



Access Permissions

SL1 version 8.12.1

Table of Contents



Introduction to Access Permissions	3
What is an Access Hook?	4
What is an Access Key?	4
Other Restrictions on User Access	4
Creating and Managing Access Keys	5
The Access Hooks Page	6
Viewing the List of Access Hooks	6
The Access Keys Page	7
Viewing the List of Access Keys	7
Default Access Keys	8
Creating an Access Key	15
Editing an Access Key	16
Deleting Access Keys	17
Assigning Access Hooks	18
Access Hooks for Top-Level Navigation	19
Navigation Access Hooks	20
Action Access Hooks	21
Action Access Hook Dependencies	22
Blacklisting or Whitelisting Access Hooks	22
Enabling the Access Hook Blacklist or Whitelist	23
Example of the Access Hook Blacklist	23
Using Access Keys with User-generated Content	24
Using Access Keys with Dashboards	25
Using Access Keys with Device Groups	26
Generating a Report for an Access Key	28
Best Practices for Access Permissions	30
Best Practices	31
Example: An Access Key to View Assets	32
Requirements	33
Selecting Access Hooks	33
Checking Access Hook Dependencies	33
Creating the Access Key	34

Introduction to Access Permissions

Overview

This manual is intended for system administrators who are responsible for controlling user access to SL1 systems. This manual describes the access permissions system used in SL1. This system comprises a selection of Access Hooks that control individual actions and user-defined Access Keys, that group together Access Hooks and are granted to users. This manual includes step-by-step instructions on how to create Access Keys and how to select appropriate Access Hooks.

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 the menu options, click the Advanced menu icon (.

This chapter includes the following topics:

<i>What is an Access Hook?</i>	4
<i>What is an Access Key?</i>	4
<i>Other Restrictions on User Access</i>	4

What is an Access Hook?

An **Access Hook** controls access to a specific action that can be performed in the user interface for SL1. These actions include navigating to a page, viewing information about an entity in the system, and editing entities in the system. Each Access Hook is designed to be highly granular, providing access to only one action on one specific entity or page. Access Hooks are not granted to users directly; instead Access Hooks are grouped together to form an Access Key, which can be granted to a user.

What is an Access Key?

Because there are several hundred Access Hooks provided in SL1, granting each individual Access Hook to a user or user policy would be a time-consuming process. Therefore, SL1 requires that Access Hooks be grouped together in an **Access Key** that can be granted to users either directly or through a user policy. By default, the Access Key "Grant All" is included with SL1. Every Access Hook, except for the Access Hook that controls the Access Key Manager, is aligned to the "Grant All" Access Key. SL1 also includes default Access Keys for the most common user profiles and common tasks in SL1.

Other Restrictions on User Access

In addition to the Access Hook and Access Key system, user access to SL1 systems is also controlled by organization memberships and the user type hierarchy.

Access Hooks and Access Keys control the pages users can navigate to and the actions they can perform; however, user access is further controlled by organization membership. Users can view and interact only with entities associated with organizations they have membership to. For example, a system might have three organizations, Org A, Org B, and Org C. If user is a member of Org A and Org B and has access to the **Device Manager** page or **Devices** page, the user will see only devices in Org A and Org B in the **Device Manager** page or **Devices** page. The user will not be able to see or interact with entities associated with Org C.

If a user is able to view the **Access Hooks** and **Access Keys** pages, the user interface is restricted so no navigation links are given to those pages. See the [Navigation Access Hooks](#) section for more information.

If a user is able to modify user accounts, user hierarchy is also enforced in the following ways:



- Users of type "user" cannot modify administrator accounts.
- Users of type "user" cannot make themselves or another user an administrator.
- Users cannot grant or remove Access Keys that they have not been granted.

Creating and Managing Access Keys

Overview

This chapter describes the layout and functionality of the **Access Keys** and **Access Hooks** pages, and includes step-by-step instructions on how to create an Access Key.

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 the menu options, click the Advanced menu icon (.

This chapter includes the following topics:

<i>The Access Hooks Page</i>	6
<i>Viewing the List of Access Hooks</i>	6
<i>The Access Keys Page</i>	7
<i>Viewing the List of Access Keys</i>	7
<i>Default Access Keys</i>	8
<i>Creating an Access Key</i>	15
<i>Editing an Access Key</i>	16
<i>Deleting Access Keys</i>	17

The Access Hooks Page

To navigate to the **Access Hooks** page, go to System > Manage > Access Hooks:

Category	ID	Name	# Aligned Keys	Description
--	TICKET_REPORTS	TICKET_REPORTS	1	TICKET_REPORTS
Application management: APP_TOPO_ELEM_TYPE_REMOVE	ApplicationComponent>Edit	ApplicationComponent>Edit	1	Edit an application component
Application management: APP_TOPO_ELEM_TYPE_REMOVE	TopologyElement>Type Rem	TopologyElement>Type Rem	1	Remove a topology element type
Application management: APP_PGRP_ADD	ProcessGroup>Add	ProcessGroup>Add	1	Add a process group
Application management: APP_PGRP_TEMPLATE_ADD	ProcessGroupTemplate>Add	ProcessGroupTemplate>Add	1	Add a process group template
Application management: APP_PGRP_TEMPLATE_VIEW	ProcessGroupTemplate>View	ProcessGroupTemplate>View	1	Read access for process group templates
Application management: APP_TOPO_ELEM>Edit	TopologyElement>Edit	TopologyElement>Edit	1	Edit an topology element
Application management: APP_TOPO_ELEM_ADD	ApplicationComponent>Add	ApplicationComponent>Add	1	Add an application component
Application management: APP_TOPO_ELEM_TYPE>Edit	TopologyElement>Type>Edit	TopologyElement>Type>Edit	1	Edit an topology element type
Application management: APP_TOPO_ELEM_VIEW	ApplicationComponent>View	ApplicationComponent>View	1	Read access for application components
Application management: APP_TOPO_ELEM_VIEW	TopologyElement>View	TopologyElement>View	1	Read access for topology elements
Application management: APP_PGRP_REMOVE	ProcessGroup>Rem	ProcessGroup>Rem	1	Remove a process group
Application management: APP_PGRP_TEMPLATE_REMOVE	ProcessGroupTemplate>Rem	ProcessGroupTemplate>Rem	1	Remove a process group template
Application management: APP_TOPO_ELEM_ADD	TopologyElement>Add	TopologyElement>Add	1	Add a topology element
Application management: APP_TOPO_ELEM_TYPE_ADD	TopologyElement>Type>Add	TopologyElement>Type>Add	1	Add a topology element type
Application management: APP_TOPO_ELEM_REMOVE	ApplicationComponent>Rem	ApplicationComponent>Rem	1	Remove an application component
Application management: APP_TOPO_ELEM_TYPE_VIEW	TopologyElement>Type>View	TopologyElement>Type>View	1	Read access for topology element types
Application management: APP_PGRP>Edit	ProcessGroup>Edit	ProcessGroup>Edit	1	Edit an process group
Application management: APP_PGRP_TEMPLATE>Edit	ProcessGroupTemplate>Edit	ProcessGroupTemplate>Edit	1	Edit an process group template
Application management: APP_PGRP_VIEW	ProcessGroup>View	ProcessGroup>View	1	Read access for process groups
Application management: APP_TOPO_ELEM_REMOVE	TopologyElement>Rem	TopologyElement>Rem	1	Remove a topology element
Asset Management: AST>Edit	Asset>Edit	Asset>Edit	2	Write access to asset records, no including add/remove
Asset Management: AST>View	Asset>View	Asset>View	3	Read access to asset records
Asset Management: AST>Add	Asset>Add	Asset>Add	2	Add an asset record
Asset Management: AST>Rem	Asset>Remove	Asset>Remove	2	Remove an asset record
Asset Management: AST>REG_PAGE	Registry-Assets-Manager	Registry-Assets-Manager	3	View the Asset Manager registry page
Business Services: BIZ_PRODUCT_CATALOG_ORG_VIEW	Product Catalog>View From Org Page	Product Catalog>View From Org Page	1	View a product catalog data from the Org properties page

Viewing the List of Access Hooks

The **Access Hooks** page displays a list of all Access Hooks in SL1. For each Access Hook, the page displays the following:

TIP: To sort the list of access hooks, 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.

- **Category.** Functional category assigned to the Access Key.
- **ID.** Alphanumeric ID that describes the access hook. These IDs have a uniform format. The first part of the ID (up to the first underscore character) describes the functional area in SL1. For example "AST_" stands for Asset Management and "DASH" stands for dashboards. The remaining parts of the ID further describe the location in SL1 and the actions allowed with the Access Hook. For example "CRED_SNMP_ADDREM" means that the Access Hook affects credentials, specifically SNMP credentials, and allows the user to add and remove SNMP credentials.
- **Name.** Name of the Access Hook.

- **# Aligned Keys.** Number of Access Keys that the Access Hook is aligned to. Clicking on the padlock icon (🔒) displays the **Access Key Alignment** modal page, which displays the list of aligned Access Keys for this hook.
- **Description.** Description of the Access Hook.

NOTE: By default, the cursor is placed in the first Filter-While-You-Type field. You can use the <Tab> key or your mouse to move your cursor through the fields.

The Access Keys Page

To navigate to the **Access Keys** page, go to System > Manage > Access Keys:

Name	Category	# Aligned Users	# Aligned Policies	Description
1. Admin Portal UI Access	SYSTEM	1	6	Grants access to the EM7 web interface.
2. Asset - Administration	ASSET	1	2	Grants create, edit, and remove permissions for asset records.
3. Asset - View	ASSET	1	2	Grants view access to asset records.
4. Basic User Privileges	SYSTEM	1	6	Grants access to the finder, inbox, and preferences tab.
5. Dashboard - Administration	DASH	1	2	Grants create, edit, and remove permissions for dashboards.
6. Dashboard - View	DASH	1	2	Grants view access to shared dashboards.
7. Dashboard - Widget Developer	DASH	1	1	Grants create and edit permissions for dashboards and permission to create and edit widget definitions.
8. Devices - Administration	DEVICES	--	1	Grants view, edit, and delete permissions for devices, device groups, device templates, monitoring policies, and interfaces.
9. Devices - Information View	DEVICES	--	2	Grants view access to device configuration, performance data, and events.
10. Devices - Operator Access	DEVICES	--	2	Grants view access to all information associated with a device and allows a user to run device toolbox commands.
11. Events - Advanced	EVENTS	--	2	Grants view, acknowledge, and clear access to events.
12. Events - View	EVENTS	--	1	Grants view and acknowledge access to events
13. Grant All	SYSTEM	1	1	Grant all access rights that are allowable for Users (non-Administrators)
14. Interfaces - View	DEVICES	--	--	Grants view access to interfaces.
15. IT Services - Administration	ITS	--	1	Grants add, edit, and remove permissions for IT Services and IT Service Dashboards.
16. IT Services - View	ITS	--	2	Grants view access to IT Services.
17. Knowledge Base - Administration	KB	--	2	Grants add, edit, remove permissions for knowledge base articles.
18. Knowledge Base - View	KB	--	2	Grants view access to the knowledge base.
19. Monitors - View	DEVICES	--	--	Grants view access to monitors.
20. Org / User / Vendor / Contact - Administration	ORG	1	1	Grants add, edit, and remove permissions for organizations, user accounts, external contacts, and vendors.
21. Org / User / Vendor / Contact - Operator	ORG	--	1	Grants view access to organizations, user accounts, external contacts, and vendors, and the ability to add and edit organization and vendor notes.
22. Org / User / Vendor / Contact - View	ORG	1	2	Grants view access to organizations, user accounts, external contacts, and vendors.
23. PowerPack Administration	SYSTEM	--	1	Grants create, edit, and import permissions for PowerPacks.
24. Provisioning Access	SYSTEM	--	1	Grants add, edit, and remove permissions for credentials and allows a user to run discovery sessions.
25. Reporting - Administration	REPORTS	--	2	Grants permissions to run and schedule reports as any user and view archived reports.
26. Reporting - Developer	REPORTS	--	1	Grants edit permissions for report definitions.

Viewing the List of Access Keys

The **Access Keys** page displays a list of all Access Keys that have been created. For each Access Key, the page displays the following:

TIP: To sort the list of Access Keys, 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.

- **Name.** Name of the access key.
- **Category.** Functional category assigned to the key.
- **# Aligned Users.** Number of user accounts that have been granted this key.
- **# Aligned Policies.** Number of user policies that have been granted this key.
- **Description.** Description of the access key.

NOTE: By default, the cursor is placed in the first Filter-While-You-Type field. You can use the <Tab> key or your mouse to move your cursor through the fields.

Default Access Keys

SL1 includes default Access Keys to use with the most common user profiles and the most common tasks in SL1. These default Access Keys are intended as a starting point for administrators to develop a set of access keys that meet their needs. You can [edit the default Access Keys](#); the default Access Keys **excluding Grant All** are not modified when a system is updated with the latest software. The Grant All key is always updated to include all Access Hooks excluding "Key Manager"

You can use the default Access Keys and **user policies** to assign groups of users the appropriate Access Keys. For details on user policies, see the manual **Organizations and Users**.

You are not required to use the default access keys.

Access Key	Description	Aligned Access Hooks	Useful For
Asset - View	Allows users to view asset records.	Asset:View Registry>Assets>Manager Registry>	Customers Help Desk Other staff who require view-only access to Asset Records
Asset - Administration	Allows users to create, edit, and delete asset records.	Asset:Add Asset:Edit Asset:Remove Asset:View Registry>Assets>Manager Custom Select Objects:Asset Add/Edit/Delete Registry>	Network Engineers System Administrators NOC Staff Provisioning Staff Support Engineers Implementation Engineers QA Analysts
Dashboard - Administration	Allows users to create, edit, and delete dashboards.	Dash:Add/Rem Dash:Add/Rem Shared Dash:Edit Dash:Edit Shared Dash:Share Dash:View Dash:View Shared Dash:Widget:Add/Rem Dash:Widget:Edit	Network Engineers System Administrators NOC Staff Provisioning Staff Support Engineers Implementation

Access Key	Description	Aligned Access Hooks	Useful For
			Engineers QA Analysts
Dashboard - View	Grants view access to shared dashboards	Dash:View Dash:View Shared	Customers Help Desk Other staff who require view-only access to Dashboards
Dashboard - Widget Developer	Grants create and edit permissions for dashboards and permission to create and edit widget definitions	Dash:Add/Rem Dash:Edit Dash:Share Dash:View Dash:View Shared Dash:Widget:Add/Rem Dash:Widget:Edit System>Customize>Dashboard Widgets	Content Developers
Devices - Information View	Grants view access to device configuration, performance data, and device events.	Dev:Events Summary Dev:IF Graphs Dev:Performance Graphs Dev:View Profile Dev:View Summary Registry>Devices>Device Manager Registry>	Customers Help Desk Other staff who require view-only access to Devices
Devices - Operator Access	Grants view access to all information associated with a device and allows a user to run device toolbox commands	Dev:Collections Dev:Events Summary Dev:IF Graphs Dev:Interfaces Dev:Logs Dev:Monitors Dev:Notes Dev:Performance Graphs Dev:Process View Dev:Remove Dev:Schedule Dev:Thresholds Dev:Tickets Dev:Tools Dev:Tools:ARIN Whois Dev:Tools:ARP Lookup Dev:Tools:ARP Ping Dev:Tools:Deep Port Scan Dev:Tools:FTP Dev:Tools:Forward DIG Dev:Tools:Ping Tool Dev:Tools:Port Scan Dev:Tools:Reverse DIG Dev:Tools:SNMP Dump Dev:Tools:SNMP Walker Dev:Tools:SSH Dev:Tools:Secure Web Dev:Tools:Telnet Dev:Tools:Terminal Dev:Tools:Traceroute Dev:Tools:Web Dev:Tools:Web Policy Dev:Topology Dev:View Dev:View Details	Network Engineers NOC Staff

Access Key	Description	Aligned Access Hooks	Useful For
		Dev:View Profile Dev:View Services Dev:View Summary Registry>Devices>Device Components Registry>Devices>Device Manager Registry>Devices>Hardware Registry>Devices>Processes Registry>Devices>Services Registry>Devices>Software Registry>Devices>Device Relationships	
Devices - Administration	Grants view, edit, and delete permissions for devices, device groups, device templates, monitoring policies, and interfaces	DevGroup:Add/Rem DevGroup:Edit DevGroup:View Registry>Devices>Groups Dev:Collections Dev:Edit Dev:Edit Class Dev:Events Summary Dev:IF Graphs Dev:Interfaces Dev:Logs Dev:Monitors Dev:Notes Dev:Performance Graphs Dev:Process View	Provisioning Staff Support Engineers Implementation Engineers QA Analysts
Devices - Administration (continued)		Dev:Redirects Dev:Remove Dev:Schedule Dev:Template:Add/Remove Dev:Template:Edit Dev:Template:View Dev:Thresholds Dev:Thresholds:Dynamic App Dev:Thresholds:Retention Dev:Tickets Dev:Tools Dev:Tools:ARIN Whois Dev:Tools:ARP Lookup Dev:Tools:ARP Ping Dev:Tools:Deep Port Scan Dev:Tools:FTP Dev:Tools:Forward DIG Dev:Tools:Ping Tool Dev:Tools:Port Scan Dev:Tools:Reverse DIG Dev:Tools:SNMP Dump Dev:Tools:SNMP Walker Dev:Tools:SSH Dev:Tools:Secure Web Dev:Tools:Telnet Dev:Tools:Terminal Dev:Tools:Traceroute Dev:Tools:Web Dev:Tools:Web Policy Dev:Topology Dev:View Dev:View Details Dev:View Profile Dev:View Services Dev:View Summary Registry>Devices>Device Components Registry>Devices>Device Manager	

Access Key	Description	Aligned Access Hooks	Useful For
		Registry>Devices>Hardware Processes Registry>Devices> Registry>Devices>Services Registry>Devices>Software Registry>Devices>Templates Registry>Devices>Device Relationships Registry> Networks:Interfaces:Edit Networks:Interfaces:View Registry>Networks>Interfaces Monitor:Add/Rem Monitors:Edit Registry>Monitors>Domain Name Registry>Monitors>Email Round-Trip Registry>Monitors>SOAP-XML Registry>Monitors>SSL Certificates Registry>Monitors>System Processes Registry>Monitors>TCP-IP Ports Registry>Monitors>Web Content Registry>Monitors>Windows Services	
Grant All	Grant all access rights that are allowable for Users (non-Administrators), excluding the ability to edit Access Keys	All Key Hooks except Key Manager	ScienceLogic Administrators
Basic User Privileges	Grants access to the finder inbox and preferences tab	Finder Inbox Preferences> Preferences>Account>Information Preferences>Account>Preferences Preferences>Account>Schedule	All users
PowerPack Administration	Grants create edit and import permissions for PowerPacks	PowerPack:Create PowerPack:Delete PowerPack:Edit PowerPack:Import System> System>Manage>PowerPacks	Content Developers Provisioning Staff Implementation Engineers
Provisioning Access	Grants add, edit, and remove permissions for credentials and allows a user to run discovery sessions	Cred:Basic:Add/Rem Cred:Basic:Edit Cred:DB:Add/Rem Cred:DB:Edit Cred:SNMP:Add/Rem Cred:SNMP:Edit Cred:SOAP:Add/Rem Cred:SOAP:Edit System>Manage>Credentials Discovery:Run System> System>Manage>Discovery	Provisioning Staff Support Engineers Implementation Engineers QA Analysts
Admin Portal UI Access	Grants access to the ScienceLogic web interface	Admin Portal Access	All users
Events - View	Grants view and acknowledge access to events	Event:Acknowledge Event:Kiosk Event:View (From Dev Properties) Event:View (From Org Page Events/Event:View	Customers Help Desk Other staff who require view-only access to Events

Access Key	Description	Aligned Access Hooks	Useful For
Events - Advanced	Grants view acknowledge and clear access to events	Event:Acknowledge Event:Clear Event:Kiosk Event:Reacknowledge Event:View (From Org Page Events/Event:View	Network Engineers NOC Staff
IT Services - View	Grants view access to IT Services	Registry> IT Service:View Registry>IT Services>IT Service Manager	Customers Network Engineers System Administrators NOC Staff
IT Services - Administration	Grants add edit and remove permissions for IT Services and IT Service Dashboards	Registry> IT Service Dashboard:Add/Rem IT Service Dashboard:Edit IT Service:Add/Rem IT Service:Edit IT Service:View Registry>IT Services>IT Service Dashboards Registry>IT Services>IT Service Manager	Provisioning Staff Support Engineers Implementation Engineers QA Analysts
Org / User / Vendor - View	Grants view access to organizations, user accounts, external contacts, and vendors	Org:Logs:view Org:Note:View Org:Print Report Org:View Org:View summary Registry>Accounts>Organizations Registry>Accounts>User Accounts Registry>Accounts>Vendors User:Print Report User:View Vendor:Notes Vendor View	Customers Help Desk Other staff who require view-only access to Organizations, Users, and Vendors
Org / User / Vendor - Administration	Grants add, edit, and remove permissions for organizations, user accounts, external contacts, and vendors	Custom Select Objects:Organization Add/Edit/Delete Custom Select Objects:User Account Add/Edit/Delete Org:AddRem Org:AltLocations:Edit Org:Edit Org:Logs:Clear Org:Logs:View Org:Notes:Add/Rem Org:Notes:Edit Org:Notes:View Org:Print Report Org:View Org:View Summary Registry>Accounts>Organization External Contact:Add/Rem External Contact:Edit External Contact:View External Contact:View (From Org Page) Registry>Accounts>External Contacts Registry>Accounts>User Accounts Registry>Accounts>Vendors User:Add/Rem User:Edit User:Edit (From Org Page) User:Print Report	Provisioning Staff Support Engineers Implementation Engineers QA Analysts

Access Key	Description	Aligned Access Hooks	Useful For
		User:View Vendor:Add/Rem Vendor:Edit Vendor:Edit Notes Vendor:Notes Vendor:View	
Org / User / Vendor - Operator	Grants view access to organizations, user accounts, external contacts, and vendors and the ability to add and edit organization and vendor notes	Org:Logs:View Org:Notes:Add/Rem Org:Notes:Edit Org:Notes:View Org:Print Report Org:View Org:View Summary Registry>Accounts>Organization Registry>Accounts>User Accounts Registry>Accounts>Vendors User:Print Report User:View Vendor:Edit Notes Vendor:Notes Vendor:View	ScienceLogic Administrators Network Engineers System Administrators NOC Staff
Reporting - Run Quick Reports	Grants permissions to run quick reports	Reports> Reports>Create Report>Quick Report	Customers Help Desk Other staff who require view-only access to Quick Reports
Reporting - Administration	Grants permissions to run and schedule reports as any user and view archived reports	Reports:Jobs:Add/Rem Reports:Jobs:Edit Reports:Jobs:Run As Any User Reports:Jobs:Run As Org User Reports:Schedule Reports> Reports>Create Report>Archived Reports Reports>Create Report>Quick Report Reports>Create Report>Report Jobs	Network Engineers NOC Staff Provisioning Staff Support Engineers Implementation Engineers QA Analysts
Reporting - Developer	Grants edit permissions for report definitions	Reports> Reports>Management>Input Forms Reports>Management>Report Manager Reports>Management>Report Output Media Reports>Management>Report Output Styles Reports>Management>Report Output Templates	Content Developers Report Developers
Ticketing - End User	Grants basic view and create permissions for tickets and allows a user to add notes to a ticket	Ticket:All in Orgs Ticket:Assign within Queue Ticket:Create Ticket:Edit Ticket:History (per Org) Ticket:History:View Ticket:Messaging Ticket:Notes:Add Ticket:Reports Ticket:Statistics:View Ticketing/Ticket:View	Customers Help Desk Other staff who need to create tickets and view tickets only

Access Key	Description	Aligned Access Hooks	Useful For
Ticketing - Operator	Grants create view and edit permissions for ticketing	Ticket:Alignment Ticket:All in Orgs Ticket:Assign Ticket:Change Severity Ticket:Clipboard Ticket:Create Ticket:Edit Ticket:History (per Org) Ticket:History: View Ticket:Inbox:Statistics Ticket:Messaging Ticket:Notes:Add Ticket:Notes:Cloaked Ticket:Notes:Cloaked:Edit Ticket:Notes:Edit Ticket:Reports Ticket:Statistics:View Ticket:View Logs Ticket:View Watchers Ticket:Watchers:Add/Rem Ticketing/Ticket:View	Network Engineers NOC Staff Provisioning Staff Support Engineers Implementation Engineers QA Analysts
Ticketing - Administration	Grants create view and edit permissions for ticketing and allows a user to configure the ticketing system	Registry> Registry> Ticketing> Custom States Registry> Ticketing> Email Tickets Registry> Ticketing> Escalations Registry> Ticketing> Queues Registry> Ticketing> Templates Ticket:Access All Ticket:Access All Queues Ticket:Alignment Ticket:All queue Members Ticket:All in Orgs Ticket:All in queues Ticket:Assign Ticket:Assign within Queue Ticket:Change Severity Ticket:Charge Back Services Ticket:Clipboard Ticket:Create Ticket:Customize Forms Ticket>Delete Ticket:Edit Ticket:Escalation:Add/Rem Ticket:Escalation:Edit Ticket:Events:Alignment Ticket:History (per Org) Ticket:History:View Ticket:Inbox:Statistics Ticket:Messaging Ticket:Notes:Add Ticket:Notes:Cloaked Ticket:Notes:Cloaked Edit Ticket:Notes:Edit Ticket:Notes:Remove Ticket:Queue:Edit Ticket:Queue:View Ticket:Reports Ticket:Scheduler Ticket:Statistics:View Ticket:Templates:Edit/Add/Rem Ticket:View Any Ticket:View Logs Ticket:View Watchers	Provisioning Staff Support Engineers Implementation Engineers QA Analysts

Access Key	Description	Aligned Access Hooks	Useful For
		Ticket:Watchers:Add/Rem Ticketing/Ticket:View Ticketing:States:Add/Rem Ticketing:States>Edit	

Creating an Access Key

You can create Access Keys on the **Key/Hook Alignment Editor** page.

To create an Access Key:

1. To navigate to the **Access Hooks** page, go to System > Manage > Access Keys.
2. Click the **[Key Manager]** button. The **Key/Hook Alignment Editor** page appears:

3. Supply a value in each of the following fields in the **Key/Hook Alignment Editor** page:
 - **Name.** Enter a name in the **Name** field. This name will be used anywhere a list of Access Keys is displayed.
 - **Key Category.** Select a category from the **Key Category** drop down list. Categories are included to help you organize your access keys. Lists of Access Keys are always displayed grouped by category. In addition, Access Keys must be in certain Categories if they will be used to control access to Dashboards, Knowledge Base Articles or Device Groups. For more information, see the [Using Access Keys with User Generated Content](#) section.

CAUTION: Caution: Due to security vulnerabilities, ScienceLogic recommends that customers who installed SL1 prior to 8.9.2 disable the Knowledge Base. For details, see the release notes for version 8.9.2 of SL1.


- **Key Description.** Enter a description in the **Key Description** field. The description is displayed on the **Access Keys** page, and is included to help you organize your Access Keys. The description is also displayed when the mouse is hovered over the Access Key on the **Account Permissions** and **User Policy Properties Editor** pages. The description is optional.
4. Select Access Hooks to align with the Access Key using the list of **Unaligned Access Hooks** and **Aligned Access Hooks** and arrow buttons ([>>], [<<]). Initially, all Access Hooks will be in the list of **Unaligned Access Hooks**.
 5. To assign an Access Hook to the current Access Key:
 - Highlight one or more Access Hooks in the **Unaligned** list.
 - Highlight one or more Access Hooks in the **Unaligned** list.
 6. To move Access Hooks from the current Access Key:
 - Highlight one or more Access Hooks in the **Aligned** select list.
 - Click the arrow button that points left ([<<]).

You can select multiple Access Hooks at once:

- To select a range of Access Hooks, click on the first Access Hook, then click on the last Access Hook while holding down the **<Shift>** key on your keyboard. The Access Hooks you clicked on and all the Access Hooks between them in the list will be selected.
 - To select several Access Hooks, hold down the **CTRL** key on your keyboard while clicking on them. Mac users should hold down the Command key instead of the **CTRL** key.
 - To select every Access Hook in a category, click on the red category name.
7. Select the **[Save]** button. The message "Save Completed" will be displayed at the top of the screen.
 8. If you select the **[Save]** button again, any changes made will be applied to the same Access Key. Select the **[New]** button if you want to create another Access Key.

Editing an Access Key

To edit an Access Key:

1. Navigate to the **Access Keys** page (System > Manage > Access Keys).
2. Find the Access Key you want to edit. Click the Key Editor icon () for that Access Key. Alternately, if you are already in the **Key/Hook Alignment Editor** page, you can select an Access Key to edit from the list of Access Keys displayed on the left side of the page.
3. When you select an Access Key to edit, all the fields in the **Key/Hook Alignment Editor** page are populated with the current data for the Access Key. You can make changes to the values in one or more fields.
4. After making changes, click the **[Save]** button to save your changes.

5. To save your changes as a new Access Key, enter a new value in the **Name** field and select the **[Save As]** button.
6. Clicking the **[Reset]** button will reload the fields with the last saved data for the Access Key, without saving any changes from this editing session.

Deleting Access Keys

"Delete Key" is the only option in the **Select Action** drop down list on the **Access Keys** page. Perform the following steps to delete Access Keys:

1. On the **Access Keys** page, click the checkbox for each Access Key to be deleted.
2. In the **Select Action** drop down list, select *Delete Key*.
3. Click the **[Go]** button.

NOTE: You cannot delete an Access Key that is currently granted to a user account or user policy. Checkboxes will not be displayed for Access Keys that cannot be deleted.

Chapter

3



Assigning Access Hooks

Overview

This chapter will help you select the Access Hooks that best fit the needs of your business. Because Access Hooks are as granular as possible, some Access Hooks have dependencies on other Access Hooks. For example, the **Asset:View** Access Hook grants the user access to view a specific asset. However, the user's granted Access Keys user must also include the **Registry>Assets>Manager** Access Hook to access the **Asset Manager** page, and the **Registry>** Access Hook to access the **[Registry]** tab.

This chapter describes the levels of access control, from providing access to the top-level navigation tabs to performing actions on specific pages.

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 the menu options, click the Advanced menu icon ().

This chapter includes the following topics:

<i>Access Hooks for Top-Level Navigation</i>	19
<i>Navigation Access Hooks</i>	20
<i>Action Access Hooks</i>	21
<i>Action Access Hook Dependencies</i>	22
<i>Blacklisting or Whitelisting Access Hooks</i>	22
<i>Enabling the Access Hook Blacklist or Whitelist</i>	23
<i>Example of the Access Hook Blacklist</i>	23

Access Hooks for Top-Level Navigation

To make it easier to determine and select the appropriate Access Hooks, each Access Hook is categorized by functional area of the product. For example, the Asset Hook **Asset:View** is in the **Asset Management** category

Access Hooks use a consistent naming convention to indicate their function, including an entity and action, for example "Asset:View". The **Access Hooks** page includes a description of each Access Hook.

If you want to allow users to view each top-level tab in SL1, you must create Access Keys that include the Access Hooks described in this section. If users do not have any Access Hooks that allow the user to view one or more top-level tabs, aligned with their granted Access Keys, those users will not see any navigation tabs when they log in to SL1:



If you want to align an Access Hook for an action with an Access Key and that Access Hooks requires a user to use the top-level navigation tabs to perform an action, such as allowing them access to a page under a tab, you must also align the corresponding Access Hook described in this section.

TIP: In certain situations, you might not want to grant users access to the top-level navigation tabs. If users have access to a page under a tab, but not the corresponding tab, they can still access the page using a direct link. If you want to restrict user access to the standard top-level navigation tabs, but still want to allow users to access pages under the tab, you may want to consider custom navigation tabs or another method of providing users with links to those pages. For information on custom navigation tabs, see the manual **Customizing User Experience**.

The following table describes the Access Hooks that allow a user to view top-level navigation tabs. Some of these Access Hooks also grant users other permissions; these permissions are described in the "Additional Access" column.

Tab	Access Hook Category	Access Hook Name	Additional Access
Dashboards	Dashboards	Dash:View	Allows user to view their own dashboards. Does not allow user to create or edit their own dashboards.
Views	Views	Views: View	Allows the user to view the Views tab and to view the Views that are embedded in Dashboards. NOTE: To allow users to view the Views embedded in Dashboards but not allow the user to view the Views tab, assign the Access Hook Views:View Embedded .
Events	Events	Events/Event:View	Allows user to view the list of events for their organizations on the Event Console screen.
Tickets	Ticketing	Ticketing/Ticket:View	Allows user to view the list of tickets in their assigned ticket queues for their organizations on the Ticket Console page.
Reports	Reports	Reports>	None
Registry	EM7 System Administration	Registry>	None
System	EM7 System Administration	System>	None
Preferences	User Account Management	Preferences>	None

NOTE: For tabs that have a left Navbar or menu bar, such as **[Registry]** and **[System]**, the top-level navigation hook will allow the user to select only the tab. On these tabs, links in the left Navbar or menu bar will appear only if the a user has additional Access Hooks specifically for the links in the left Navbar or menu bar.

Navigation Access Hooks

Access Hooks that allow users to navigate to pages within the user interface follow a similar naming convention. The Access Hook name represents the sequence of mouse clicks required to navigate to the page. For example:

Registry>Accounts>User Accounts

In this example, the Access Hook grants access to the **User Accounts** page. To navigate to this page a user would click on the **[Registry]** tab, then the "Accounts" and "User Accounts" links in the left Navbar or menu bar.

When you assign an Access Key containing a navigation Access Hook, the user is allowed to navigate to and view the page only. To perform action in the page, such as adding, removing, viewing, and editing entities, the user must be assigned additional Access Hooks.

The "System>Manage>Access Hooks" and "System>Manage>Access Keys" Access Hooks behave differently from other navigation Access Hooks. The left Navbar or menu bar links to the **Access Hooks** and **Access Keys** pages are displayed only to accounts of type Administrator. Even if you assign "System>Manage>Access Hooks" and "System>Manage>Access Keys" to a user, the user will not see the **Access Hooks** and **Access Keys** links. However, the user will be able to navigate to the **Access Hooks** and **Access Keys** pages by going directly to the URL of those pages.

NOTE: All Access Hooks that control navigation to specific pages are dependent on Access Hooks described in the [Access Hooks for top-level navigation](#) section. If you want to allow a user to navigate to a page that is controlled by a navigation key, you **must** grant that user the top-level navigation Access Hook and the navigation Access Hook.

Action Access Hooks

Access Hooks that allow users to perform an action on or view specific information about an element use a consistent naming convention. The Access Hook name includes the following information separated by colons:

- The general entity type or area of SL1, e.g. "Ticket" or "Org".
- If applicable, the specific part of the entity or area of SL1, e.g. "Watchers" for ticketing, or "Notes" for organization.
- If there are multiple actions that can be performed, the specific action that can be taken, e.g. "Add/Rem" or "Edit". If the action information is not included in an Access Hook name, the Access Hook allows a user to take any available action on the entity or area of the product.

The following are examples of action Access Hooks:

- **Cred:SNMP:Add/Rem.** "Cred" indicates that the general entity type is a credential, "SNMP" indicates the Access Hook applies only to SNMP credentials, and "Add/Rem" indicates the Access Hook allows a user to add or remove an SNMP credential.
- **Dev:Tools.** "Dev" indicates that the general entity type is a device and "Tools" indicates the Access Hook applies only to the Device Toolbox. Because there is no action included in the Access Hook name, when you grant a user this Access Hook, the user will be able to perform every action available on the **Device Toolbox** page.
- **Discovery:Run.** "Discovery" indicates that the Access Hook applies to the Discovery Manager section, and "Run" indicates the Access Hook allows a user to schedule or execute a discovery session.

NOTE: In general, separate Access Hooks are provided for adding/removing entities and editing entities.

Action Access Hook Dependencies

The following dependencies apply to Access Hooks that allow users to perform actions:

- If a user has an Access Hook that allows them to perform an action, you must also grant them access to the page on which the action is performed. For example, a user who has the "Org:Edit" Access Hook should also have the "Registry>Accounts>Organizations" Access Hook to navigate to and edit an organization. If you are not restricting user access to top-level navigation tabs, you must also grant the user the "Registry>" Access Hook.
- If a user has an Access Hook that allows them to view a tab in a panel separate from the main screen (for example, the **Device Details** panel, **Device Summary** panel, or the **Ticket** panel), the user should also have the Access Hook that allows them to view the default tab in the panel. For example, suppose you grant a user with the "Dev:View IFs" Access Hook, which allows a user to view the Interfaces tab in the **Device Administration** panel. You should also grant the user the "Dev:View Details" Access Hook so the user can access to the **Device Properties** page, which is the default page in the **Device Administration** panel.
- If a user has an "Access All", or "View Any" Access Hook, the user will still need the corresponding "View" Access Hook. For example, a user with the "Ticket:Access All" Access Hook must have the "Ticket:View" Access Hook to view tickets.

Blacklisting or Whitelisting Access Hooks

You can override existing user permissions and Access Keys in SL1 by *blacklisting* or *whitelisting* Access Hooks for all users, administrators, or regular users:

- **Blacklisting** disables one or more access hooks. You can disable an access hook for all users, users-level users, administrator-level users, or a combination of user types.
- **Whitelisting** enables one or more access hooks. You can enable an access hook for all users, users-level users, administrator-level users, or a combination of user types.

NOTE: Blacklisting Access Hooks using the following method does not disable links to blacklisted pages, but a user on the black list cannot load blacklisted pages.

Enabling the Access Hook Blacklist or Whitelist

To enable the Access Hook blacklist or whitelist:

1. Go to the console of the Administration Portal, All-In-One Appliance, or Database Server that provides web access for your system or use SSH to access the command line.
2. Use vi (or a text editor of your choice) to create the file `/etc/.custom_alignment.conf`.
3. Configure the permissions for `/etc/.custom_alignment.conf` to allow nginx to read the file:

```
chmod a+r /etc/.custom_alignment.conf
```

4. Add one or more of the following sections to the file; add only the sections that will include at least one blacklist or whitelist rule:
 - **[ALL]**. Blacklist or whitelist Access Hooks for all users
 - **[USER]**. Blacklist or whitelist Access Hooks for all regular users
 - **[ADMIN]**. Blacklist or whitelist Access Hooks for all administrator users
5. Add the hooks that you want to add to your black list or white list:
 - To blacklist an Access Hook, add the following line to the appropriate section, substituting the Access Hook ID where indicated:

```
<access_hook_ID>=deny
```

where `access_hook_ID` is the alphabetic ID that describes the Access Hook. For example, the following code prevents users from viewing passwords in plaintext:

```
CRED_VIEW_PASSWORD=deny
```

- To whitelist an Access Hook:

```
<access_hook_ID>=allow
```

5. Go to the **Cache Management** page (System > Tools > Cache) and delete all cache entries.

Example of the Access Hook Blacklist

Requirement: Make the Database Tool page (System > Tools > DB Tool) inaccessible to all users.

Process: Update `/etc/.custom_alignment.conf` with the following:

```
[ALL]
```

```
SYS_TOOLS_DB=deny
```



Using Access Keys with User-generated Content

Overview

You can use Access Keys to restrict access to user-defined content, specifically dashboards and device groups. Each dashboard or device group can have an associated Access Key that controls user access. The following sections describe how to use Access Keys with each type of content.

TIP: You can create dedicated Access Keys that provide access only to user-defined, shared content by creating an Access Key without any aligned Access Hooks.

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 the menu options, click the Advanced menu icon (.

This chapter includes the following topics:

<i>Using Access Keys with Dashboards</i>	25
<i>Using Access Keys with Device Groups</i>	26
<i>Generating a Report for an Access Key</i>	28

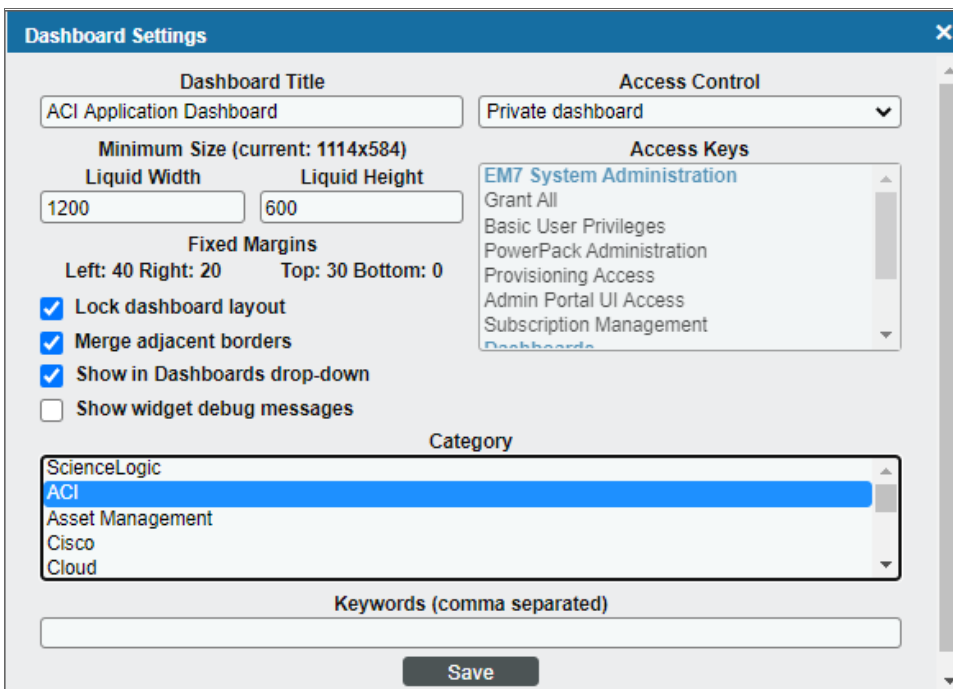
Using Access Keys with Dashboards

To share a classic dashboard with users, you must configure the Access Control for the dashboard to permit other organizations to use it.

To edit a classic dashboard:

1. Open the dashboard you want to configure on the Dashboards tab.
2. Click **[Actions]** and select *Configure Dashboard*. The Dashboard Settings modal opens.
3. Set **Access Control** to *Share with organizations*.
4. Select one or more **Access Keys** to grant access to the dashboard as needed.

NOTE: For more information on dashboards, see the *Dashboards* manual.



The screenshot shows the "Dashboard Settings" modal window. It has a blue header with the title "Dashboard Settings" and a close button (X). The main content area is divided into several sections:

- Dashboard Title:** A text input field containing "ACI Application Dashboard".
- Access Control:** A dropdown menu currently set to "Private dashboard".
- Minimum Size (current: 1114x584):** Two input fields for "Liquid Width" (1200) and "Liquid Height" (600).
- Fixed Margins:** Four input fields for "Left: 40", "Right: 20", "Top: 30", and "Bottom: 0".
- Checkboxes:** Four checkboxes, all of which are checked: "Lock dashboard layout", "Merge adjacent borders", "Show in Dashboards drop-down", and "Show widget debug messages".
- Access Keys:** A list box containing several keys: "EM7 System Administration", "Grant All", "Basic User Privileges", "PowerPack Administration", "Provisioning Access", "Admin Portal UI Access", "Subscription Management", and "Dashboards".
- Category:** A list box containing "ScienceLogic", "ACI" (which is highlighted in blue), "Asset Management", "Cisco", and "Cloud".
- Keywords (comma separated):** An empty text input field.
- Save:** A button at the bottom center.

When you define the dashboard as shared, the Access Keys field will become active. Access Keys in the "EM7 System Administration" and "Dashboards" categories will appear in the **Required Keys** select field. You can select any number of keys from the **Required Keys** select field.

A user must meet the following criteria to use a dashboard controlled by an Access Key:

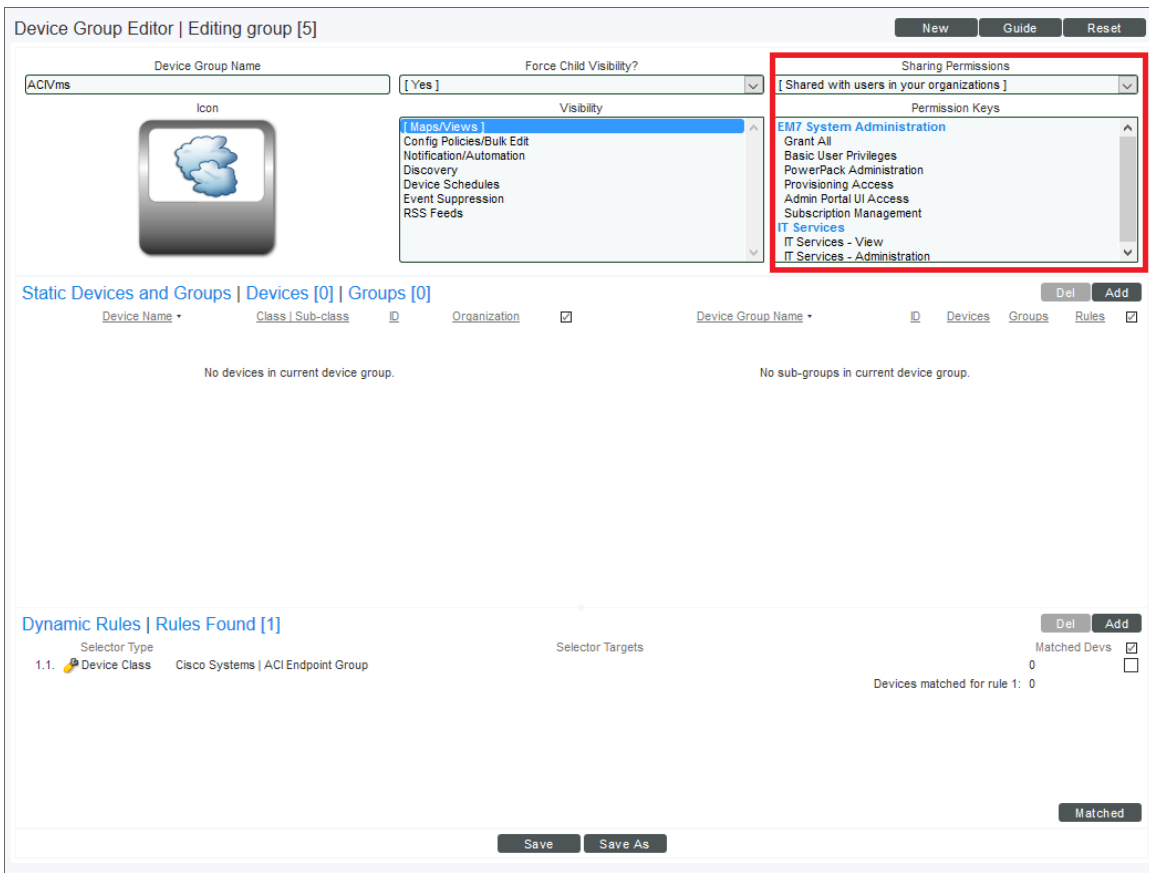
- The user must have at least one of the Access Keys selected in the **Required Keys** select field for the Dashboard. If no Access Keys are selected, any user meeting the following two requirements may access the dashboard.
- The user must be granted an Access Key that includes the "Dash:View" and "Dash:View Shared" Access Hooks.
- The user and the creator of the Dashboard must be members of the same organization.

CAUTION: If a user meets the above requirements and also has been granted an Access Key that includes the "Dash:Edit Shared" Access Hook, that user will be able to edit the shared Dashboard. If a user has been granted an Access Key that includes the "Dash:Add/Rem Shared" Access Hook, that user may delete shared Dashboards.

Using Access Keys with Device Groups

To share a device group with users, you must select the "yes" option in the **Shared (visible to all users)** radio button group when creating or editing a device group:

NOTE: For details on device groups, see the manual *Device Groups and Device Templates*.



The **Permission Keys** select field will become active when "yes" is selected. Access Keys in the "EM7 System Administration" and "Device Groups" categories will appear in the **Permission Keys** select field. You can select any number of keys from the **Permission Keys** select field.

A user must meet the following criteria to use an Access Key controlled device group:

- The user must have at least one of the Access Keys selected in the **Permission Keys** select field for the device group. If no Access Keys are selected, any user meeting the following two requirements will be able to access the device group.
- The user must have the Registry> and Registry>Devices>Groups Access Hooks aligned with one of their granted Access Keys
- The user and creator of the device group must be members of the same organization.

CAUTION: If a user has the DevGroup:Edit Access Hook aligned with one of their granted Access Keys in addition to meeting the above requirements, they will be able to edit the shared device group.

Generating a Report for an Access Key


From the **Access Keys** page you can generate a report on any access key in SL1. The report displays the hook category, hook ID, and hook name of each access hook included in the access key.

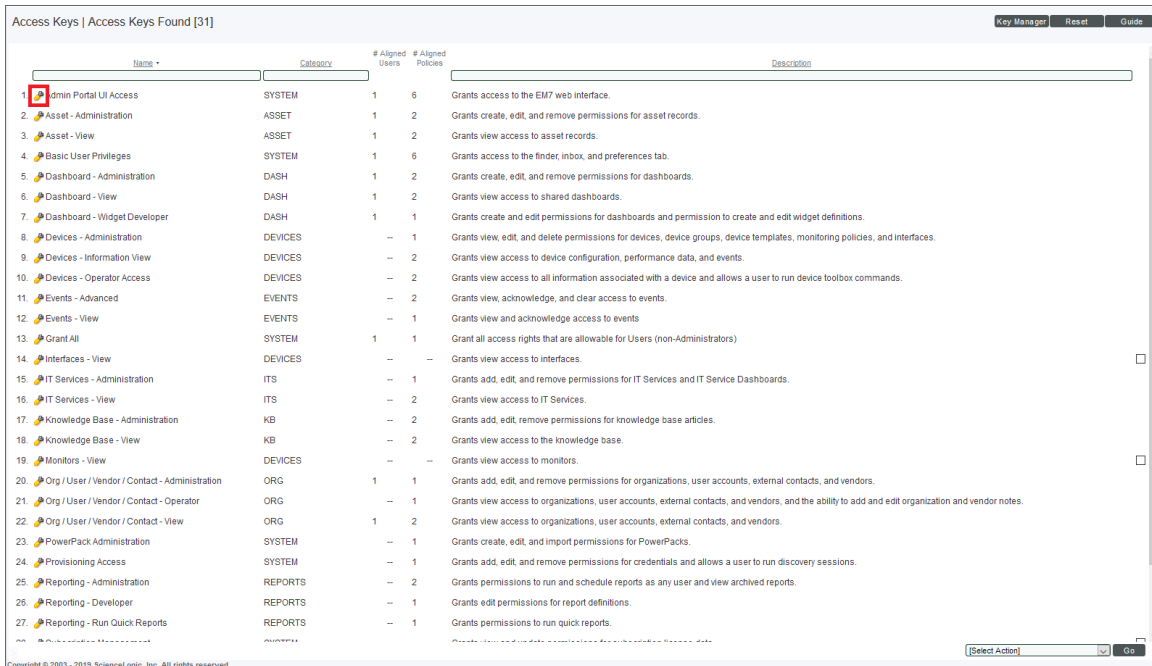
Key Alignment Report generated by em7admin on 2015-06-30 11:17:18
Key Name: Asset - View
Category: Asset Management
Description: Grants view access to asset records.

Hook Category: Asset Management	
Hook ID	Hook Name
AST_VIEW	Asset.View
AST_REG_PAGE	Registry>Assets>Manager




























Hook Category: EM7 System Administration	
Hook ID	Hook Name
SYS_REGISTRY_PAGE	Registry>

To generate a report on access keys:

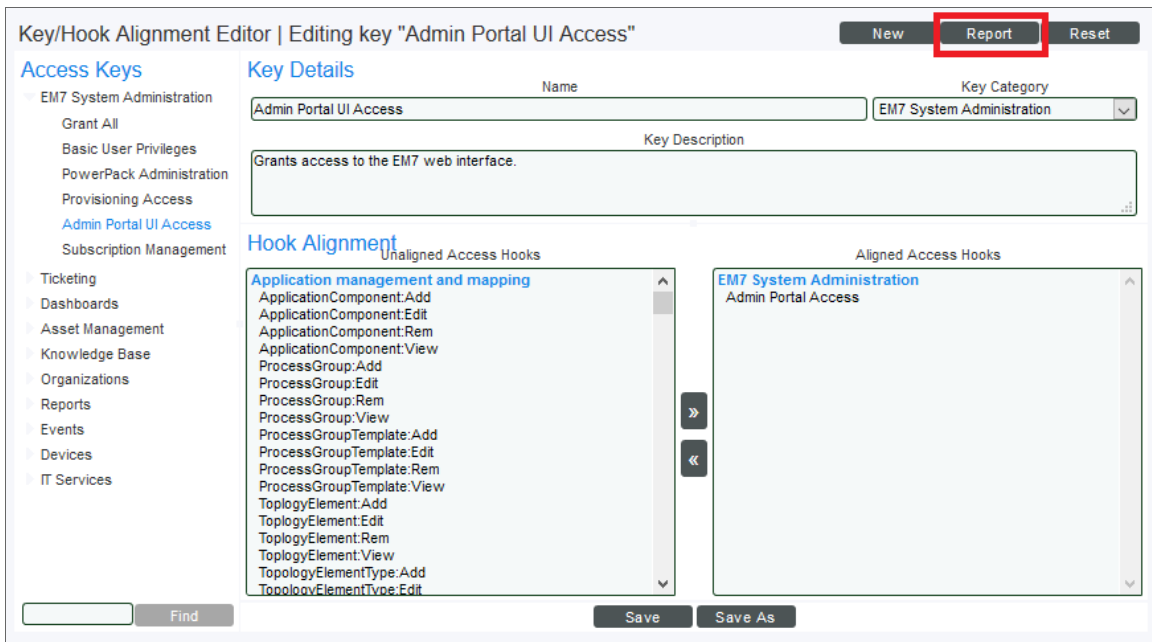
1. Navigate to the **Access Keys** page (System > Manage > Access Keys).
2. Locate the access key for which you want to generate a report and click its wrench icon ():



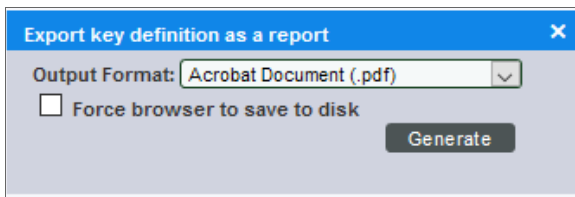
Access Keys | Access Keys Found [31]

Name	Category	# Aligned Users	# Aligned Policies	Description
1  Admin Portal UI Access	SYSTEM	1	6	Grants access to the EM7 web interface.
2  Asset - Administration	ASSET	1	2	Grants create, edit, and remove permissions for asset records.
3  Asset - View	ASSET	1	2	Grants view access to asset records.
4  Basic User Privileges	SYSTEM	1	6	Grants access to the finder, inbox, and preferences tab.
5  Dashboard - Administration	DASH	1	2	Grants create, edit, and remove permissions for dashboards.
6  Dashboard - View	DASH	1	2	Grants view access to shared dashboards.
7  Dashboard - Widget Developer	DASH	1	1	Grants create and edit permissions for dashboards and permission to create and edit widget definitions.
8  Devices - Administration	DEVICES	--	1	Grants view, edit, and delete permissions for devices, device groups, device templates, monitoring policies, and interfaces.
9  Devices - Information View	DEVICES	--	2	Grants view access to device configuration, performance data, and events.
10  Devices - Operator Access	DEVICES	--	2	Grants view access to all information associated with a device and allows a user to run device toolbox commands.
11  Events - Advanced	EVENTS	--	2	Grants view, acknowledge, and clear access to events.
12  Events - View	EVENTS	--	1	Grants view and acknowledge access to events.
13  Grant All	SYSTEM	1	1	Grant all access rights that are allowable for Users (non-Administrators)
14  Interfaces - View	DEVICES	--	--	Grants view access to interfaces.
15  IT Services - Administration	ITS	--	1	Grants add, edit, and remove permissions for IT Services and IT Service Dashboards.
16  IT Services - View	ITS	--	2	Grants view access to IT Services.
17  Knowledge Base - Administration	KB	--	2	Grants add, edit, remove permissions for knowledge base articles.
18  Knowledge Base - View	KB	--	2	Grants view access to the knowledge base.
19  Monitors - View	DEVICES	--	--	Grants view access to monitors.
20  Org / User / Vendor / Contact - Administration	ORG	1	1	Grants add, edit, and remove permissions for organizations, user accounts, external contacts, and vendors.
21  Org / User / Vendor / Contact - Operator	ORG	--	1	Grants view access to organizations, user accounts, external contacts, and vendors, and the ability to add and edit organization and vendor notes.
22  Org / User / Vendor / Contact - View	ORG	1	2	Grants view access to organizations, user accounts, external contacts, and vendors.
23  PowerPack Administration	SYSTEM	--	1	Grants create, edit, and import permissions for PowerPacks.
24  Provisioning Access	SYSTEM	--	1	Grants add, edit, and remove permissions for credentials and allows a user to run discovery sessions.
25  Reporting - Administration	REPORTS	--	2	Grants permissions to run and schedule reports as any user and view archived reports.
26  Reporting - Developer	REPORTS	--	1	Grants edit permissions for report definitions.
27  Reporting - Run Quick Reports	REPORTS	--	1	Grants permissions to run quick reports.

3. The **Key/Hook Alignment Editor** modal page appears. Click the **[Report]** button:



4. The **Export key definition as a report** modal page appears:



Select from the following output formats to generate the report:

- Web page (.html)
- OpenDocument Spreadsheet (.ods)
- Excel Spreadsheet (.xlsx)
- Acrobat Document (.pdf)



5. Click the **[Generate]** button to generate the report. If you selected the *Force browser to save to disk* checkbox on the **Export key definition as a report** modal page, you will be promoted to designate a location to save the report before you can view the report.

Best Practices for Access Permissions

Overview

This chapter describes the best practices that ScienceLogic recommends you follow when creating Access Keys. Although you can completely customize your own Access Keys, the recommendations provided in this section will make managing Access Keys easier.

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 the menu options, click the Advanced menu icon ().

This chapter includes the following topics:

<i>Best Practices</i>	31
-----------------------------	----

Best Practices

ScienceLogic recommends you follow these best practices when creating Access Keys:

- In general, Access Keys should include Access Hooks for one area of the product. It is a good idea to select a category for an Access Key and then include only Access Hooks from the same category. If you want to easily grant a user Access Hooks that cover different sections of the product, we recommend you create an Access Key for each section and then align them with a User Policy.
- If you are creating an Access Key that includes Access Hooks with dependencies, you should also align the Access Hooks they depend on with the Access Key, even if they are in a different category.
- To avoid confusion, you shouldn't create too many similar Access Keys. If there is a large overlap between Access Keys, consider creating an Access Key that only includes the overlapping Access Hooks, then create additional Access Keys for users that must be granted the non-overlapping Access Hooks.
- If you are using Access Keys to control access to user generated content, consider creating Access Keys without aligned Access Hooks solely for that purpose. If you do this, it is easier to grant and remove access to dashboards, knowledge base articles, and device groups without affecting a user's granted Access Hooks.

CAUTION: Due to security vulnerabilities, ScienceLogic recommends that customers who installed SL1 prior to 8.9.2 disable the Knowledge Base. For details, see the release notes for version 8.9.2 of SL1.

Appendix



A

Example: An Access Key to View Assets

Overview

In this example we will create a simple Access Key. We will use the example of a SL1 system used by a service provider to monitor customer devices. The service provider uses the ticketing features of SL1 to track issues reported by customers, and also maintains asset records in SL1 for every hardware device monitored. The Access Key we will design and create is to be granted to the service provider's technical support personnel so they can access asset information for devices.

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 the menu options, click the Advanced menu icon ()

This chapter includes the following topics:

<i>Requirements</i>	33
<i>Selecting Access Hooks</i>	33
<i>Checking Access Hook Dependencies</i>	33
<i>Creating the Access Key</i>	34

Requirements

The service provider has determined their technical support personnel must be able to do the following with assets:

1. Access the **Asset Manager** page.
2. View information about an asset.

Although their technical support personnel must be able to view asset information, the service provider does not want their technical support personnel to add, remove, or edit asset records.

Selecting Access Hooks

If we look at the list of Access Hooks, the following Access Hooks are in the "Asset" category:

- Asset:Add
- Asset:Remove
- Asset:Edit
- Registry>Assets>Manager
- Asset:View

To meet requirement 1, access the **Asset Manager** page, we will align the "Registry>Assets>Manager" Access Hook with this Access Key. To meet requirement 2, view information about an asset, we will align the "Asset:View" Access Hook with this Access Key. We will not align the other three asset Access Hooks to this Access Key so technical support personnel cannot add, remove, or edit assets.

Checking Access Hook Dependencies

Now we have selected the Access Hooks that allow users to do what we want, we must check if that the selected Access Hooks have any dependencies on other Access Hooks. We will look at each selected Access Hook in turn:

- **Registry>Assets>Manager**. This is a navigation Access Hook. As described in the Navigation Access Hooks section of this manual, all navigation access hooks are dependent on a top-level navigation Access Hook. In this case, the **Asset Manager** page is accessed using the **[Registry]** tab, so the user must also be granted the "Registry>" Access Hook. The Best Practice for Access Hook dependencies is to align all the required Access Hooks to the Access Key, so we will include the "Registry>" Access Hook with this Access Key.
- **Asset:View**. This is an action Access Hook. As described in the Action Access Hooks section, we must ensure the user has access to the page on which the action is performed. In this case, the "Asset:View" action is performed on the **Asset Manager**. We have already selected Access Hooks that will grant access to the **Asset Manager** page, so we do not need to align any other Access Hooks to this Access Key.

Creating the Access Key

We have now selected the following Access Hooks to be aligned with the Access Key:

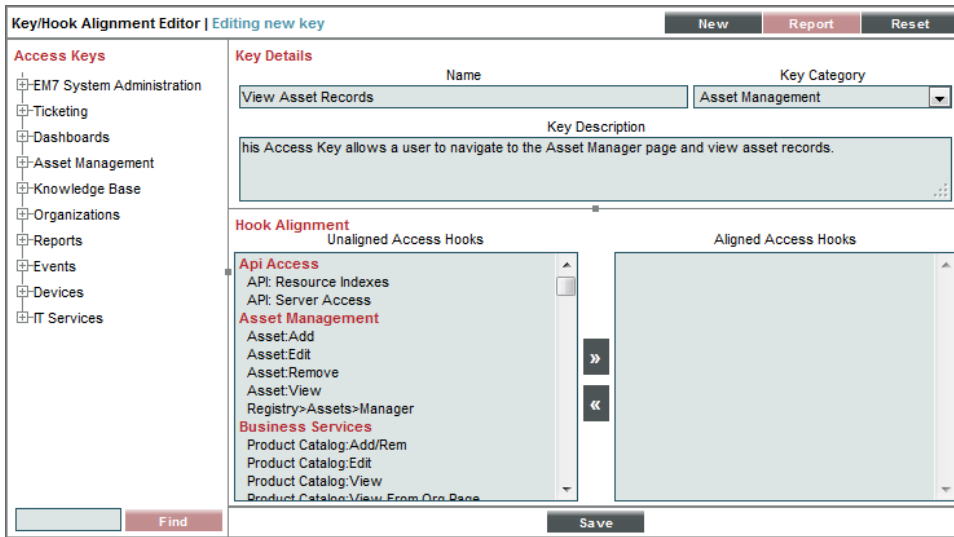
- Registry>Assets>Manager
- Asset:View
- Registry>

We will now perform the following steps to create the Access Key:

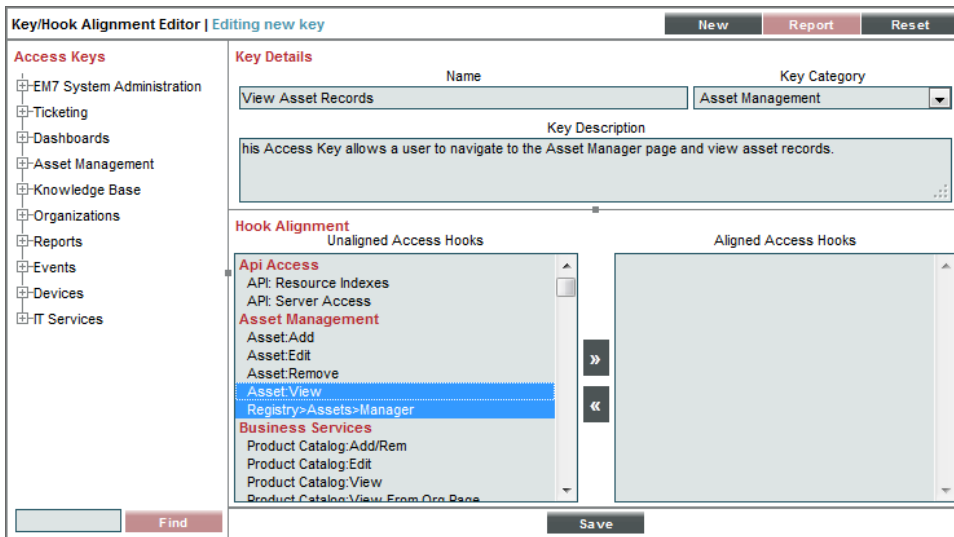
1. To navigate to the **Access Keys** page, go to System > Manage > Access Keys.
2. Click the **[Key Manager]** button to open the **Key/Hook Alignment Editor** page in create mode:

The screenshot shows the 'Key/Hook Alignment Editor' interface. The title bar indicates 'Editing new key' and includes 'New', 'Report', and 'Reset' buttons. The left sidebar shows a tree view of 'Access Keys' with categories like EM7 System Administration, Ticketing, Dashboards, Asset Management, Knowledge Base, Organizations, Reports, Events, Devices, and IT Services. The main area is divided into 'Key Details' and 'Hook Alignment'. 'Key Details' has fields for 'Name', 'Key Category' (set to 'API Access'), and 'Key Description'. 'Hook Alignment' has two columns: 'Unaligned Access Hooks' and 'Aligned Access Hooks'. The 'Unaligned' list includes 'Api Access', 'API: Resource Indexes', 'API: Server Access', 'Asset Management', 'Asset:Add', 'Asset:Edit', 'Asset:Remove', 'Asset:View', 'Registry>Assets>Manager', 'Business Services', 'Product Catalog:Add/Rem', 'Product Catalog:Edit', 'Product Catalog:View', and 'Product Catalog:View From Org Page'. There are right and left arrow buttons between the columns. At the bottom are 'Find' and 'Save' buttons.

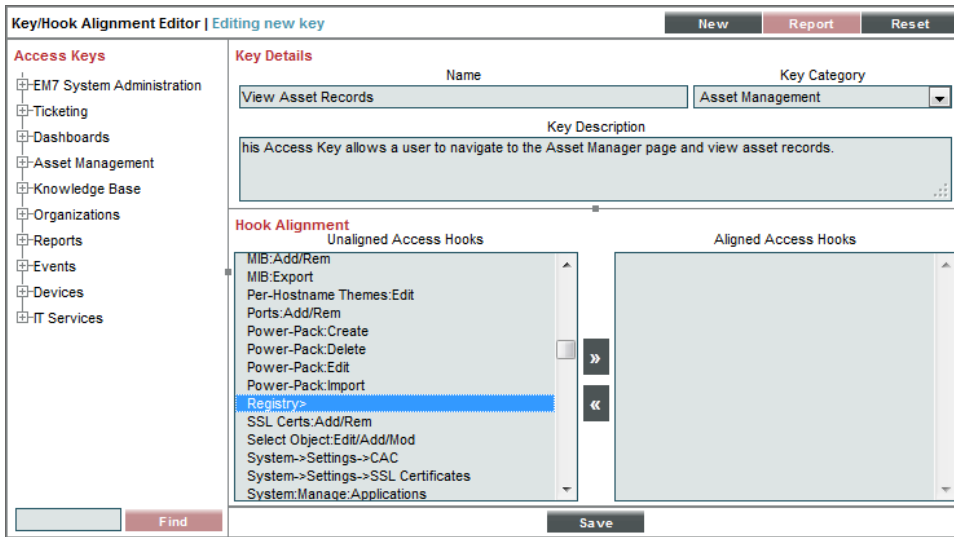
3. It's preferable to name an Access Key based on what it does, so enter "View Asset Records" in the **Name** field.
4. Because this Access Key grants access to Assets, select "Asset Management" from the **Key Category** drop down list.
5. The description for a key should give a clear indication of what a user who is granted this Access Key will be able to do. Although this Access Key is being designed for a specific user, it is a good idea to make the description as generic as possible to prevent confusion if the Access Key is reused for another purpose. Enter this description in the **Key Description** field: "This Access Key allows a user to navigate to the **Asset Manager** page and view asset records." The Key Manager should now look like this:



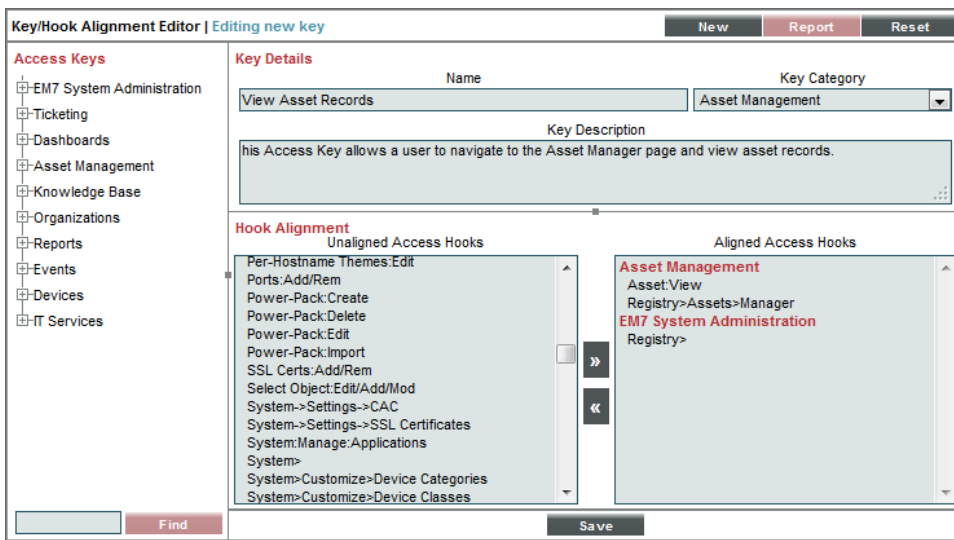
6. We need to select the Access Hooks to be aligned with the Access Key. Locate the "Asset Management" section of the **Unaligned Access Hooks** select list, then click on "Asset:View" and "Registry>Assets>Manager" while holding down the **CTRL** key on your keyboard:



7. Then scroll to the "EM7 System Administration" section of the **Unaligned Access Hooks** select and click on "Registry>" while holding down the **CTRL** key on your keyboard:



- Click the right arrow button ([>>]) to move these three Access Hooks to the **Aligned Access Hooks** select list:



- Click the **[Save]** button to save the Access Key. The Access Key is now finished and ready to be granted.

© 2003 - 2022, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

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

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

Copyrights and Trademarks

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

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

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

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

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

Other

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

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



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

International: +1-703-354-1010