Access Permissions

Skylar One version 12.5.1

Table of Contents

Chapter 1

Introduction to Access Permissions

Overview

This manual is intended for system administrators who are responsible for controlling user access to Skylar One (formerly SL1) systems. This manual describes the access permissions system used in Skylar One. 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 Skylar One user interface:

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

This chapter covers the following topics:

What is an Access Hook?

An ***access hook*** controls access to a specific action that can be performed in the Skylar One user interface. These actions include navigating to a page, viewing information about an element in the system, and editing elements in the system. Each access hooks is designed to be highly granular, providing access to only one action on one specific entity or page. Because of this granularity, there are hundreds of access hooks available in Skylar One.

Access hooks are not granted to users directly; instead, access hooks are grouped together to form an access key, which can be granted to users either directly through their user account or indirectly through a user policy.

What is an Access Key?

Because there are several hundred access hooks provided in Skylar One, granting each individual access hook to a user or user policy would be a time-consuming process.

Therefore, Skylar One 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 Skylar One. Every access hook, except for the access hook that controls the Access Key Manager, is aligned to the "Grant All" access key. Skylar One also includes default access keys for the most common user profiles and common tasks in Skylar One.

Role-Based Access Control Restrictions

Role-based access control (RBAC) is a methodology that enables Skylar One administrators to determine which end users have access to which features within the system. It has three primary components:

- Organization memberships
- Access hooks and access keys
- User accounts and user policies

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 elements associated with organizations to which they have membership.

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 is assigned the appropriate access keys to view the **Devices** page or **Device Manager** page, the user will see only devices in Org A and Org B on those pages. The user will not be able to see or interact with elements 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:

- Non-administrator users cannot modify administrator accounts.
- Non-administrator users cannot make themselves or another user an administrator.
- Users cannot grant or remove access keys that they have not also been granted.

NOTE: For more information about RBAC, see the section on "Role-Based Access Control" in the ***Organizations and Users*** manual.

High-Level Access Keys

In Skylar One, the "Grant All" access key assigns most available access hooks to users who have that access key aligned to their user account. It should be reserved for only administrator users and high-level, non-administrator users that require access to all of the functionality within Skylar One.

In Skylar One 12.5.1 and above, the following additional access keys can be used to grant varying levels of administrator access, based on the user's role and the type of Skylar One deployment:

- Tenant - Administration, which provides most of the functionality of the "Grant All" access key, excluding the features controlled by the "Platform - Administration" access key and the ability to create or edit access keys or their alignment with access hooks.
- Platform - Administration, which is assigned by default to administrator user accounts and specifically grants the following permissions that are not aligned with the "Tenant - Administration" access key:
    - The ability to access the **Backup Management** and **Database Tool** pages
    - The ability to enable and disable administrative processes or edit the collection frequency of those processes
    - The ability to edit email gateway settings

Chapter 2

Creating and Managing Access Keys

Overview

This chapter describes the layout and functionality of the **Access Keys** and **Access Hooks** pages in Skylar One (formerly SL1), and includes step-by-step instructions on how to create an Access Key.

Use the following menu options to navigate the Skylar One user interface:

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

This chapter covers the following topics:

Viewing the List of Access Hooks

The **Access Hooks** page (System > Manage > Access Hooks) displays a list of all Access Hooks in Skylar One. 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***. Alphabetic 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 Skylar One. For example "AST_" stands for Asset Management and "DASH" stands for dashboards. The remaining parts of the ID further describe the location in Skylar One 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.

Viewing the List of Access Keys

The **Access Keys** page (System > Manage > Access Keys) 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

Skylar One includes default Access Keys to use with the most common user profiles and the most common tasks in Skylar One. 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 Public Dash:Edit Shared	Network Engineers System Administrators

Access Key	Description	Aligned Access Hooks	Useful For
		Dash:Share Dash:View Dash:View Public Dash:View Shared Dash:Widget:Add/Rem Dash:Widget:Edit Dashboard:Scheduler	NOC Staff Provisioning Staff Support Engineers Implementation Engineers QA Analysts
Dashboard - View	Grants view access to shared dashboards	Dash:View Dash:Public 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 Public 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.	DevGroup:View 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 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	Dev:Collections Edit Dev:Collections View Dev:Config Dev:Events Summary Dev:IF Graphs Dev:Interfaces Dev:Logs	Network Engineers NOC Staff

Access Key	Description	Aligned Access Hooks	Useful For
	run device toolbox commands	Dev:Monitors Dev:Notes:View Dev:Performance Graphs Dev:Process View Dev:Remove Dev:Schedule:View Dev:Software Dev:TCP Ports 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 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>Vanished Device Manager Registry>Devices>Device Relationships	
Devices - Administration	Grants view, edit, and delete permissions for devices, device groups, device templates, monitoring policies, and	DevGroup:Add/Rem DevGroup:Edit DevGroup:View Registry>Devices>Groups Dev:Collections Edit Dev:Collections View Dev:Config Dev:Edit	Provisioning Staff Support Engineers Implementation Engineers

Access Key	Description	Aligned Access Hooks	Useful For
	interfaces	Dev:Edit Class Dev:Events Summary Dev:IF Graphs Dev:Interfaces Dev:Logs Dev:Monitors Dev:Notes:Add Dev:Notes:Edit Dev:Notes:View Dev:Notes: Remove Dev:Performance Graphs Dev:Process View Dev:Redirects Dev:Remove Dev:Schedule:View Dev:Software Dev:TCP Ports Dev:Template:Add/Remove Dev:Template:Edit Dev:Template:View Dev:Thresholds Dev:Thresholds:Dynamic App Dev:Threshold General 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	QA Analysts

Access Key	Description	Aligned Access Hooks	Useful For
		Registry>Devices>Hardware Registry>Devices>Processes Registry>Devices>Services Registry>Devices>Software Registry>Devices>Templates Registry>Devices>Vanished Device Manager Registry>Networks>Device Relationships Registry> Networks:Interfaces:Add Networks:Interfaces:Edit Networks:Interfaces:Remove 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>Webhooks 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 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	Create a cred Cred:Basic:Add/Rem Cred:Basic:Edit Cred:DB:Add/Rem	Provisioning Staff Support

Access Key	Description	Aligned Access Hooks	Useful For
	allows a user to run discovery sessions	Cred:DB:Edit Cred:POWERSHELL:Add/Rem Cred:POWERSHELL:Edit Cred:Passwords:Edit Cred:Passwords:View Cred:SNMP:Add/Rem Cred:SNMP:Edit Cred:SOAP:Add/Rem Cred:SOAP:Edit Cred:SSH:Add/Rem Cred:SSH:Edit Credential field:create Credential field:delete Credential field:update Credential field:view Edit Credential System>Manage>Credentials View a credential delete a cred Appliances:View Collector Groups:View Discovery:Add Discovery:Delete Discovery:Edit Discovery:Run Discovery:View System> System>Manage>Discovery	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:Resolution Rating:View Event:Resolution:View 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
Events - Advanced	Grants view acknowledge and clear access to events	Event:Acknowledge Event:Clear Event:Kiosk Event:Reacknowledge Event:Resolution Rating:Add/Rem Event:Resolution Rating:Edit Event:Resolution Rating:View Event:Resolution:Add/Rem Event:Resolution:Edit Event:Resolution:View Event:View (From Org Page	Network Engineers NOC Staff

Access Key	Description	Aligned Access Hooks	Useful For
		Events/Event:View	
Interfaces - View	Grants view access to Interfaces	Dev:View Network:Interfaces:View	Customers Network Engineers System Administrators NOC Staff
IT Services - View	Grants view access to IT Services	DevGroup:View 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
Monitors - View	Grants view access to monitors	Monitors:View	
Org / User / Vendor/ Contact - View	Grants view access to organizations, user accounts, external contacts, and vendors	Contact:View 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/ Contact - Administration	Grants add, edit, and remove permissions for organizations, user accounts, external	Custom Select Objects:Organization Add/Edit/Delete Custom Select Objects:User Account Add/Edit/Delete Registry> Org:AddRem Org:AltLocations:Edit	Provisioning Staff Support Engineers Implementation

Access Key	Description	Aligned Access Hooks	Useful For
	contacts, and vendors	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 User:View Vendor:Add/Rem Vendor:Edit Vendor:Edit Notes Vendor:Notes Vendor:View	Engineers QA Analysts
Org / User / Vendor/ Contact - 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	Report Output Format: HTML Report Output Format: ODS Report Output Format: PDF Report Output Format: XLSX Reports> Reports>Create Report>Quick Report	Customers Help Desk Other staff who require view-only access to Quick Reports

Access Key	Description	Aligned Access Hooks	Useful For
Reporting - Administration	Grants permissions to run and schedule reports as any user and view archived reports	Report Output Format: HTML Report Output Format: ODS Report Output Format: PDF Report Output Format: XLSX 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
Subscription Management	Grants view and update permissions for subscription license data	Subscription:Edit Subscription: View	Customers Help Desk
Ticketing - End User	Grants basic view and create permissions for tickets and allows a user to add notes to a ticket	Ticket:Console: View Ticket:All in Orgs Ticket:Assign within Queue Ticket:Create Ticket:Edit Ticket:External Ticket Access Ticket:History (per Org) Ticket:History:View Ticket:Messaging Ticket:Notes:Add Ticket:Notes:Attachments:Add Ticket:Reports Ticket:Statistics:View Ticket:View	Customers Help Desk Other staff who need to create tickets and view tickets only
Ticketing - Operator	Grants create view and edit permissions for ticketing	Ticket:Console: View Ticket:Alignment Ticket:All in Orgs Ticket:Assign Ticket:Change Severity Ticket:Create Ticket:Edit Ticket:External Ticket Access Ticket:History (per Org) Ticket:History: View Ticket:Inbox:Statistics	Network Engineers NOC Staff Provisioning Staff Support Engineers Implementation

Access Key	Description	Aligned Access Hooks	Useful For
		Ticket:Messaging Ticket:Notes:Add Ticket:Notes:Attachments: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	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:Console:View 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:Create Ticket:Customize Forms Ticket:Delete Ticket:Edit Ticket:Escalation:Add/Rem Ticket:Escalation:Edit Ticket:Events:Alignment Ticket:External Ticket Access Ticket:History (per Org) Ticket:History:View Ticket:Inbox:Statistics Ticket:Messaging Ticket:Notes:Add Ticket:Notes:Attachments:Add Ticket:Notes:Attachments:Blacklist:Edit/Add/Rem Ticket:Notes:Cloaked Ticket:Notes:Cloaked Edit Ticket:Notes:Edit Ticket:Notes:Remove Ticket:Queue:Edit Ticket:Queue:View Ticket:Reports Ticket:Scheduler	Provisioning Staff Support Engineers Implementation Engineers QA Analysts

Access Key	Description	Aligned Access Hooks	Useful For
		Ticket:Statistics:View Ticket:Templates:Edit/Add/Rem Ticket:View Ticket:View Any Ticket:View Logs Ticket:View Watchers Ticket:Watchers:Add/Rem 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 Skylar One prior to 8.9.2 disable the Knowledge Base. For details, see the release notes for version 8.9.2 of Skylar One.

    - ***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. Click **[Save]**. The message "Save Completed" will be displayed at the top of the screen.
8. If you click the **[Save]** button again, any changes made will be applied to the same Access Key. Click 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 wrench 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, select 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 in Skylar One (formerly SL1) 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 Skylar One 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:

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 Skylar One, 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 Skylar One.

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 Acces 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 Skylar One, e.g. "Ticket" or "Org".
- If applicable, the specific part of the entity or area of Skylar One, 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 Skylar One by *blacklisting* or *whitelisting* Access Hooks for all users, administrators, or regular users:

- ***Blacklisting*** disables one or more access hooks. You can disables 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_PASSWORDS=deny
     ```

   - To whitelist an Access Hook:

     ```
     <access_hook_ID>=allow
     ```

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

Chapter 4

Using Access Keys with User-generated Content

Overview

You can use Access Keys to restrict access to user-defined content in Skylar One (formerly SL1), 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 Skylar One 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:

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.

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 Skylar One. The report displays the hook category, hook ID, and hook name of each access hook included in the access key.

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 (). The **Key/Hook Alignment Editor** modal page appears.
3. Click the **[Report]** button. The **Export key definition as a report** modal page appears.
4. 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.

Chapter 5

Best Practices for Access Permissions

Overview

This chapter describes the best practices that ScienceLogic recommends you follow when creating Access Keys in Skylar One (formerly SL1). 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 Skylar One 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:

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 Skylar One prior to 8.9.2 disable the Knowledge Base. For details, see the release notes for version 8.9.2 of Skylar One.

Appendix

A

Skylar One Access Hooks

Overview

This appendix lists the Access Hooks that are available to align to your Access Keys in Skylar One (formerly SL1).

Use the following menu options to navigate the Skylar One 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:

Application Management

Name	Access Hook ID	Description
ApplicationComponent:Rem	APP_COMP_ REMOVE	Remove an application component
ApplicationComponent:Edit	APP_COMP_EDIT	Edit an application component
ApplicationComponent:Add	APP_COMP_ADD	Add an application component
ApplicationComponent:View	APP_COMP_VIEW	Allows read access for application components

Asset Management

Name	Access Hook ID	Description
Asset:Remove	AST_REM	Remove an asset record
Asset:View	AST_VIEW	Allows read access to an asset record
Asset:Edit	AST_EDIT	Allows write access to asset records, not including add/remove.
Asset:Add	AST_ADD	Add an asset record
Registry>Assets>Manager	AST_REG_PAGE	View the Asset Manager registry page

Business Services

Name	Access Hook ID	Description
Product Catalog:Add/Rem	BIZ_PRODUCT_ CATALOG_ADDREM	Add or remove catalog items (SKUs)
Registry>Business Services>Product Catalog	BIZ_PRODUCT_ CATALOG_REG_ PAGE	Access the Product Catalog registry page
Service Catalog:View	BIZ_SERVICE_ CATALOG_VIEW	View a service within the Service Catalog
Registry>Business Services>Bandwidth Billing	BIZ_BW_BILLING_ REG_PAGE	Access the Bandwidth Billing registry page

Registry>Business Services>Distribution Lists	BIZ_DIST_LIST_REG_ PAGE	Access the Distribution List registry page
Product Catalog: View From Org Page	BIZ_PRODUCT_ CATALOG_ORG_VIEW	View product catalog data from the Org properties page
Registry>Business Services>Service Catalog	BIZ_SERVICE_ CATALOG_REG_ PAGE	View the Service Catalog registry page
Registry>Business Services>Service Usage	BIZ_SERV_USAGE_ REG_PAGE	Access the Service Usage registry page
Product Catalog:Edit	BIZ_PRODUCT_ CATALOG_EDIT	Edit/Alter a Product Catalog item (SKU)
Product Catalog:View	BIZ_PRODUCT_ CATALOG_VIEW	View a Product Catalog item
Registry>Business Services>Service Notifier	BIZ_ERVICE_ NOTIFIER_REG_PAGE	Utilize the Business Services notifier tool

Contacts

Name	Access Hook ID	Description
Contact:View	CONTACT_VIEW	View a contact

Credentials

Name	Access Hook ID	Description
Cred:DB:Add/Rem	CRED_DB_ADDREM	Add or remove a credential of type 'DB'
Cred:LDAP:Add/Rem	CRED_LDAP_ ADDREM	Add or remove a credential of type 'LDAP'
delete a cred	CREDENTIAL_ DELETE	Delete a credential
Cred:POWERSHELL:Edit	CRED_ POWERSHELL_EDIT	Edit a credential type of 'POWERSHELL'
Credential field: delete	CREDENTIAL_ FIELDS_DELETE	Delete a credential field
Cred:SNMP:Edit	CRED_SNMP_EDIT	Edit a credential type of 'SNMP'

View a credential	CREDENTIAL_VIEW	View a credential
Cred:SSH:Add/Rem	CRED_SSH_ ADDREM	Add or remove a credential of type 'SSH'
Cred:Passwords:Edit	CRED_CHANGE_ PASSWORDS	Change passwords in a credential
Credential Tests: View and Edit	SYS_CREDENTIAL_ TESTS_PAGE	Access the System>Customize>Credential Test page
Cred:Test	CRED_EXECUTE_ TEST	Execute a credential test
Create a cred	CREDENTIAL_ CREATE	Create a credential
Cred:POWERSHELL:Add/Rem	CRED_ POWERSHELL_ ADDREM	Add or remove a credential type of 'POWERSHELL'
Credential field: create	CREDENTIAL_ FIELDS_CREATE	Create a credential field
Cred:SNMP:Add/Rem	CRED_SNMP_ ADDREM	Add or remove a credential type of 'SNMP'
Credential field:view	CREDENTIAL_ FIELDS_VIEW	View a credential field
Cred:SOAP:Edit	CRED_SOAP_EDIT	Edit a credential of type 'SOAP'
Cred:Basic:Edit	CRED_BASIC_EDIT	Edit a credential of type 'basic'
Cred:Passwords:View	CRED_VIEW_ PASSWORDS	View passwords in a credential
Cred:DB:Edit	CRED_DB_EDIT	Edit a credential type of 'DB'
Cred:LDAP:Edit	CRED_LDAP_EDIT	Edit a credential type of 'LDAP'
Edit credentials	CREDENTIAL_EDIT	Edit credentials
System>Manage>Credentials	CRED_REG_PAGE	Access the Credentials Management registry page
Credential field: update	CREDENTIAL_ FIELDS_EDIT	Update a credential field
Cred:SOAP:Add/Rem	CRED_SOAP_ ADDREM	Add or remove a credential of type 'SOAP'
Cred:Basic:Add/Rem	CRED_BASIC_ ADDREM	Add or remove a credential of type 'basic'
Cred:SSH:Edit	CRED_SSH_EDIT	Edit a credential of type 'SSH'

Customer Portal

Name	Access Hook ID	Description
Customer Portal: Can view portal	CP_USER	Allows user to login to the customer portal
Customer Portal: Admin	CP_ADMIN	Allows user to administer the customer portal

Dashboards

Name	Access Hook ID	Description
Dashboard:Scheduler	DASH_SCHEDULER	View and edit scheduled dashboards
Device Dashboards:Unalign All	DEVICE_DASH_ UNALIGN	Allows a device dashboard to have all alignments removed
Dash:View Public	DASH_VIEW_ PUBLIC	View public dashboards
Dash:Widget:Edit	DASH_WIDGET_ EDIT	Edit dashboard widget definitions
Dash:Edit	DASH_EDIT	Edit a dashboard's properties
Device Dashboards: Assign to Device Category	DEVICE_DASH_ ASSIGN_CAT	Allows a device dashboard to be assigned to a device category
Dash:Proxy Service:Add/Rem	DASH_PROXY_ ADDREM	Add or remove a web proxy service
Device Dashboards:Add/Rem/Edit	DEVICE_DASH_EDIT	Allows adding, editing, and removing device dashboards
System>Customize>Dashboards	DASH_REG_PAGE	Access the Dashboards registry page
Device Dashboards: Set Global	DEVICE_DASH_ SET_GLOBAL	Allows a device dashboard to be set as the global default
Dash:View	DASH_VIEW	View owned dashboards
Dash:Widget:Add/Rem	DASH_WIDGET_ ADDREM	Add or remove dashboard widget definitions
Registry>Devices>Groups	DGRP_REG_PAGE	View Device Groups registry page
DevGroup:Edit	DGRP_EDIT	Edit a Device Group
DevGroup:Add/Rem	DGRP_ADDREM	Add or remove a Device Group

Dash:Add/Rem Shared	DASH_ADDREM_ SHARED	Remove someone else's shared dashboard
Device Dashboards:Assign To An Application	DEVICE_DASH_ ASSIGN_APP	Allows a device dashboard to be assigned to an application
Dash:Edit Shared	DEVICE_EDIT_ SHARED	Edit a shared dashboard's properties
Device Dashboards: Assign to Device	DEVICE_DASH_ ASSIGN_DEVICE	Allows a device dashboard to be assigned to a device
Registry>Web Proxies	DASH_PROXY_ REG_PAGE	Access the Web Proxy Services registry page
System>Customize>Device Dashboards	DEVICE_DASH_ REG_PAGE	Allows viewing of the Device Dashboards registry page
Dash:Share	DASH_SHARE	Share a dashboard with other users
Dash:View Shared	DASH_VIEW_ SHARED	View a shared dashboard
Dash:Add/Rem	DASH_ADDREM	Add or remove a custom dashboard
System>Customize>Dashboard Widgets	DASH_WIDGET_ REG_PAGE	Access the Dashboard Widgets registry page
Dash:Edit:Public	DASH_EDIT_PUBLIC	Edit a public dashboard's properties
Device Dashboards:Assign To Device Class	DEVICE_DASH_ ASSIGN_CLASS	Allows a device dashboard to be assigned to a device class
Dash:Proxy Service:Edit	DASH_PROXY_EDIT	Edit a web proxy service
Device Dashboards: Replace Alignments	DEVICE_DASH_ REASSIGN	Allows a device dashboard to have all alignments replaced

Device Groups

Name	Access Hook ID	Description
Registry>Devices>Groups	DGRP_REG_PAGE	View Device Groups registry page
DevGroup:Edit	DGRP_EDIT	Edit a Device Group
DevGroup:Add/Rem	DGRP_ADDREM	Add or remove a Device Group
DevGroup:View	DGRP_VIEW	Delete a device category

Devices

Name	Access Hook ID	Description
Dev:Unmerge Physical/Component	DEV_COMPONENT_ UNMERGE	Separate a merged device into physical and component devices
Dev:Notes:View	DEV_NOTES_VIEW	View Device Notes
Dev:Template:Edit	DEV_TEMPLATE_ EDIT	Edit Device Templates
Dev:Tools:PingTool	DEV_TOOLS_RUN_ PING_TOOL	Access the Ping tool in the Device Toolbox
Dev:Agent:Edit	DEV_AGENT_EDIT	Edit an agent
Dev:Remove	DEV_DEL	Remove a device from the classic user interface (EM7)
Registry>Devices>Processes	DEV_PROCESS_ REG_PAGE	View the Device Processes registry page
Dev:Thresholds:Dynamic App	DEV_THRESHOLDS_ DYNAPP	Edit Dynamic Application thresholds for a device (Does not require Dev:Edit)
Dev:Tools:Secure Web	DEV_TOOLS_RUN_ SECURE_WEB	Access the Secure Web tool in the Device Toolbox
Dev:Category:Add	DEV_CATEGORY_ ADD	Add a device category
Dev:Events Summary	DEV_EVENTS_VIEW	View Events on the Device Properties pop-up window
Dev:Redirects	DEV_REDIRECT_ VIEW	View the Redirects tab on the device summary pop-up window
Dev:Thresholds	DEV_THRESHOLDS_ VIEW	View the Thresholds tab on the device summary pop-up window
Dev:Tools:SSH	DEV_TOOLS_RUN_ SSH	Access the SSH tool in the Device Toolbox
Dev:View Category	DEV_CATEGORY_ VIEW	View a category
Dev:Interfaces	DEV_INTERFACES_ VIEW	View the Interfaces tab within the properties pop-up window

Registry>Devices>Services	DEV_SERVICES_ REG_PAGE	Access the Device Services registry page
Dev:Tool:ARIN Whois	DEV_TOOLS_RUN_ ARIN_WHOIS	Access the ARIN Whois tool in the Device Toolbox
Dev:Software	DEV_SOFTWARE_ VIEW	View the Software tab on the device summary pop-up window
Dev:Tools:Availability Check	DEV_TOOLS_RUN_ AVAIL	Access to run the Availability Check
Dev:Topology	DEV_TOPOLOGY_ VIEW	View the Topology tab on the device summary pop-up window
Dev:Collections Edit	DEV_COLLECTIONS_ EDIT	Edit the Collections tab on the device summary pop-up window
Dev:Schedule:View	DEV_MAINT_VIEW	View the Schedule tab on the device summary pop-up window
Dev:Template:Add/Remove	DEV_TEMPLATE_ ADDREM	Add or remove Device templates
Dev:Tools:FTP	DEV_TOOLS_RUN_ FTP	Access the FTP tool in the Device Toolbox
Registry>Devices>Device Components	DEV_COMPONENT_ REG_PAGE	View Device Components registry page
Dev:Notes:Remove	DEV_NOTES_ REMOVE	Remove device notes
Dev:Template:View	DEV_TEMPLATE_ VIEW	View Device templates
Dev:Tools:Reverse DIG	DEV_TOOLS_RUN_ REVERSE_DIG	Access the Reverse DIG tool in the Device Toolbox
Dev:Agent:Add	DEV_AGENT_ADD	Add an agent
Dev:Create	DEV_CREATE	Create a new device
Dev:Monitors	DEV_POLICIES_VIEW	View the Monitors tab on the device summary pop-up window
Dev:Thresholds:Retention	DEV_THRESHOLDS_ RETENTION	Edit Data Retention thresholds for a device (Does not require Dev:Edit)
Dev:Tools:SNMP Walker	DEV_TOOLS_RUN_ SNMP_WALKER	Access the SNMP Walker tool in the Device Toolbox
Dev:Agent:View	DEV_AGENT_VIEW	Read access for agents
Dev:Edit	DEV_EDIT	Edit the properties of a device

Dev:Tools:Traceroute	DEV_TOOLS_RUN_ TRACEROUTE	Access the Traceroute tool in the Device Toolbox
Dev:View:Profile	DEV_PROFILE_VIEW	View the device profile page
Dev:Category:Rem	DEV_CATEGORY_ REM	Delete a device category
Dev:IF Graphs	DEV_IF_ PERFORMANCE_ GRAPHS	View Interface Performance Graphs of a device
Registry>Networks>Device Relationships	DEV_RELATIONS_ REG_PAGE	Access the Device Relationship registry page
Dev:Tools	DEV_TOOLS_RUN	Access the Device Toolbox on the device details pop-up window
Dev:Tools:Terminal	DEV_TOOLS_RUN_ TERMINAL	Access the Terminal tool in the Device Toolbox
Dev:View Class	DEV_CLASS_VIEW	View a class
Dev:Schedule:Add/Rem/Edit	DEV_MAINT_ ADDREM	Change events in the Schedule tab on the device summary pop-up window (Does not require Dev:Edit)
Registry>Devices>Software	DEV_SOFTWARE_ REG_PAGE	View the Device Software registry page
Dev:Tools:ARP Ping	DEV_TOOLS_RUN_ ARP_PING	Access the ARP Ping tool in the Device Toolbox
Dev:Tools:Web Policy	DEV_TOOLS_RUN_ WEB_POLICY	Access Web Policy tool in the Device Toolbox
Dev:Merge Physical/Component	DEV_COMPONENT_ MERGE	Merge a physical and component device together
Dev:Notes:Edit	DEV_NOTES_EDIT	Edit Device notes
Dev:TCP Ports	DEV_TCP_PORT_ VIEW	View the TCP Ports tab on the device details pop-up window
Dev:Tools:Forward DIG	DEV_TOOLS_RUN_ FORWARD_DIG	Access the Forward DIG tool in the Device Toolbox
Dev:View	DEV_VIEW	View basic device details from assorted pop-up windows/modals/etc
Device Investigator Layout: Set Global	DEVICE_ INVESTIGATOR_SET_ GLOBAL	Allows all users to access the Device Investigator Layout
Dev:Config	DEV_CONFIG_VIEW	View the Config tab n the device summary pop-up window

Dev:Performance Graphs	DEV_PERF_ REPORT_VIEW	View a device's performance graphs
Registry>Devices>Templates	DEV_TEMPLATE_ REG_PAGE	View the Device Templates registry page
Dev:Tools:Port Scan	DEV_TOOLS_RUN_ PORT_SCAN	Access the Port Scan tool in the Device Toolbox
Dev:Agent:Rem	DEV_AGENT_ REMOVE	Remove an agent
Dev:View Details	DEV_DETAILS_VIEW	View the Device Properties page
Dev:Process View	DEV_PROCESS_ VIEW	View a process from the Devices>Processes page
Dev:Thresholds:General	DEV_THRESHOLDS_ GENERAL	Edit system thresholds for a device (Does not require Dev:Edit)
Dev:Tools:SNMP Dump	DEV_TOOLS_RUN_ SNMP_DUMP	Access the SNMP Dump tool in the Device Toolbox
Dev:Category:Edit	DEV_CATEGORY_ EDIT	Edit a device category
Registry>Devices>Hardware	DEV_HARDWARE_ REG_PAGE	View a Hardware registry page
Registry>Devices>Device Manager	DEV_REG_PAGE	View the Device registry
Dev:Tickets	DEV_TKT_VIEW	View the Tickets tab on the device details pop-up window
Dev:Tools:Telnet	DEV_TOOLS_RUN_ TELNET	Access the Telnet tool in the Device Toolbox

EM7 Administration

Name	Access Hook ID	Description
MIB:Add/Rem	SYS_MIB_ADDREM	Upload or remove an MIB
Misc>Skylar One License Info: View	MISC_LICENSE_ VIEW	View the Skylar One License information
System>Manage>PowerPacks	SYS_POWERPACK_ REG_PAGE	Access the PowerPack registry page

System>Settings>Password Reset Email	SYS_SETTINGS_ PASSWORD_ RESET_EMAIL	Access the Password Reset Email configuration page
Library:Import	SILOLIB_IMPORT	Import or upload a library
Ports:Add/Rem	SYS_ CUSTOMERIZE_ PORTS_ADDREM	Alter port configurations withing System>Customize>TCP-IP Ports
Application Component Criteria:Add	APP_COMP_ CRITERIA_ADD	Add an application component criteria
Device Class License:View	SYS_DEVICE_ CLASS_LICENSE_ VIEW	View device class license data
Customer Select Objects:Asset Add/Edit/Delete	ASSET_CUSTOM_ FORM_EDIT	Add/edit/delete the Custom Select Object of application type 'Asset'
Host File: Remove	SYS_HOST_FILE_ REM	Remove a host file entry
Business Service Thresholds:Create	BIZ_SVC_ALERT_ CREATE	Create a threshold for Business Services, IT Services, and Device Services
MIB:Export	SYS_MIB_EXPORT	Export an MIB compilation
Registry>Schedules>Schedule Manager:Administration	SYS_SCHEDULE_ MGMT	Delete and edit schedules
System>Customize>ScienceLogic Libraries	SYS_SILOLIB_REG_ PAGE	Access the Library registry page
SmartView:Edit	SMARTVIEW_EDIT	Edit a SmartView
UserGroup:Delete	USER_GROUP_ DELETE	Delete a user group
System>Customize>Device Categories	SYS_CUSTOM_ DEV_CAT_PAGE	Access the Device Category Customization page
Application Component Criteria Admin:Remove	APP_COMP_ CRITERIA_ADMIN_ REMOVE	Remove an Application Component Criteria as an Administrator
System>Manage>Discovery	SYS_DISCOVERY_ PAGE	Access the Discovery page
System>Customize>IPMI Sensor Defs	SYS_IPMI_SENSOR_ DEFS	IPMI Sensor Definitions page
Business Services Thresholds:View	BIZ_SVC_ALERT_ VIEW	View thresholds for Business Services, IT Services, and Device Services

System>Monitor>Collector Status	SYS_MONITOR_ CUG_STATUS_ PAGE	Access the Collector Status page
System>Settings>Assets	SYS_SETTINGS_ ASSET_OPTS_PAGE	Access the Asset Options Settings page
Subscription Data:Edit	SYS_SUBSCR_ DATA_EDIT	Update subscription license user data
Package:View	PKG_VIEW	View package properties
Key Manager	SYS_ACCESS_ CONTROL_KEY_ MANAGER	Access the Key Manager tool for creating access keys and aligning them with access control hooks.
Select Object: Edit/Add/Mod	SYS_CUSTOM_ FORM_EDIT	Prerequisite check to edit entries on the Select Objects page (System>Customize>Select Objects)
Application Component Criteria:Remove	APP_COMP_ CRITERIA_REMOVE	Remove an Application Component criteria
Discovery:View	SYS_DISCOVERY_ VIEW	View an existing discovery session
System>Customize>IPMI Sensor Types	SYS_IPMI_SENSOR_ TYPES	IPMI Sensor Type definitions
User:Edit:Lockouts	SYS_LOCKOUTS_ EDIT	Manage user lockouts
Business Service Template:Remove	BIZ_SVC_ TEMPLATE_ REMOVE	Remove a template for Business Services, IT Services, and Device Services
System>Monitor>System Processes	SYS_MONITOR_ PROCESSES_PAGE	Access the System Processes page
System>Settings>Authentication> CAC/ClientCert Auth	SYS_SETTING_ CAC_PAGE	Access the CAC Configuration page
System>Tools>Cache Management	SYS_TOOLS_ CACHE_MGMT	Access the classic user interface (EM7)Admin Portal Cache Manager
PowerPack:Edit	PPACK_EDIT	Edit PowerPack contents and properties
Scheduler:Add	SCH_ADD	Add a new schedule
System>Settings>Authentication> Multi-Factor	SYS_AUTH_ MULTIFACTOR_ PAGE	Access the Multi-factor Resources registry page
Appliances:Delete	APPLIANCE_ REMOVE	Delete an existing appliance

System>Customize>TCP-IP Ports	SYS_CUSTOM_ PORT_REG_PAGE	Access the TCP-IP Port Customization page
System>Settings>API	SYS_SETTINGS_ API_PAGE	Access the classic user interface (EM7) API Configuration page
System>Settings>Authentication> SSL Certificates	SYS_SSL_CERTS_ PAGE	Access the SSL Certificate manager
PowerPack:Delete	PPACK_DELETE	Delete a PowerPack
Customer Select Objects:User Account Add/Edit/Delete	ACT_CUSTOM_ FORM_EDIT	Add/edit/delete the Custom Select Objects of application type 'User Account'
Registry>Schedules>Schedule Manager: View	SCHEDULE_MNGR_ PAGE	View the Schedule Manager page
Application Thresholds:Add	APP_COMP_ALERT_ ADD	Add a threshold for applications and application components
System>Tools>API Browser	SYS_API_ BROWSWER_PAGE	Access the API Browser page
Application Template: Remove	APP_COMP_ TEMPLATE_ REMOVE	Remove templates for applications and application components
System>Customize>MAC Vendors	SYS_CUSTOM_ MAC_VENDOR_ REG_PAGE	Access the MAC Vendors registry page
DynamicApplication:Edit	DYN_APP_EDIT	Edit an existing Dynamic Application using the current user interface and GQL
Collector:generate DATABASE_ INITIATED token	COLLECTOR_ DATABASE_ INITIATED	Generate a token to onboard a traditional collector
System>Monitor>Unhandled Exceptions	SYS_MONITOR_ EXCEPTIONS_PAGE	Access the page for monitoring unhandled exception logs
Collector Groups:Edit	CUG_EDIT	Edit an existing collector group
System>Settings>Behavior	SYS_SETTINGS_ BEHAVIOR_PAGE	Access the classic user interface (EM7) Behavior Settings page
Icon:Add	ICON_ADD	Add an icon
System>	SYS_SYSTEM_ PAGE	Prerequisite check for System>* pages (needed in addition to page-specific hooks)

System>Tools>Guide Browser	SYS_TOOLS_ GUIDE_BROWSER_ PAGE	Access the Guide Browser page
Scheduler:Delete	SCH_REMOVE	Delete an existing schedule
Application Thresholds:View	APP_COMP_ALERT_ VIEW	View thresholds for applications and application components
System>Settings>Authentication> Resources	SYS_AUTH_ RESOURCE_PAGE	Access the Authentication Resources registry page
Admin Portal Access	AP_ACCESS	Prerequisite for direct access to the Admin Portal
Per-Hostname Themes:Edit	SYS_CUSTOM_ THEMES_DNS_EDIT	Add, remove, or edit definitions to choose which theme is presented to any given hostname
Finder	SYS_FINDER	Access the Finder tool
Log File Monitoring Policies:Add	SYS_LOG_FILE_ MON_POLICIES_ ADD	Add a Log File Monitoring policy
System>Monitor>System Logs	SYS_MONITOR_ SYS_LOGS_PAGE	Access the System Logs page
System>Settings>Data Retention	SYS_SETTINGS_ DATA_RETENTION_ PAGE	Access the Data Retention Settings page
Customer Select Objects:IP Address Add/Edit/Delete	IP_CUSTOM_FORM_ EDIT	Add/edit/delete the Custom Select Objects of application type 'IP Address'
Customer Select Objects: Organization Add/Edit/Delete	ORG_CUSTOM_ FORM_EDIT	Add/edit/delete the Custom Select Objects of application type 'Organization'
Registry>Run Book>Schedules	RBK_SCHEDULE_ REG_PAGE	Access the Run Book Schedules registry page
Execution Environment:Manage	SILOENV_EDIT	Create environments and align libraries
Application Component Criteria Admin:Edit	APP_COMP_ CRITERIA_ADMIN_ EDIT	Edit an application component criteria as an Administrator
System>Customize>Uptime OIDs	SYS_CUSTOM_ UPTIMEOID_PAGE	Access the Uptime OID list editor
Host File:Edit	SYS_HOST_FILE_ EDIT	Write access to host file entries, not including add/remove

Log File Monitoring Policies:Remove	SYS_LOG_FILE_ MON_POLICIES_ REMOVE	Remove a Log File Monitoring policy
System>Tools>OID Browser	SYS_OID_ BROWSER_PAGE	Access the OID Browser
System>Settings>Appliances	SYS_SETTINGS_ LICENSE_PAGE	Access the classic user interface (EM7) Appliance page
SmartView:Create	SMARTVIEW_ CREATE	Create a SmartView
Application Component Criteria:Edit	APP_COMP_ CRITERIA_EDIT	Edit an application component criteria
System>Customize>Ports	SYS_CUSTOMIZE_ PORTS_VIEW	Access the TCP-IP Port Customization page
Discovery:Add	SYS_DISCOVERY_ ADD	Add a new discovery session
Business Service Thresholds:Edit	BIZ_SVC_ALERT_ EDIT	Edit thresholds for Business Services, IT Services, and Device Services
Host File:View	SYS_HOST_FILE_ VIEW	Read access to host file entries
Compile MIB	SYS_MIB_COMPILE	Execute MIB compilation
Misc>Regular Expression Tester:View	MISC_REGEX_ TESTER_VIEW	View the Regular Expression Tester
System>customize>Presentation Labels	SYS_ PRESENTATION_ LABELS_REG_PAGE	Access to manage Presentation Labels
System>Settings>Processes	SYS_SETTINGS_ PROCS_PAGE	Access the System Process Settings page
Appliances:Edit	APPLIANCE_EDIT	Edit an existing appliance
SSL Certs:Add/Rem	SSL_CERT_ ADDREM	Add or remove SSL certificates
System>Custom>Device Classes	SYS_CUSTOM_ DEV_CLASS_PAGE	Access the Device Class Customization page
Discovery:Delete	SYS_DISCOVERY_ REM	Delete an existing discovery session
System>Monitor>Access Logs	SYS_MONITOR_ ACCESS_PAGE	Access the Access Logs Page
Ticket:Pager(email)	SYS_SEND_EMAIL	Access the Ticket Pager and send email

SNMP Trap: Push Configuration	SYS_SNMP_TRAP_ CONFIG_PUSH	Push the SNMP V3 trap configuration to Collector appliances
Business Service Template: Edit	BIZ_SVC_ TEMPLATE_EDIT	Edit templates for Business Services, IT Services, and Device Services
System>Manage>Access Keys	SYS_ACCESS_ CONTROL_KEY_ PAGE	Access the Access Key registry page
Collector Groups:Add	CUG_ADD	Add a new collector group
System>Customize>Interfaces	SYS_CUSTOM_IF_ REG_PAGE	Access Interfaces Customization page
System>Customize>Document Templates	SYS_DOC_ TEMPLATE_REG_ PAGE	Access the Document Templates registry page
System>Customize>IPMI Sensor Type:ADDREM	SYS_IPMI_SENSOR_ TYPE_ADDREM	Add/remove IPMI Sensor Types
System>Monitor>Event Overview	SYS_MONITOR_ EVENT_PERF_PAGE	Access the Event Overview page
System>Settings>Backup	SYS_SETTINGS_ BACKUP_PAGE	Access the classic user interface (EM7) Backup Configuration page
Application Template:Edit	APP_COMP_ TEMPLATE_EDIT	Edit templates for applications and application components
Subscription Data:View	SUS_SUBSCR_ DATA_VIEW	View subscription license usage data
PowerPack:Create	PPACK_CREATE	Create a new PowerPack
Dynamic Appication:Add	DYN_APP_ADD	Add a new Dynamic Application using the current user interface/GQL
Collector:generate NO_VERIFY token	COLLECTOR _ AUTO_CONNECT	Generate a token to onboard a phone home collector via an automatically accepted connection request
Scheduler:Edit	SCH_EDIT	Edit an existing schedule
System>Settings>Authentication> Profiles	SYS_AUTH_ PROFILE_PAGE	Access the Authentication Profiles registry page
Collector Groups:View	CUG_VIEW	View an existing collector group
Icon:Remove	ICON_REMOVE	Remove an icon
System>Customize>Select Objects	SYS_CUSTOM_ SELECT_OBJ_PAGE	Access the Custom Select Objects page

System>Manage>Applications	SYS_DYN_APP_ MANAGEMENT	Access the Dynamic Applications registry page in the classic user interface
Users:View:Lockouts	SYS_LOCKOUTS_ VIEW	Manage user lockouts
System>Monitor>Event Statistics	SYS_MONITOR_ SYSLOG_ PERF>PAGE	Access the Event Statistics page for per-collector statistics
Application Thresholds:Remove	APP_COMP_ALERT_ REMOVE	Remove a threshold for applications and application components
System>Settings>Collector Groups	SYS_SETTINGS_ CUGS PAGE	Access the Collector Group Management page
System>Tools>DBTool	SYS_TOOLS_DB	Access DB Tool page
PowerPack:Import	PPACK_IMPORT	Import/upload a PowerPack
Dynamic Application:View	DYN_APP_VIEW	View an existing Dynamic Application using the current user interface/GQL
Setup and Config	SETUP_CONFIG_ PAGE	Access the Setup and Config page
System>Manage>Collection Labels	SYS_COLLECT_ LABEL_PAGE	Access the Collection Label Management page
Workspace	WORKSPACE_PAGE	Access the Workspace page
System_Customize>Themes	SYS_CUSTOM_ THEMES_ REG_PAGE	Access the classic user interface (EM7) theme/brand editor
Host File:Add	SYS_HOST_FILE_ ADD	Add a host file entry
System>Manage>Log File Monitoring Policies	SYS_LOG_FILE_ MON_ POLICIES_PAGE	View the Log File Monitoring Policies registry page
System>Customize>Tabs	SYS_NAV_TABS_ PAGE	Access the Tab Customization page
Application Component Criteria Admin:Add	APP_COMP_ CRITERIA_ ADMIN_ADD	Add an application component criteria as an Administrator
System>Settings>EULA	SYS_SETTINGS_ EULA_PAGE	Access the classic user interface (EM7) EULA page

User:Manage Sessions	SYS_USER_ SESSIONS_ MANAGE	Delete/log-out user sessions
Ports:Add/Rem	SYS_CUSTOMIZE_ PORTS _ADDREM	Alter port configuration within System>Customize>TCP-IP Ports
Misc>Skylar One License Info: View	MISC_LICENSE-VIEW	View the Skylar One License information
Registry>Run Book>Actions>Snippets	RBK_ACTIONS_ SNIPPET	Access Snippet Code in the Action Editor

Events

Name	Access Hook ID	Description
Event Insights:View	EVT_INSIGHTS_VIEW	View Event Insights
Event:Resolution Rating:View	EVT_RESOL_RATE_ VIEW	View event resolution rating
Event:Acknowledge	EVT_ACK	Acknowledge an event
Event Note:Add/Rem	EVT_NOTE_ADDREM	Add or remove an event note
Event:Statistics	EVT_STATISTICS	View the event statistics graph from the Event Console
Event Category:Edit	EVT_CATEGORY_ EDIT	Edit an event category
Event:Edit	EVT_POLICY_EDIT	Edit an event policy
Event:Suppression:View	EVT_SUPPRESSION_ VIEW	View event suppression definitions in the Event Policy Editor
Event Category:View	EVT_CATEGORY_ VIEW	View an event category
Registry>Events>Predictive Alerting	EVT_PREDICTIVE_ ALERTING_REG_ PAGE	Access the Predictive Alerting registry page
Registry>Events>SNMP Trap Filters	EVT_TRAP_FILTERS_ REG_PAGES	Access the Trap Filters registry page
Registry>Events>Inbound Email	EVT_INBOUND_ EMAIL_REG_PAGE	Access the Event Emailer redirection page

Event:Resolution:Edit	EVT_RESOLUTION_ EDIT	Update event resolution properties
Event Insights Event Metrics:View	EVT_INSIGHTS_ EVENT_METRICS_ VIEW	View Event metrics
Event:Resolution Rating:Edit	EVT_RESOL_RATE_ EDIT	Update event resolution rating properties
Registry>Events>Event Manager	EVT_MANAGER_ REG_PAGE	Access the Event Policy definitions registry page
Registry>Events>RSS Feeds	EVT_RSS_REG_ PAGE	Access the Events RSS Feeds registry page
Event Category:Add	EVT_CATEGORY _ ADD	Add an event category
Event: Add/Rem	EVT_POLICY_ ADDREM	Add/ remove an Event Policy
Registry>Events>Supressions	EVT_SUPPRESSION_ REG_PAGE	Access the Event Suppressions registry page
Event Category:Rem	EVT_CATEGORY_ REM	Delete an event category
Event:Predictive Alerting Policy:Add	EVT_PREDICTIVE_ ALERTING_ADD	Add predictive alerting policies
Event:SNMP Trap Filters:Edit	EVT_TRAP_FILTERS_ EDIT	Edit SNMP Trap Filter definitions
Event:View (from Dev Properties)	EVT_DEV_VIEW	View events related to a given device from the Device Properties page
Event:Resolution:Add/Rem	EVT_RESOLUTION_ ADDREM	Add/remove an event resolution
Event Insights Device Metrics: View	EVT_INSIGHTS_ DEVICE_METRICS_ VIEW	View Device metrics
Event:Resoultion Rating:Add/Rem	EVT_RESOL_RATE_ ADDREM	Add/remove an event resolution rating
Event:Kiosk	EVT_KIOSK	View the Event Kiosk
Event:Reacknowledge	EVT_RE_ACK	Reacknowledge an event
Event:User Initiated Run Book Automation	EVT_AUTOMATION_ USER_INITIATED	Execute a user-initiated Run Book Automation
Event:View (From Org Page)	EVT_ORG_VIEW	View events related to a given organization from the Organization Properties page

Event:Suppressions:Add/Rem	EVT_SUPPRESSION_ADDREM	Add/remove event suppression definitions
Registry>Events>Categories	EVT_CATEGORY_REG_PAGE	Access event categories definitions from the registry page
Event:View	EVT_POLICY_VIEW	View an event policy
Event:SNMP Trap Filters:Add/Rem	EVT_TRAP_FILTERS_ADDREM	Add/remove SNMP Trap filters
Event:Clear	EVT_CLEAR	Clear an event
Event:Predictive Alerting Policy:Rem	EVT_PREDICTIVE_ALERTING_REM	Remove Predictive Alerting policies
Events/Event:View	EVT_VIEW	Basic event access which includes the Event console
Event Insights Alert Metrics:View	EVT_INSIGHTS_ALERT_METRICS_VIEW	View Alert metrics
Event:Resolution:View	EVT_RESOLUTION_VIEW	View Event resolution

Global Manager

Name	Access Hook ID	Description
Global Manager Stack:Add	GM_STACK_ADD	Add Global Manager stacks
Global Manager Stack:View	GM_STACK_VIEW	View Global Manager stacks
Global Manager Stack:Remove	GM_STACK_REMOVE	Remove Global Manager stacks
Global Manager Stack:Edit	GM_STACK_EDIT	Edit Global Manager stacks

Guides

Name	Access Hook ID	Description

Guides:Search	GDE_SEARCH	Access to search feature within Guides **NOTE:** As of version 8.12.2, ScienceLogic no longer updates the help that appears when you click the **[Guide]** button that appears in the classic user interface. Instead, ScienceLogic recommends clicking the **[Help]** button that appears at the top of each page in the default Skylar One user interface to open a Help topic about that page within Skylar One.

IP/Network

Name	Access Hook ID	Description
Registry>Networks>IPv4 Networks	IP_NETWORKS_ REG_PAGE	Access IPv4 Networks registry page
Networks:Ports:Edit	IP_PORTS_EDIT	Perform bulk operations on Registry>Networks>IP Ports page
Registry>Networks>Virtual Interfaces	IP_VIF_REG_PAGE	Access the VIF registry page
Networks:Interfaces:Add/Mod (not used)	IP_INTERFACES_ ADDMOD	Placeholder hook for future use
Networks:Interfaces:Remove	IP_INTERFACES_ REM	Remove network interfaces
Networks:IPv4:Edit	IP_NETWORKS_EDIT	Edit an IPv4 network
Registry>Networks>Quality of Service	IP_QOS_REG_PAGE	Access the Quality of Service registry page
Networks:Interfaces:Add	IP_INTERFACES_ ADD	Add network interfaces
Registry>Networks>Interfaces	IP_INTERFACES_ REG_PAGE	Access the Network Interfaces registry page
Networks:IPv4:Add/Rem	IP_NETWORKS_ ADDREM	Add or remove an IPv4 network
Networks:IPv4:View	IP_NETWORKS_ VIEW	View/browse an IPv4 network
Registry>Networks>IP Ports	IP_PORTS_REG_ PAGE	Access the IP Ports registry page
Networks:Interfaces:Edit	IP_INTERFACES_ EDIT	Edit the properties of an interface

IT Services

Name	Access Hook ID	Description
IT Service Dashboard:Edit	ITS_DASHBOARD_EDIT	Edit IT Service dashboards
Registry>IT Services>IT Service Manager	ITS_SERVICE_REG_PAGE	Access the IT Service Manager registry page
SLA Definition:Edit	ITS_SLA_EDIT	Edit SLA definitions
IT Service Dashboard:Add/Rem	ITS_DASHBOARD_ADDREM	Add or remove IT Service dashbords
IT Service:Edit	ITS_SERVICE_EDIT	Edit IT Service definitions
SLA Definiton:Add/Rem	ITS_SLA_ADDREM	Add or remove SLA definitions
Registry>IT Services>IT Service Dashboards	ITS_DASHBOARD_REG_PAGE	Access the IT Service Dashboard registry page
IT Service:Add/Rem	ITS_SERVICE_ADDREM	Add or remove IT Service definitions
IT Service:View	ITS_SERVICE_VIEW	View IT Service details
Registry>IT Services>SLA Definitions	ITS_SLA_REG_PAGE	Access the SLA definitions registry page

Machine Learning

Name	Access Hook ID	Description
Machine Learning:Create	ML_CREATE	Create a machine learning
Machine Learning:View	ML_VIEW	View a machine learning
Machine Learning:Delete	ML_DELETE	Delete a machine learning
Machine Learning:Edit	ML_EDIT	Edit a machine learning

Monitors

Name	Access Hook ID	Description
Monitors:View	MON_VIEW	View a monitor policy
Monitor:Add/Rem	MON_ADDREM	Add/remove a monitoring policy
Registry>Monitors>Windows Services	MON_WIN_ SERVICES_REG_ PAGE	Access the Windows Service Monitors policy registry page
Registry>Monitors>Email Round-Trip	MON_EMAIL_RT_ REG_PAGE	Access the Email Round-Trip Monitors policy registry page
Registry>Monitors>Logs	MON_LOG_FILE_ REG_PAGE	Access the Log File Monitors policy registry page
Registry>Monitors>TCP-IP Ports	MON_PORTS_REG_ PAGE	Access the TCP-IP Ports Monitors policy registry page
Registry>Monitors>System Processes	MON_SYS_PROCS_ REG_PAGE	Access the System Process Monitors policy registry page
Registry>Monitors>Web Content	MON_WEB_CV_ REG_PAGE	Access the Web CV Monitors policy registry page
Monitors:Edit	MON_EDIT	Edit a monitor policy
Log File:Edit	MON_LOG_FILE_ EDIT	Edit a Log File monitor
Log File:View	MON_LOG_FILE_ VIEW	View a Log File monitor
Registry>Monitors>SSL Certificates	MON_SSL_CERTS_ REG_PAGE	View the SSL Certificates Monitors page
Registry>Monitors>Webhooks	MON_WEBHOOK_ REG_PAGE	Access the Webhook Monitor registry page
Registry>Monitors>Domain Name	MON_DOMAIN_REG_ PAGE	Access the Domain Name Monitor registry page
Log File Monitor:Add	MON_LOG_FILE_ ADD	Add a Log File Monitor
Log File Monitor:Remove	MON_LOG_FILE_ REM	Remove a Log File Monitor
Registry>Monitors>SOAP-XML	MON_SOAP_REG_ PAGE	Access the SOAP-XML Monitor registry page

Organizations

Name	Access Hook ID	Description
Org:View	ORG_VIEW	View the properties of an organization of which the user is a member
Org:Logs:Clear	ORG_CLEAR_LOGS	Clear logs for an organization of which the user is a member
Org:Logs:View	ORG_LOGS_VIEW	View the logs of an organization
Org:Notes:View	ORG_NOTE_VIEW	View the notes of an organization
Org:View Summary	ORG_SUMMARY_ VIEW	View the Summary information of an organization
Org:AltLocations:Edit	ORG_ALT_ LOCATIONS_EDIT	Edit the alternate locations of an organization
Org:Edit	ORG_EDIT	Edit the properties of an organization
Org:Notes:Edit	ORG_NOTE_EDIT	Edit notes for an organization
Registry>Accounts>Organizations	ORG_REG_PAGE	Access the Organizations registry page
Org:AddRem	ORG_ADDREM	Create new organizations or delete organizations of which the user is a member
Org:Notes:Add/Rem	ORG_NOTE_ ADDREM	Add/remove notes for an organization
Org:Print Report	ORG_PRINT_ REPORT	Generate a printable report of organizations from the registry page

Platform Administration

Name	Access Hook ID	Description
Settings Processes: Edit	PLAT_SETTINGS_ PROCS_EDIT	Edit an existing process
Settings Email: Edit	PLAT_SETTINGS_ EMAIL_EDIT	Edit an existing field in the Email Settings page
System>Tools>DB Tool	SYS_TOOLS_DB	Access DB Tool page
System>Settings>Backup	SYS_SETTINGS_ BACKUP_PAGE	Access the EM7 Backup Configuration page

Reports

Name	Access Hook ID	Description
Reports>Create Report>Quick Report	RPRT_QUICK_REP_ PAGE	View the Quick Reports page and execute reports
Reports>Management>Report Output Styles	RPRT_TEMPLATE_ STYLE_REG_PAGE	Access the Report Output Styles registry page
Reports:Jobs:Add/Rem	RPRT_JOBS_ ADDREM	Add or remove Report Jobs
Reports>Create Report>Archived Reports	RPRT_JOBS_ ARCHIVE_REG_PAGE	Access the Archived Reports registry page
Reports:Jobs:Run As Any User	RPRT_JOBS_ RUNASANY	Schedule a report job to run with the permissions of any user
Reports>Management>Report Manager	RPRT_MANAGER_ REG_PAGE	View the Report Manager registry page
Reports:Archive:Delete	RPRT_JOBS_ ARCHIVE_ADDREM	Delete archived reports, removing them from classic user interface (EM7) user inboxes
Reports:Jobs:Edit	RPRT_JOBS_EDIT	Edit report jobs
Reports:Jobs:Run As Org User	RPRT_JOBS_ RUNASORG	Schedule a report job to run with the permissions of any user within your organization
Reports>Management>Report Output Media	RPRT_MEDIA_REG_ PAGE	Access the Report Output Media registry page
Report Output Format:PDF	RPRT_PDF_FORMAT	PDF report output form access check
Reports>Management>Report Output Templates	RPRT_TEMPLATE_ REG_PAGE	Access the Report Output Templates registry page
Reports>Management>Input Forms	RPRT_INPUT_FORM_ REG_PAGE	Access the Report Input Forms registry page
Reports:Archive:Prune Archived	RPRT_JOBS_ ARCHIVE_PRUNE	Delete archived reports that are not in any classic user interface (EM7) user's inbox
Report Output Format:XLSX	RPRT_XLSX_FORMAT	XLSX report output format access check
Reports>Create Report>Report Jobs	RPRT_JOBS_REG_ PAGE	Access the Report Jobs registry page

Reports>Leaderboards	RPRT_ LEADERBOARDS_ PAGE	Access to the assorted Leaderboards reports
Reports Output Format:ODS	RPRT_ODS_FORMAT	ODS report output format access check
Reports Output Format: HTML	RPRT_HTML_ FORMAT	HTML report output format access check
Reports:Scheduler	RPRT_SCHEDULER_ PAGE	View and edit report schedules
Reports>	RPRT_VIEW	Prerequisite check for all Reports>* pages

RSS Feed

Name	Access Hook ID	Description
RSS:Add/Rem	RSS_FEED_ADDREM	Add or remove an RSS feed (currently Events only)
RSS:Edit	RSS_FEED_EDIT	Edit an RSS feed (currently Events only)

Run Book

Name	Access Hook ID	Description
Automation Engine Settings:View	RBK_SETTINGS_VIEW	View Automation Engine settings
Registry>Run Book>Action Types	RBK_ACTIONS_ TYPES_REG_PAGE	Access the Run Book Actions Types registry page
Automation Engine Settings:Edit	RBK_SETTINGS_EDIT	Edit Automation Engine settings
Registry>Run Book>Actions	RBK_ACTIONS_REG_ PAGE	Access the Run Book Actions registry page
Registry>Run Book>Automations	RBK_AUTOMATION_ REG_PAGE	Access the Run Book Automations registry page

Ticketing

Name	Access Hook ID	Description

Ticket: All Queue Members	TKT_ACESS_ALL_ QUEUE_MEMBERS	Access all members in a ticket queue regardless of organization
Ticket:Customize Forms	TKT_CUSTOM_ FORM_EDIT	Edit custom fields for tickets
Ticket: Scheduler	TKT_SCHEDULER	View and edit automated ticket schedules
Ticket:Assign within Queue	TKT_ASSIGN_IN_ QUEUE	Assign a ticket to another user within the same queues
Ticket:Element Alignment	TKT_ELEMENT_ ALIGN	Edit a ticket element alignment
Ticketing:States:Edit	TKT_STATE_EDIT	Edit Ticket States (workflow rules)
Ticket:Change Severity	TKT_CHANGE_ SEVERITY	Alter the severity of a ticket to which a user has edit access
Registry>Ticketing>Escalations	TKT_ESCALATION_ REG_PAGE	Access the Ticket Escalations registry page
Registry>Ticketing>Templates	TKT_TEMPLATES_ REG_PAGE	Access the Ticket Template registry page
Ticket:Notes:Add	TKT_COMMENT_ ADD	Add a new note to a ticket
Ticket:View Logs	TKT_LOGS_VIEW	View ticket logs
Ticket:View Any	TKT_VIEW_ANY	Grant view access to any ticket (redundant-see 'Ticket:Access All Queues'
Ticket:Access All Queues	TKT_ACCESS_ALL_ QUEUES	Grant read access to all ticket queues
Ticket:Notes:Attachments: Blacklist:Edit/Add/Rem	TKT_COMMENT_ MEDIA_BLACKLIST_ EDIT	Add, remove, or edit a ticket attachment blacklist rule
Registry>Ticketing>Queues	TKT_QUEUES_REG_ PAGE	Access the Ticketing Queues registry page
Ticket:Watchers:Add/Rem	TKT_WATCHERS_ ADDREM	Add or remove ticket watchers
Ticket:All in queues	TKT_ACCESS_ QUEUES	Access all tickets within member queues
Ticket:Alignment	TKT_ALIGN_ PARENTS	Set ticket parent/child relationships
Ticket:Edit	TKT_EDIT	Edit a ticket to which a user has view access
Ticketing:States:Add/Rem	TKT_STATE_ ADDREM	Add or remove Custom Ticket states and set workflow rules

Ticket:Automation	TKT_AUTOMATION	View the Automation tab in the Ticket Editor
Ticket:Escalation:Edit	TKT_ESCALATION_ EDIT	Edit a ticket escalation policy
Ticket:Statistics:View	TKT_STATS_VIEW	View the ticket statistics summary from the Ticket console
Ticket:Notes:Cloaked:Edit	TKT_COMMENT_ CLOAKED_EDIT	Edit a cloaked note; allows removing a cloak from a note (also requires Ticket:Notes:Edit)
Ticket:History:View	TKT_HISTORY_VIEW	View a ticket's history
Ticket:View	TKT_VIEW	View access to tickets
Ticket:Access All	TKT_ACCESS_ALL	Circumvent organization/queue restrictions (must still have Ticket:View)
Ticket:Notes:Edits	TKT_COMMENT_ EDIT	Edit existing ticket notes
Ticket:Messaging	TKT_PAGER	Enable the ticket messenger (pager) in the ticket properties user interface
Ticket:Reports	TKT_REPORTS	Run/view ticket reports
Ticket:Inbox:Statistics	TKT_VIEW_ REPORTS	View ticket statistics from an inbox page
Ticket:All in Orgs	TKT_ACCESS_ORG	Access all tickets within member organizations
Ticket:Console:View	TKT_CONSOLE_ VIEW	Allows view access to a ticket console
Ticket:Queue:Edit	TKT_QUEUE_EDIT	Edit a ticket queue
Ticket:Events:Alignment	TKT_ALIGN_EVENTS	Set the event alignment for a ticket
Ticket:Delete	TKT_DELETE	Permanently delete tickets from the database (non_ITIL compliant)
Ticket:Charge Back Services	TKT_SERVICE_ ADDREM	Add charge-backs to a ticket

User Account Management

Name	Access Hook ID	Description
External Contact:View	ACT_EMAIL_SUB_ VIEW	View an external contact's information

Vendor:Add/Rem	ACT_VENDOR_ ADDREM	Add or remove a vendor account
Preferences>Account>Preferences	ACT_MY_ PREFERENCES_ PAGE	Access the My Preferences page (can be accessed from the Toolbox without Preferences>hook)
Vendor:Notes	ACT_VENDOR_ NOTES_VIEW	View the Notepad tab on the vendor pop-up window
User:Edit (from Org pages)	ACT_ORG_USER_ EDIT	Edit a user from the Organization Properties page
User Policy:Add/Rem	ACT_USER_POLICY_ ADDREM	Add or remove a user policy
External Contact:Add/Rem	ACT_EMAIL_SUB_ ADDREM	Add or remove an external contact
User Policy:View	ACT_USER_POLICY_ VIEW	View a user policy
Registry>Accounts>External Contacts	ACT_EMAIL_SUB_ REG_PAGE	Access the External Contacts registry page
User:View	ACT_USER_VIEW	Grants read access to classic user interface (EM7) user accounts
Preferences>	ACT_MY_PAGE	Prerequisite check for all Preferences>* pages (required in additions to specific page rights)
Vendor:Edit Notes	ACT_VENDOR_ NOTES_EDIT	Grants write access to vendor notes
Preferences>Account>Schedule	ACT_MY_ SCHEDULE_PAGE	Acces the My Schedule page
Vendor:View	ACT_VENDOR_VIEW	Read access to vendor accounts
User:Edit	ACT_USER_EDIT	Grants write access to classic user interface (EM7) user accounts; does not include add/remove
Registry>Accounts>User Policies	ACT_USER_POLICY_ REG_PAGE	Access the User Policies registry page
External Contact: View (from Org Page)	ACT_EMAIL_SUB_ ORG_VIEW	View an Email Subscriber from the Organization Properties page
Registry>Accounts>User Accounts	ACT_USER_REG_ PAGE	Access the User Accounts registry page

Preferences>Account>Information	ACT_MY _INFO_ PAGE	Access My Info page
Vendor:Edit	ACT_VENDOR_EDIT	Grants write access for Vendor accounts; does not include add/remove
Preferences>Desktop Tools>RSS Feeds	ACT_MY_RSS_PAGE	Access the RSS Feeds pages
Registry>Accounts>Vendors	ACT_VENDOR_REG_ PAGE	Access the Vendors registry page
User:Add/Rem	ACT_USER_ ADDREM	Add or remove a classic user interface (EM7) user account
User Policy:Edit	ACT_USER_POLICY_ EDIT	Edit a user policy
External Contact:Edit	ACT_EMAIL_SUB_ EDIT	Edit an external contact
User:Print Report	ACT_USER_PRINT_ REPORT	Print a report for a given user

Views

Name	Access Hook ID	Description
Views:View Any	VIEWS_VIEW_ANY	Bypass shared restrictions and view any view
Views:Shared:Create	VIEWS_SHARED_ CREATE	Create shared views; share existing views
Views:View	VIEWS_VIEW	Grants read access to Views (prerequisite to Views:View Any)
Views:View Embedded	VIEWS_EMBEDDED	Access views embedded in other pages (e.g. Dashboards); implied by Views:View
Views:Shared:View	VIEWS_SHARED_ VIEW	Access a shared view
Views:Edit	VIEWS_EDIT	Edit a view
Views:Shared:Edit	VIEWS_SHARED_EDIT	Edit as shared view

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

International: +1-703-354-1010