', and 'Logs'. The 'Dyn Apps' tab is active, displaying the following sections:

- Subtemplate Selection:** Contains a '+ Add New Dynamic App Sub-Template' button.
- Template Application Behavior:** Features a dropdown menu for 'Align Dynamic Application With' set to 'All devices (align new applications and update collection states)'.
- Dynamic Application Settings:** Includes a 'Dynamic Application' dropdown set to 'Alteon: Load Trending', a 'Credentials' dropdown set to 'Default SNMP credential', and a 'Poll Rate' dropdown set to 'Every 15 Minutes'.
- Dynamic Application Presentation Object(s):** A list of settings, all set to 'Enabled':
  - Concurrent Connections Per Port
  - Connection Rate Per Virtual Server
  - Port Bindings
  - ARP Entries
  - Real Server Current Sessions
- Dynamic Application Thresholds:** Three sliders for retention periods:
  - Raw Data Retention: 90 days
  - Daily Rollup Retention: 730 days
  - Hourly Rollup Retention: 365 days

At the bottom of the interface are 'Save' and 'Save As' buttons.

- In the **Subtemplate Selection** pane, select *Add New Dynamic App Sub-Template*.
- In the **Align Dynamic Application With** field, select *All devices*. The selected Dynamic Application will be aligned to all devices to which this template is applied.
- In the **Dynamic Application** field, select *Net-SNMP: CPU*. This Dynamic Application monitors CPU utilization on devices that support Net-SNMP. If you are configuring a device template for a different type of device, you could select a Dynamic Application that is applicable to that device in this field.
- To enable the **Credentials** field, select its label. The Net-SNMP: CPU Dynamic Application uses SNMP to collect data. Select *Default SNMP credential* in this field.
- To configure memory utilization collection, repeat steps 5 - 8, selecting *Net-SNMP: Physical Memory* in the **Dynamic Application** field.
- Enter a name for the template in the **Template Name** field. For example, "Silver-Level Net-SNMP".
- To save the device template, select the **[Save]** button.

## Example Gold-Level Apache/Linux Web Server Template

In this example, the gold-level service includes all monitoring included in the silver-level, plus more frequent Interface utilization collection and additional, device-specific collection. The template described in this section includes gold-level monitoring for an Apache Web Server running on a device that supports Net-SNMP. This example includes the following monitors in the gold-level service:

- Port monitoring policies for ports 80 and 443.
- A web content verification policy.
- A system process monitoring policy for the "httpd" process.

To configure the example gold-level template for an Apache Web Server running on a device that supports Net-SNMP, perform the following steps:

1. To include all monitoring included in the silver-level service, perform steps 1 - 9 listed in the [Example Silver-Level Net-SNMP Template](#) section.
2. To configure more frequent Interface collection, select the **[Interface]** tab.

The screenshot displays the 'Device Template Editor | Config Template Settings' window for a 'Cisco: CE Series' device. The 'Interface' tab is selected, showing the following configuration:

- Template Application Behavior:** Apply Settings To: [ All interfaces on device ]
- Interface Settings:**
  - Collection State: Disabled
  - Collection Frequency: 1 min.
  - Interface Alerting: Disabled
  - Rollover Alerting: Disabled
  - Collect Errors: Disabled
  - Collect Discards: Disabled
  - Measurement Scale: Kilo
  - Percentile Calculation: Accumulative
  - Counter Type: Counter 32
  - Percentile Factor: 100%
  - Auto Name Update: Disable
  - Interface Name Format: {name}
- Interface Thresholds:**
  - Inbound %: 65%
  - Outbound %: 65%
  - Inbound Bandwidth: 0 Mbps
  - Outbound Bandwidth: 0 Mbps
  - Inbound Errors: 1000 Pkts
  - Outbound Errors: 1000 Pkts
  - Inbound Discards: 1000 Pkts
  - Outbound Discards: 1000 Pkts
  - Inbound Error %: 1%
  - Outbound Error %: 1%

Buttons for 'Save' and 'Save As' are visible at the bottom.

3. In the **Apply Settings To** field, select *All interfaces on device*.
4. To enable the **Collection State** field, select its label. Select *Enabled* in this field.

5. To enable the **Collection Frequency** field, select its label. To perform more frequent collection for gold-level devices, select *5 min.* in this field.
6. To configure the port monitoring policies, select the **Port Policies** tab.

The screenshot shows the 'Device Template Editor | Editing Port Policy Subtemplates' window. At the top, there are 'New' and 'Reset' buttons. Below is a 'Template Name' input field. A navigation bar contains tabs for 'Config', 'Interface', 'CV Policies', 'Port Policies' (which is selected), 'Svc Policies', 'Proc Policies', 'Dyn Apps', and 'Logs'. The main area is split into two panes. The left pane, titled 'Subtemplate Selection', contains a '+ Add New Port Sub-Template' button. The right pane, titled 'Template Application Behavior', has an 'Add Policy To' dropdown set to 'Only devices whose IP(s) have a matching port' and a 'Per-IP Policy Creation' dropdown set to '[ Management IP only ]'. Below this is the 'Port Policy Definition' section with several fields: 'Port / Service' (set to '1 / tcpmux'), 'State' (set to 'Disabled'), 'Method' (set to 'Port Scan (NMAP)'), 'Critical Poll' (set to 'Disabled'), and 'Timeout (ms)' (empty). At the bottom of the right pane are 'Save' and 'Save As' buttons.

7. In the **Subtemplate Selection** pane, select *Add New Port Sub-Template*.
8. In the Port / Service field, select 80 / http. Leave all fields set to the default values, which will add the policy to the management IP address for all devices to which the template is applied. SL1 will collect availability information for the port every 5 minutes.
9. In the **Subtemplate Selection** pane, select *Add New Port Sub-Template*.
10. In the Port / Service field, select 443 / https. Leave all fields set to the default values, which will add the policy to the management IP address for all devices to which the template is applied. SL1 will collect availability information for the port every 5 minutes.

11. To configure the web content monitoring policy, select the **CV Policies** tab.

The screenshot shows the 'Device Template Editor | Editing CV Policy Subtemplates' interface. At the top, there are 'New' and 'Reset' buttons. Below is a 'Template Name' input field. A navigation bar contains tabs for 'Config', 'Interface', 'CV Policies' (which is selected), 'Port Policies', 'Svc Policies', 'Proc Policies', 'Dyn Apps', and 'Logs'. On the left, the 'Subtemplate Selection' pane has a '+ Add New CV Sub-Template' button. The main configuration area is divided into two columns. The left column contains fields for: Policy Name, State (set to 'Disabled'), Port, Timeout (set to '1 Sec.'), Uniform Resource Locator (URL), Post String, Cookie Value, Browser Emulation (User Agent) (set to 'None'), Min Page size (Kb), Max Page Size (kb), Min Download Speed (kb/s), Max nslookup time (msec), Max TCP connect time (msec), and Max overall transaction time (msec). The right column contains fields for: HTTP Auth Username:Password, HTTP Auth Method (set to 'Default'), SSL Encryption (set to 'Disabled'), Expression Check #1 (case sensitive), Expression Check #2 (case sensitive), Error Code (set to 'n/a'), Referrer String, Host Resolution, Proxy Server:Port, Proxy Username:Password, and Proxy Auth Method (set to 'Default'). At the bottom, there are 'Save' and 'Save As' buttons.

12. In the **Subtemplate Selection** pane, select *Add New CV Sub-Template*.

13. Supply values in the following fields:

- **Policy Name.** Enter a name for the policy in this field. For example "Standard Gold-Level Monitor".
- **State.** Select *Enabled* in this field.
- **Uniform Resource Locator (URL).** Enter "http://%D" in this field. When SL1 performs collection for this policy, the IP address of the device for which collection is being performed will be substituted in to the %D value.
- **Error Code.** If you expect all monitored devices to return a specific HTTP status code, select that status code in this field. This example assumes all monitored devices will return the most common healthy status code. Select *200 OK* in this field. SL1 will generate an alert if a web site returns a status code other than the one selected.

**NOTE:** This example does not have specific requirements for the other settings defined in this page. You can leave the remaining fields set to the default values.

14. To configure the system process monitoring policy, select the **Proc Policies** tab.

The screenshot shows the 'Device Template Editor | Editing Process Policy Subtemplates' window. At the top, there are 'New' and 'Reset' buttons. Below is a 'Template Name' input field. A navigation bar contains tabs for 'Config', 'Interface', 'CV Policies', 'Port Policies', 'Svc Policies', 'Proc Policies' (which is selected), 'Dyn Apps', and 'Logs'. The main area is split into two panes. The left pane, 'Subtemplate Selection', has a green plus icon and the text 'Add New Process Sub-Template'. The right pane, 'Template Application Behavior', contains several fields: 'Add Policy To' (a dropdown menu with 'Only devices that have a matching process' selected), 'Process Policy Definition' section with 'Process Name' (a dropdown menu with 'ACLIENT.EXE' selected), 'Process Argument' (an empty text field), 'Memory Limit (kilobytes per instance)', 'Total Memory Limit (kilobytes)', and 'Total CPU Utilization Limit (%)' (all empty text fields), 'Minimum Instances' and 'Maximum Instances' (both dropdown menus with '0' selected), 'Process User' (an empty text field), and 'Alert if Found' (a dropdown menu with 'No' selected). At the bottom of the right pane are 'Save' and 'Save As' buttons.

15. In the **Subtemplate Selection** pane, select *Add New Process Sub-Template*.

16. Supply values in the following fields:

- **Add Policy To.** Select *All Devices* in this field.
- **Process Name.** Select *httpd* in this field. If *httpd* has not been discovered as a running process for any device discovered in the system, select the plus icon (+), then enter "httpd" in this field.
- **Alert if Found.** Select *No* in this field. The system will generate an event if the *httpd* process is not running on a monitored device.

**NOTE:** This example does not have specific requirements for the other settings defined in this page. You can leave the remaining fields set to the default values.

17. Enter a name for the template in the **Template Name** field. For example, "Gold-Level Apache/Net-SNMP".

18. To save the device template, select the **[Save]** button.

---

# Chapter

# 4



## Configuring User Policies

---

### Overview

In SL1, user policies allow you to define a set of user account properties and permissions to re-use for multiple user accounts. When you create a user account, you can use a user policy to quickly apply settings to the new user account. User policies have a dynamic relationship with their member user accounts. When you make a change to a user policy, the user accounts associated with that user policy are automatically updated. In this example, a single user policy is defined that grants customer-level access to the system. When a new customer is provisioned, the user policy is used to create a user account for the new customer.

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:

<i>Using the Default User Policies</i> .....	17
<i>Editing a User Policy</i> .....	18
<i>Editing an Access Key</i> .....	19



---

## Using the Default User Policies

SL1 includes a set of sample user policies that are created when the platform is installed. These sample user policies are intended as a starting point for you to create a set of user policies to meet your needs. If you edit the sample user policies, your changes will not be overwritten when you upgrade SL1.

The sample user policies use a sample set of **access keys**. An access key is a customized group of privileges that allow a user to perform actions in SL1. Each privilege (called an **access hook**) typically grants a single action, such as viewing a specific page or editing a specific entity. Access hooks are grouped in to access keys for easier management and alignment with users. SL1 includes 28 sample access keys by default. Similar to the default user policies, these access keys are intended as a starting point for you to create a set of access keys to meet your needs. If you edit the sample access keys, your changes will not be overwritten when you upgrade SL1.

This example uses the default "End User" user policy, which grants limited, view-only access to the user interface. This user policy was designed primarily to be used by customers of service providers. The "End User" user policy is assigned access keys that allow associated users to:

- Use the basic user tools, including the Inbox, Finder, and User Preferences.
- View, create, and add notes to tickets.
- View dashboards that other users have shared with them.
- View articles in the knowledge base
- View their organization record and user accounts associated with their organization.
- View performance data and events for their devices.
- View data about IT Services that other users have shared with them.

The following sections describe how you can customize the default "End User" user policy and the default access keys to meet your needs.

## Editing a User Policy

To edit a user policy, including removing or adding permissions, perform the following steps:

1. Go to the **User Policies** page (Registry > Accounts > User Policies). The page displays the default user policies and any additional user policies that have been configured in the platform:

User Policies   Policies Found [7]										Create	Reset	Guide
	Policy Name	User Type	Members	Login State	Organization	Theme	ID	Edited By	Last Edited			
1.	End User	User	--	Active	--	--	5	em7admin	2011-08-25 19:05:50			
2.	Executive	User	--	Active	--	--	3	em7admin	2011-09-13 10:57:42			
3.	Operations Manager	User	--	Active	--	--	8	em7admin	2011-08-25 19:09:05			
4.	Operator	User	--	Active	--	--	4	em7admin	2011-08-25 19:04:29			
5.	Provisioning & Device Configuration	User	--	Active	--	--	7	em7admin	2011-08-25 19:08:23			
6.	Report & Widget Developer	User	--	Active	--	--	6	em7admin	2011-08-25 19:06:45			
7.	Sciencelogic Administrator	User	--	Active	--	--	9	em7admin	2012-03-22 16:00:22			

[Select Action] [Go]

2. Select the wrench icon (🔧) for the user policy you want to edit. For this example, edit the "End User" user policy. The **User Policy Properties Editor** page is displayed:

The screenshot shows the 'User Policy Properties Editor' for the 'End User' policy group. The interface includes buttons for 'New', 'Reset', and 'Guide' at the top right. The main area is divided into three columns:

- Left Column:** Configuration fields for the user policy, including Policy Name, Login State, Account Type, Password Strength, Password Expiration, Password Shadowing, Require Password Reset, Authentication Method, Restrict to IP, Event Console Default Display, and Ticket Queue Memberships.
- Middle Column:** Primary Organization (System), Theme (Classic "EM7 Operations"), Time Zone ([ UTC]), and Additional Organization Memberships (Test, All organizations).
- Right Column:** Privilege Keys section with a list of access keys and checkboxes, including EM7 System Administration, Ticketing, Dashboards, Asset Management, Knowledge Base, Organizations, and Reports.

At the bottom, there are 'Save' and 'Save As' buttons, and a checkbox for 'Re-Apply All Settings To All Policy Members'.

Some fields have been disabled in the default user policies; disabled fields appear grayed out in the **User Policy Properties Editor** page. When you disable a field in a user policy, that field can be edited on a per-user account basis for all user accounts that are associated with the user policy. For example, if you are using a single user policy for multiple customers, you would leave the **Organization** field disabled; you would align each customer account with the corresponding customer organization when you create their user account. To enable or disable a field, select the field name.

3. To customize the user policy, you can edit the value in one or more fields in this page. For details on each field in the user policy editor, select the **[Guide]** button. A common customization is adding and removing access keys. The right pane in the **User Policy Properties Editor** page lists all the access keys in the platform; select the checkboxes for the access keys that you want to grant to your customers. You might want to remove some of the default access keys based on your use of SL1. For example, if you are not using the knowledge base feature, you might want to remove the "Knowledge Base - View" access key.
4. Select the **[Save]** button to save your changes.

## Editing an Access Key

To change the permissions that are granted by a specific access key, perform the following steps:

1. Go to the **Access Keys** page (System > Manage > Access Keys).
2. Select the wrench icon (🔧) for the access key that you want to edit. For example, select the "Devices - Information View" access key. This access key grants view-only access to performance data and events for devices. The **Key/Hook Alignment Editor** is displayed:

The screenshot shows the 'Key/Hook Alignment Editor' for the 'Devices - Information View' access key. The interface is divided into several sections:

- Access Keys:** A sidebar on the left with a tree view showing the system hierarchy, including 'EM7 System Administration', 'Ticketing', 'Dashboards', 'Asset Management', 'Knowledge Base', 'Organizations', 'Reports', 'Events', and 'Devices'. The 'Devices' section is expanded to show 'Devices - Information View'.
- Key Details:** A top section with a 'Name' field containing 'Devices - Information View' and a 'Key Category' dropdown set to 'Devices'. Below it is a 'Key Description' field containing the text: 'Grants view access to device configuration, performance data, and events.'
- Hook Alignment:** A central section with two lists:
  - Unaligned Access Hooks:** A list of available hooks including 'Asset Management' (AssetAdd, AssetEdit, AssetRemove, AssetView), 'Registry>Assets>Manager', 'Business Services' (Product Catalog: Add/Rem, Product Catalog: Edit, Product Catalog: View, Product Catalog: View From Org Page, Registry>Business Services>Bandwidth Billing, Registry>Business Services>Distribution Lists, Registry>Business Services>Product Catalog, Registry>Business Services>Service Catalog, Registry>Business Services>Service Notifier, Registry>Business Services>Service Usage, Service Catalog: View, View SKU (deprecated)), and 'Contacts' (Contact: View).
  - Aligned Access Hooks:** A list of hooks currently granted by the key, including 'Device Groups' (DevGroup: View) and 'Devices' (Dev: Config, Dev: Events Summary, Dev: IF Graphs, Dev: Performance Graphs, Dev: Software, Dev: TCP Ports, Dev: View, Dev: View Category, Dev: View Class, Dev: View Profile, Dev: View Services, Dev: View Summary, Registry>Devices>Device Manager, Registry>Devices>Vanished Device Manager, EM7 System Administration, Registry>).
- Navigation:** A 'Find' button is at the bottom left, and 'Save' and 'Save As' buttons are at the bottom right.

3. The **Aligned Access Hooks** field displays the access hooks that are granted by this access key. The **Unaligned Access Hooks** field displays all the other access hooks that are available in the platform:
  - To add an access hook to the access key, select the access hook in the **Unaligned Access Hooks** field, then select the right arrow button ([> >]).
  - To remove an access hook from the access key, select the access hook in the **Aligned Access Hooks** field, then select the left arrow button ([< <]).
  - For example, the "Devices - Information View" includes the *Dev:View Profile* access hook. This access hook allows a user to view the **[Profile]** tab in the **Device Reports** panel. If you do not want your customers to have access to this tab, select *Dev:View Profile* in the **Aligned Access Hooks** field, then select the left arrow button ([< <]).
4. Select the **[Save]** button to save your changes.

---

# Chapter

# 5

## Provisioning a New Customer



---

### Overview

This chapter describes how to provision a customer that has subscribed to a monitoring service. This example includes the following steps in the provisioning process:

- [Creating an Organization and aligning product SKUs](#).
- Creating and running a discovery session, either [for "pingable" devices](#) (Bronze-level monitoring) or [using a device template](#) (Silver-level and Gold-level monitoring).
- [Creating 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:

<a href="#">Creating an Organization and Aligning Product SKUs</a> .....	22
<a href="#">Creating a Discovery Session for Pingable Devices</a> .....	24
<a href="#">Creating a Discovery Session that includes a Device Template</a> .....	25
<a href="#">Creating a User Account</a> .....	26

## Creating an Organization and Aligning Product SKUs

The first step for provisioning a new customer is to create an organization record. All of the main entity types in a SL1 system are associated with an organization. In this example, the monitoring services that a customer has subscribed to are tracked by aligning the product SKUs for the services to the customer's organization record. The personnel responsible for discovering that customer's devices in the SL1 system can then view the customer's product subscriptions to determine which device template to include in the discovery session.

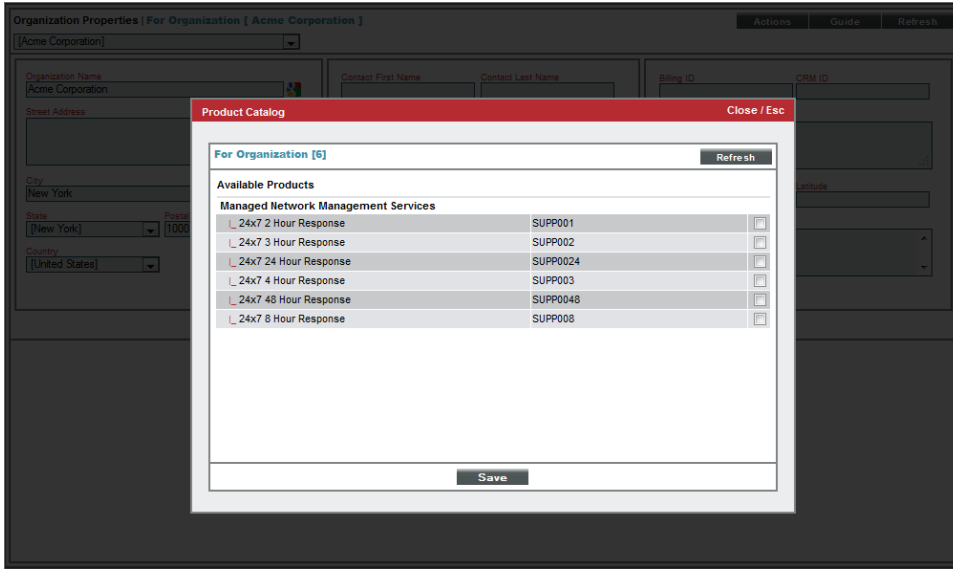
To create an organization and align product SKUs, perform the following steps:

1. Go to the **Organizational Account Administration** page (Registry > Accounts > Organizations).
2. Select the **[Create]** button. The **Add Organizational Record** page is displayed in a new window:

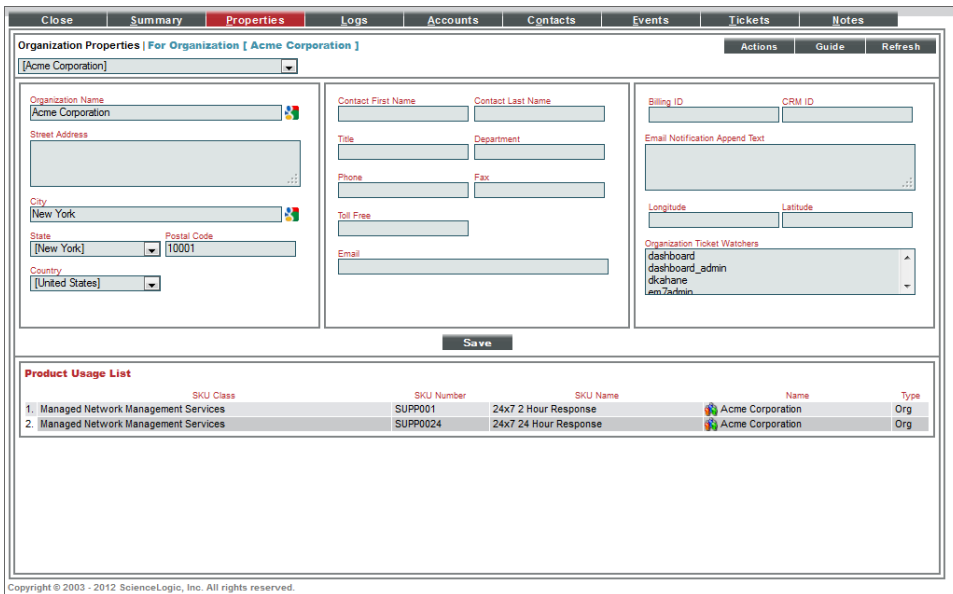
The screenshot shows a web form titled "Add Organizational Record" with a blue header bar containing "Guide" and "Refresh" buttons. The form is organized into three columns. The first column on the left includes a required field for "Organization Name", a "Street Address" text area, a "City" text field, a "State" dropdown menu (currently set to "[None]"), a "Postal Code" text field, and a "Country" dropdown menu (currently set to "[United States]"). The middle column contains "Contact First Name" and "Contact Last Name" text fields, "Title" and "Department" text fields, "Phone" and "Fax" text fields, a "Toll Free" text field, and an "Email" text field. The right column includes "Billing ID" and "CRM ID" text fields, an "Email Notification Append Text" text area, "Longitude" and "Latitude" text fields, and an "Organization Ticket Watchers" dropdown menu with "dashboard\_admin" and "em7admin" as visible options. A "Save" button is positioned at the bottom center of the form.

3. Based on your business requirements, supply values in the fields in this page. The required field is:
  - **Organization Name**. Enter the name of the customer.
4. Select the **[Save]** button.

- To align the SKUs for the monitoring services that customer has subscribed to the organization record, select the **[Actions]** button, and then select *Product Catalog*. The **Product Catalog** modal page is displayed:



- Select the checkbox for each SKU to which the customer has subscribed.
- Select the **[Save]** button.
- Close the **Product Catalog** modal page and then select the **[Refresh]** button in the **Organization Properties** page. The selected SKUs appear in the **Product Usage List** pane:



# Creating a Discovery Session for Pingable Devices

In this example, Bronze-level monitoring includes only availability and latency monitoring. To create a discovery session that uses only the ICMP protocol to discover devices, perform the following steps:

1. Go to the **Discovery Control Panel** page (System > Manage > Discovery).
2. Select the **[Create]** button. The **Discovery Session Editor** page is displayed in a new window:

The screenshot shows the 'Discovery Session Editor | Create New' interface. It is organized into four main columns:

- Identification Information:** Fields for 'Name' and 'Description'.
- IP and Credentials:** Includes 'IP Address/Hostname Discovery List' with an 'Upload File' button and a 'Browse...' button. Below are 'SNMP Credentials' and 'Other Credentials' dropdown menus.
- Detection and Scanning:** Features dropdowns for 'Initial Scan Level', 'Scan Throttle', 'Port Scan All IPs', and 'Port Scan Timeout'. A 'Detection Method & Port' dropdown menu is open, showing a list of protocols and ports (e.g., UDP: 161 SNMP, TCP: 1 - tcpmux, TCP: 2 - compressnet, etc.). Below are input fields for 'Interface Inventory Timeout (ms)' (600000), 'Maximum Allowed Interfaces' (10000), and a 'Bypass Interface Inventory' checkbox.
- Basic Settings:** Includes checkboxes for 'Discover Non-SNMP', 'Model Devices', and 'DHCP'. It also has a 'Device Model Cache TTL (h)' input field (2), a 'Collection Server PID' dropdown (ayoung-dist-cu-251), an 'Organization' dropdown ([ System]), and an 'Add Devices to Device Group(s)' dropdown (None Servers). At the bottom of this section is an 'Apply Device Template' dropdown (Choose a Template).

At the bottom of the page, there is a 'Save' button and a 'Log All' checkbox.

3. Supply values in the following fields:
  - **IP Address/Hostname Discovery List.** Enter the IP addresses or hostnames for the customer's devices.
  - **Initial Scan Level.** Select *0. Model Device Only* in this field. For a tiered service, you will want to limit what is monitored on each device. Choosing this option disables automatic alignment of Dynamic Applications during initial discovery.
  - **Discover Non-SNMP.** By default, the system will not create device records for devices that respond only to ICMP requests. Select this checkbox to enable discovery of "pingable" devices.
  - **Collection Server PID.** Select the Data Collector that will run the discovery session. All devices discovered using this discovery session will be monitored by the Collector Group that includes this Data Collector. If you are using an All-In-One Appliance, leave this field set to the default value.
  - **Organization.** Select the customer's organization. All devices discovered using this discovery session will be associated with this organization.



**NOTE:** This example does not have specific requirements for the other settings defined in this page. You can leave the remaining fields set to the default values or select values based on your business requirements.

4. Select the **[Save]** button.
5. Close the **Discovery Session Editor** page.
6. Select the **[Reset]** button in the **Discovery Control Panel** page. The new discovery session is displayed in the list of discovery sessions.
7. To run the discovery session, select its lightning bolt icon (⚡).

## Creating a Discovery Session that includes a Device Template

In this example, you must include a device template in the discovery session when you discover devices with silver-level or gold-level monitoring. As part of the provisioning process, personnel should check the SKUs associated with the organization record to determine which device template should be included in each discovery session. To create a discovery session that includes a device template, perform the following steps:

1. Go to the **Discovery Control Panel** page (System > Manage > Discovery).
2. Select the **[Create]** button. The **Discovery Session Editor** page is displayed in a new window:

Discovery Session Editor | Create New

New Reset

Identification Information

Name Description

IP and Credentials

IP Address/Hostname Discovery List

Upload File

Browse for file... Browse...

SNMP Credentials

Other Credentials

Basic/Snippet

Detection and Scanning

Initial Scan Level

System Default (recommended)

Scan Throttle

System Default (recommended)

Port Scan All IPs

System Default (recommended)

Port Scan Timeout

System Default (recommended)

Detection Method & Port

Discover Method

UDP: 161 SNMP

TCP: 1 - tcpmux

TCP: 2 - compressnet

TCP: 3 - compressnet

TCP: 5 - rje

TCP: 7 - echo

TCP: 9 - discard

TCP: 11 - systat

TCP: 13 - daytime

TCP: 15 - riostat

TCP: 17 - qotd

TCP: 18 - msp

TCP: 19 - chargen

TCP: 20 - ftp-data

Interface Inventory Timeout (ms)

600000

Maximum Allowed Interfaces

10000

Bypass Interface Inventory

Basic Settings

Discover Non-SNMP Model Devices DHCP

Device Model Cache TTL (h)

2

Collection Server PID

ayoung-dist-cu-251

Organization

[ System ]

Add Devices to Device Group(s)

None Servers


Apply Device Template

[ Choose a Template ]

Save Log All

3. Supply values in the following fields:
  - **IP Address Discovery List.** Enter the IP addresses or hostnames for the customer's devices.
  - **SNMP Credentials.** Select the SNMP credentials that the system should use to communicate with the customer's devices.
  - **Initial Scan Level.** Select *0. Model Device Only* in this field. For a tiered service, you will want to limit what is monitored on each device. Choosing this option disables automatic alignment of Dynamic Applications during initial discovery.
  - **Collection Server PID.** Select the Data Collector that will run the discovery session. All devices discovered using this discovery session will be monitored by the Collector Group that includes this Data Collector. If you are using an All-In-One Appliance, leave this field set to the default value.
  - **Organization.** Select the customer's organization. All devices discovered using this discovery session will be associated with this organization.
  - **Apply Device Template.** Select the device template to apply to all devices discovered using this discovery session.

**NOTE:** This example does not have specific requirements for the other settings defined in this page. You can leave the remaining fields set to the default values or select values based on your business requirements.

4. Select the **[Save]** button.
5. Close the **Discovery Session Editor** page.
6. Select the **[Reset]** button in the **Discovery Control Panel** page. The new discovery session is displayed in the list of discovery sessions.
7. To run the discovery session, select its lightning bolt icon ().

---

## Creating a User Account

To create a user account using the pre-defined "End User" user policy, perform the following steps:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. Select the **[Create]** button. The **Create New Account** page is displayed:
3. Supply values in the following fields:
  - **First Name.** Enter the first name of the customer.
  - **Last Name.** Enter the last name of the customer.
  - **Account Login Name.** Enter a username for the customer. This is the username that the customer will use to log in to the user interface.
  - **Primary Email.** Enter the Email address of the customer.

- **Password**. Enter an initial password for the user account. If you leave the **Require Password Reset** checkbox selected, the customer will log in with this password and will immediately be prompted to change their password.
- **Confirm Password**. Enter the initial password again.
- **Organization**. Select the organization that you created for this customer.
- **Account Type**. To align the account with a user policy, select *Policy Membership* in this field.
- **Account Templates**. Select the user policy for this account. For example, select *End User*.

**NOTE:** This example does not have specific requirements for the other settings defined in this page. You can leave the remaining fields set to the default values or select values based on your business requirements.

4. Select the **[Save]** button. Select **[OK]** in the pop-up window that appears.

© 2003 - 2020, ScienceLogic, Inc.

All rights reserved.

#### LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

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

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

#### Copyrights and Trademarks

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

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

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

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

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

#### Other

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

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



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

International: +1-703-354-1010