System Administration

SL1 version 8.12.1

Table of Contents

Chapter 1

Introduction

Overview

This manual describes the tasks that System Administrators who monitor and maintain the health of SL1 must perform, and the tools they can use to perform those tasks.

This chapter includes the following topics:

Who Should Read This Manual?

This manual is intended for System Administrators who must monitor and maintain the health of SL1.

This manual describes tasks in the **[System]** tab that are related to maintenance and monitoring of SL1. This manual also includes advanced tasks that are performed at the console or in an SSH session.

What's In This Manual?

This manual includes information on global settings, collector groups, health tasks, maintenance tasks, and tools for troubleshooting and debugging.

Requirements

To follow some of the steps listed in this manual, you must have administrator-level access to the console of your SL1 appliances.

Chapter 2

Global Settings

Overview

In SL1, global settings allow you to define default behavior that applies to all elements in the platform. For settings that affect devices, these global settings can be overridden by applying device-level settings.

SL1 includes global settings for:

- *API*
- *SL1 appliances*
- *Asset Automation*
- *Logins, discovery, data collection, and expiration warnings*
- *Data retention*
- *Inbound email and outbound email*
- *Login Alert Messages*
- *Password Reset Emails*
- Thresholds for:
    - *System latency, file system usage, counter rollovers, availability, and component devices*
    - *Interfaces*
    - *Class-based quality of service (CBQoS)*

You can also define global settings for SL1 appliances, *system backups*, *collector groups*, *API behavior*, and *processes*.

These global settings allow system administrators to define and automate best practices and SOPs for SL1.

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

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

This chapter includes the following topics:

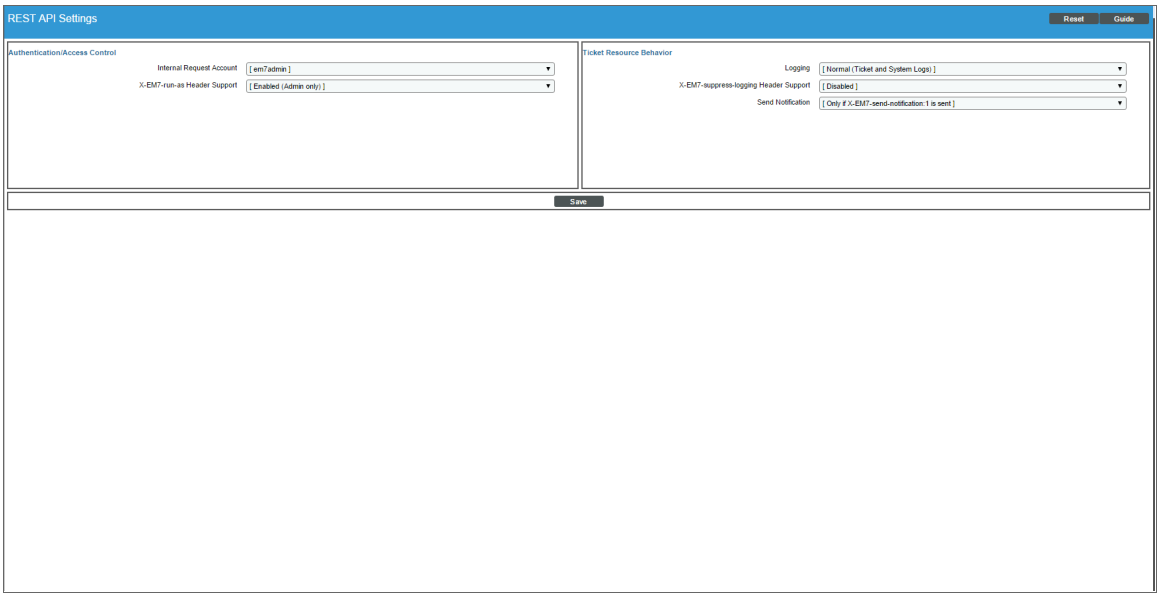
Global Settings for API

The **REST API Settings** page (System > Settings > API) allows you to define global parameters that affect the behavior of the REST API. When defined, these parameters affect all interaction with the API.

> **NOTE**: This page is available only to administrator users.

To edit the settings in the REST API Settings page:

1. Go to the **REST API Settings** page (System > Settings > API).



2. In the **REST API Settings** page, edit the values in one or more of the following fields:

   - ***Internal Request Account***. Specify the user account that allows SL1 to make API requests without a password. For details on building such an API request, see the ***ScienceLogic API*** manual.
   - ***X-EM7-run-as Header Support***. Specifies whether administrator users can make API requests using the permissions of another user without that user's password. Choices are:
     - *Disabled*. Administrator users cannot make API requests using the permissions of another user.
     - *Enabled (Admin only)*. Administrator users can include the X-EM7-run-as Header to make API requests using the permissions of another user. For details on using this header, see the ***ScienceLogic API*** manual.
   - ***Logging***. Specifies which logs SL1 will write to when tickets are created or updated using the API. Choices are:
     - *Transaction Logging Only (System Logs)*. If a ticket is created or updated using the API, SL1 will write the standard entry to the audit log that indicates a user performed a write-operation using the API. However, SL1 will not write to the ticket log for the ticket that was created or updated.
     - *Normal (Ticket and System Logs)*. If a ticket is created or updated using the API, SL1 will write to the audit log and to the ticket log for the ticket that was created or updated.
   - ***X-EM7-suppress-logging Header Support***. If *Normal (Ticket and System Logs)* is selected in the ***Logging*** field, this field specifies whether the X-EM7-suppress-logging header can be used when an administrator creates or updates a ticket using the API. If the X-EM7-suppress-logging header is used when creating or updating a ticket, SL1 will not write to the ticket log for the ticket that was created or updated. Choices are:

- *Disabled*. The X-EM7-suppress-logging header cannot be used.
- *Enabled (Admin only)*. The X-EM7-suppress-logging header can be used to stop SL1 from writing to the ticket log for the ticket that was created or updated.

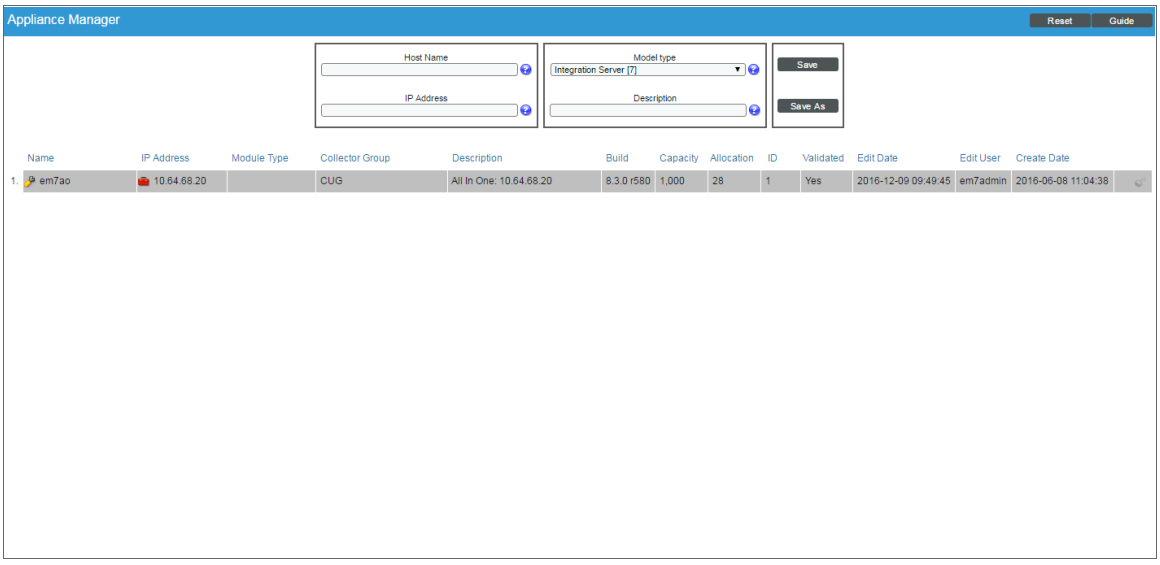
- ***Send Notification***. When a ticket is created or updated, SL1 can automatically send notification emails to the ticket assignee and ticket watchers. This option specifies the conditions under which SL1 will send notification emails when tickets are created or updated using the API. Choices are:
  - *Only if X-EM7-send-notification:1 is sent*. SL1 will send notification emails for a ticket only when the X-EM7-send-notification header is set to 1. For details on using this header, see the manual ***Using the ScienceLogic API***.
  - *Sent after every write operation*. SL1 will send notification emails for every API request that creates or updates a ticket.

3. Click the **[Save]** button to save changes in this page.

Global Settings for Appliances

The **Appliance Manager** page (System > Settings > Appliances) allows you to view information, including license status, about each ScienceLogic appliance in your system.

From the **Appliance Manager** page, you can also access the Web Configuration Utility for each ScienceLogic appliance by clicking the toolbox icon( ), or you can access the database administration tool for each Database Server or All-In-One Appliance by clicking the gear icon ( ).



To edit information about a ScienceLogic appliance:

1. Go to the **Appliance Manager** page (System > Settings > Appliances).
2. Locate the ScienceLogic appliance you want to edit. Click its wrench icon ().
3. The fields in the top pane are populated with values from the selected ScienceLogic appliance.
4. You can edit one or more of the following fields:

    - ***Host Name***. Name of the ScienceLogic appliance.
    - ***IP Address***. Primary IP address for the ScienceLogic appliance.

NOTE: For Data Collection Units that are part of a Phone Home configuration, ensure that the Primary IP address for the Data Collection Unit is its loopback IP.

    - ***Module Type***. This field is read-only. Possible values are:
        - *All In One*
        - *Database*
        - *Administration Portal*
        - *Data Collection Unit*
        - *Message Collection Unit*

NOTE: The combination appliance with a Database Server and an Administration Portal on a single appliance will appear with ***Module Type*** of *Database*. The combination appliance with a Message Collection Unit and a Data Collection Unit will appear with ***Module Type*** of *Data Collection Unit*.

    - ***Description***. Description of the ScienceLogic appliance.

5. Click the **[Save]** button to save any changes. Click the **[Save As]** button to save your changes to a new appliance name.

The Web Configuration Utility

The Web Configuration Utility allows you to configure system-level settings for your appliances. Each appliance includes access to the Web Configuration Utility.

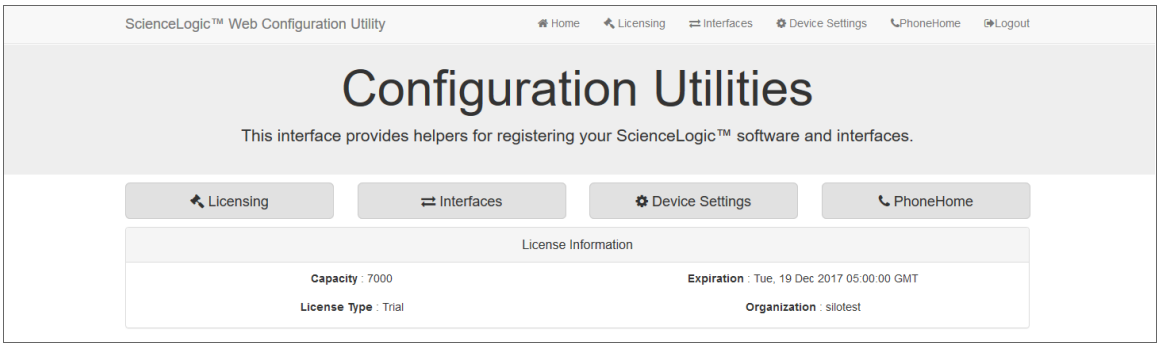
The Web Configuration Utility adds an additional layer of security to SL1 by segregating administrative functions from the rest of the user interface and by exposing system-level settings and diagnostic tools that might otherwise require command-line access to the appliance. The Web Configuration Utility can be accessed only through an HTTPS connection and requires its own administrator-level password.

Perform the following steps to log in to the Web Configuration Utility:

1. You can log in to the Web Configuration Utility using any web browser supported by SL1. The address of the Web Configuration Utility is in the following format:

https://*ip-address-of-appliance*:7700

2. Type the address of the Web Configuration Utility into the address bar of your browser, replacing "ip-address-of-appliance" with the IP address of the appliance.
3. You will be prompted to type your username and password. Log in as ***em7admin*** with the appropriate password. The default password is ***em7admin***. After logging in, the main **Configuration Utility** page appears:

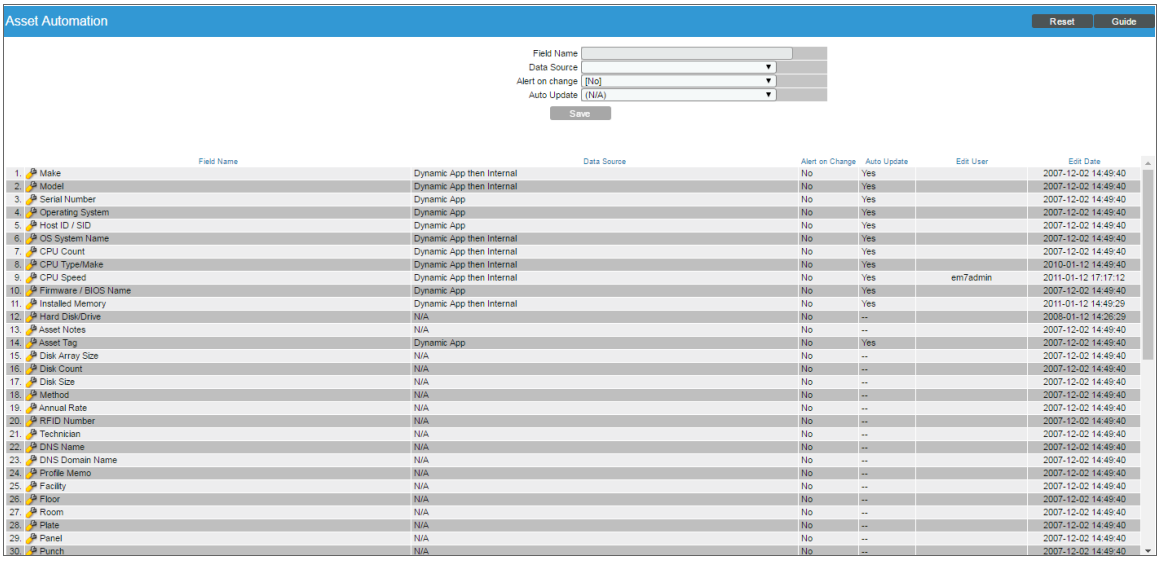


4. In the **Configuration Utility**, you can license a SL1 appliance, configure interfaces, and edit settings for the SL1 appliance and the Database Server if applicable.

    - For details on using the **Configuration Utility** to license a SL1 appliance, see the manual ***Installation and Initial Configuration***.
    - For details on using the the **Configuration Utility** to inform Data Collectors, Message Collectors, and Administration Portals when you change the IP address of a Database Server, see the section on *Changing IP Addresses*.

Global Settings for Asset Automation

The **Asset Automation** page (System > Settings > Assets) allows you to define the default behavior for all asset records.



For each standard asset field, you can specify:

- Whether the field can be automatically populated by SL1.
- Whether the field's value should be automatically updated by SL1.
- Whether or not SL1 should generate an event if the field's value changes.

You can define the default behavior for each standard field in the following asset pages:

- **Asset Properties**
- **Asset Maintenance & Service**
- **Asset Configuration**
- **Asset Licenses**
- **Asset IP Networks**
- **Asset Components**

The defined behavior will be applied to every asset record in SL1.

For more details on asset records and enabling automation for asset records, see the manual ***Asset Management and Vendors***.

Global Settings for User Logins, Discovery, Data Collection, UI Features, and Expiration Warnings

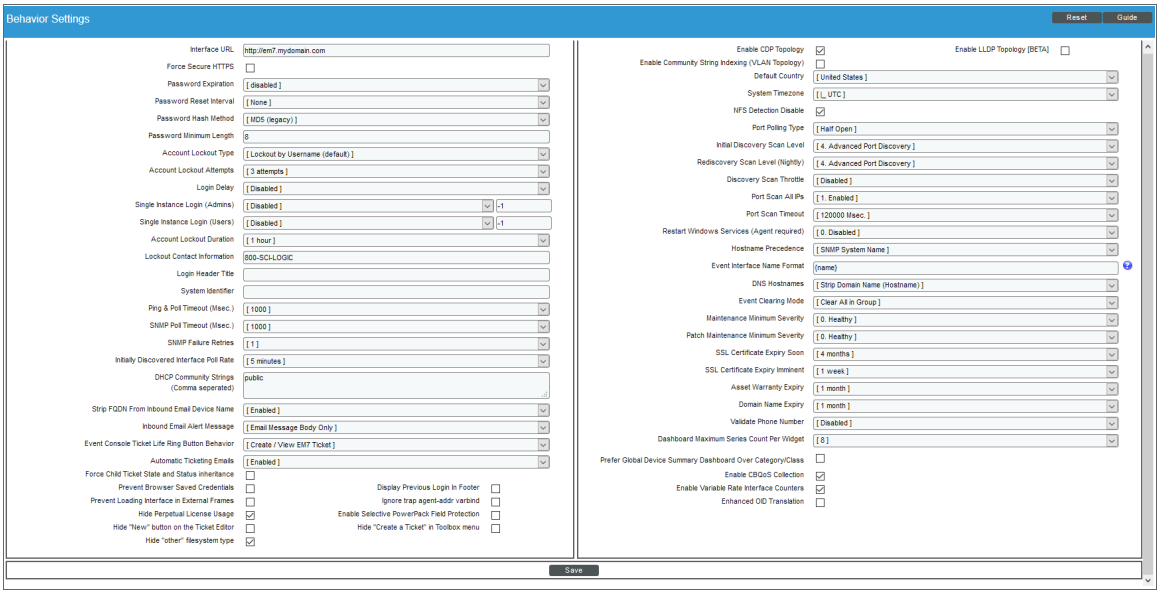
The **Behavior Settings** page (System > Settings > Behavior) allows you to define global parameters that affect:

- User Logins
- Discovery
- Data collection
- Settings that affect the display and behavior of the user interface
- Expiration warnings for asset warranties and SSL certificates

The parameters in the **Behavior Settings** page affect all pages, devices, and discovery functionality in SL1. For most settings, you can define a one-time, manual override in the affected page. You can also override many of these settings per device. For example, you can define global parameters for nightly discovery in this page, but in a device's **Device Properties** page (Devices> Device Manager > wrench icon), you can override these settings for a specific device.

To define or edit the settings in the **Behavior Settings** page:

1. Go to the **Behavior Settings** page (System > Settings > Behavior).
2. In the **Behavior Settings** page, edit the values in one or more of the following fields:



- ***Interface URL***. URL for accessing the user interface. This value should be in URL format and can be up to 64 characters in length.

NOTE: Do not include a trailing forward slash ("/") at the end of the Interface URL. When SL1 generates URLs for tickets or events (for example, in email messages), the trailing forward slash will be automatically included.

- ***Force Secure HTTPS***. If enabled, forces users to use HTTPS (secure HTTP) instead of HTTP when users connect to the user interface.
- ***Password Expiration***. Specifies whether or not the password for a user account will expire and if so, when the password will expire. Choices are:
  - *Disabled*. Passwords do not expire.
  - *30 Days*. Passwords will expire after 30 days.
  - *60 Days*. Passwords will expire after 60 days.
  - *90 Days*. Passwords will expire after 90 days.
  - *180 Days*. Passwords will expire after 180 days.
- ***Password Reset Interval***. The minimum amount of time that must pass before a user can change a password. For example, if the value in this field is *2 Hours*, a user can change a password every two hours. This applies to users changing their own passwords and administrators changing other users' passwords. Values range from 1 hour to 24 hours, in increments of one hour.
- ***Password Hash Method***. Specifies how user passwords will be encrypted for storage in the ScienceLogic database. You can choose the hashing algorithm that works best for your enterprise. Choices are:
  - *MD5 (Legacy)*
  - *SHA-512 (FIPS 140-2 Compliant)*
  - *Automatic (PHP Password API)*
- ***Password Minimum Length***. Specifies the minimum number of alphanumeric characters allowed for the password. You can specify any value from 1 to 99. The default value is "8" characters.
- ***Account Lockout Type***. If a user enters incorrect login information multiple times in a row, that user will be locked out of the user interface. In this field, you can select how the lockout will be applied. Choices are:
  - *Lockout by IP Address*. All login attempts from the IP address will be denied.
  - *Lockout by Username and IP Address*. All login attempts by the username from the IP address will be denied.
  - *Lockout by Username (default)*. All login attempts by the username will be denied.
  - *Disabled*. Lockouts are disabled.
- ***Account Lockout Attempts***. Number of times a user can enter incorrect login information before a lockout occurs. Choices are 1 time through 10 times.

- ***Login Delay***. To prevent unauthorized users from using brute-force login attempts, you can set a login delay in this field. After each failed login, SL1 will not allow another attempt for the number of seconds specified in this field. Choices are:
    - *Disabled*. SL1 does not enforce a delay between failed logins.
    - *1 Second*. After a failed login, SL1 will not allow another attempt for one second.
    - *2 seconds*. After a failed login, SL1 will not allow another attempt for two seconds.
    - *4 seconds*. After a failed login, SL1 will not allow another attempt for four seconds.
    - *8 seconds*. After a failed login, SL1 will not allow another attempt for eight seconds.
- ***Single Instance Login (Admins)***. Specifies whether more than one instance of a single username can be logged in to the user interface at the same time. Defines the default behavior for users of account type "Administrator". You can specify the following types of behavior:
    - *Disabled*. Multiple instances of the same account name can be logged in to the user interface. There are no requirements or limitations on any of the instances. None of the instances will be automatically logged out.
    - *Session can be transferred after*. If you select one of these options, the second instance of a user account can log in only after the first instance of the account is inactive. In SL1, an account is considered "inactive" if the user has not performed any tasks or navigated within the user interface. You can specify how long the first instance must be inactive before the second instance can log in. When the second instance successfully logs in to the user interface, the browser where the first instance is logged in will display the following message:

      "User id 'account name' logged in from a different browser and transferred this session."

NOTE: If this field is set to any value other than *disabled*, you can still override an earlier instance. If you try to log in to the user interface and there is another instance of the account already logged in to the user interface, the login page will display the following message: "User id 'account name' is already logged in to the system. To transfer the session, check 'Transfer Session' and log in."

    - If you select the ***Transfer Session*** checkbox, this logs the first instance out of the user interface and allows the second instance to log in to the user interface.

      The browser where the first instance was logged in will see the message:

      "User id 'account name' logged in from a different browser and transferred this session."

    - *Other (manual entry)*. Allows you to enter a custom value, in seconds. When the first instance of a user account is inactive in the user interface for the specified number of seconds, the first instance is logged out and the second instance is allowed

- ***Single Instance Login (Users)***. Specifies whether more than one instance of a single username can be logged in to the user interface at the same time. Defines the default behavior for users of account type "User". You can specify the following types of behavior:

  - *Disabled*. Multiple instances of the same account name can be logged in to the user interface. There are no requirements or limitations on any of the instances. None of the instances will be automatically logged out.
  - *Session can be transferred after*. If you select one of these options, the second instance of a user account can log in only after the first instance of the account is inactive. In SL1, an account is considered "inactive" if the user has not performed any tasks or navigated within the user interface. You can specify how long the first instance must be inactive before the second instance can log in. When the second instance successfully logs in to the user interface, the browser where the first instance is logged in will display the following message:

    "User id 'account name' logged in from a different browser and transferred this session."

NOTE: If this field is set to any value other than disabled, you can still override an earlier instance. If you try to log in to the user interface and there is another instance of the account already logged in to the user interface, the login page will display the following message: "User id 'account name' is already logged in to the system. To transfer the session, check 'Transfer Session' and log in."

  - If you select the ***Transfer Session*** checkbox, this logs the first instance out of the user interface and allows the second instance to log in to the user interface.

    The browser where the first instance was logged in will see the message:

    "User id 'account name' logged in from a different browser and transferred this session."

  - *Other (manual entry)*. Allows you to enter a custom value, in seconds. When the first instance of a user account is inactive in the user interface for the specified number of seconds, the first instance is logged out and the second instance is allowed.

- ***Account Lockout Duration***. Specifies how long a user will be locked out of the user interface. Choices are 1 hour – 24 hours, in one hour increments.
- ***Lockout Contact Information***. This contact information will be displayed when a user is locked out of the user interface. Can be any combination of alphanumeric characters, up to 255 characters in length. This information should allow the user to contact his/her administrator to unlock the account.
- ***Login Header Title***. HTML title of the login page. This text will appear at the very top of the browser on the login page.
- ***System Identifier***. Unique name for the current SL1 system. Can be up to 128 characters in length. This field is useful for companies or organizations with multiple SL1 systems. If a value is provided in this field, SL1 will include a "system identifier" value in each event generated by the current SL1 system. This allows users to easily determine the source SL1 system associated with the event.

- ***Ping & Poll Timeout (Msec.)***. This field specifies the number of milliseconds the discovery tool or availability polling will wait for a response after pinging a device. After the specified number of milliseconds have elapsed, the poll will timeout. The choices are between 100 and 5000 milliseconds.
- ***SNMP Poll Timeout (Msec.)***. This field specifies the number of milliseconds the discovery tool will wait for a response after sending an SNMP query to a device. After the specified number of milliseconds have elapsed, the SNMP poll will timeout. The choices are between 100 and 5000 milliseconds.
- ***SNMP Failure Retries***. This field specifies the number of times the discovery tool will try to communicate with a device after a timeout or failure. After that number of times has been met, the discovery tool will not retry unless the user manually restarts the discovery process. The choices are 0–6.
- ***Initially Discovered Interface Poll Rate.*** This field specifies the frequency with which SL1 will poll newly discovered interfaces. This setting does not affect interfaces that have been previously discovered with a different value in this field or interfaces for which the ***Frequency*** field has been manually edited in the Interface Properties page. Choices in this field are:
    - *1 min*. SL1 will poll the newly discovered interfaces every minute.
    - *5 mins*. SL1 will poll the newly discovered interfaces every five minutes. This is the default value for this field.
    - *10 mins*. SL1 will poll the newly discovered interfaces every 10 minutes.
    - *15 mins*. SL1 will poll the newly discovered interfaces every 15 minutes.
    - *30 mins*. SL1 will poll the newly discovered interfaces every 30 minutes.
    - *60 mins*. SL1 will poll the newly discovered interfaces every 60 minutes.
    - *120 mins*. SL1 will poll the newly discovered interfaces every 120 minutes.
- ***DHCP Community Strings (Comma separated)***. SNMP "read only" community string to use during discovery. This is required only if DHCP servers and devices use a different SNMP community string than other devices in the network. If the community string specified in the **Discovery Control Panel** page (System > Manage > Discovery) does not work for DHCP devices, SL1 will automatically use the community string specified in this field.
- ***Strip FQDN From Inbound Email Device Name***. In Events from Email policies, specifies how SL1 will match the regular expression for device name. Choices are:
    - *Enabled*. SL1 will search the text string in the incoming email and match all characters up to the first period that appears in the text string. If multiple devices match the characters up to the first period (for example, my_device.1 and my_device.2), SL1will align the event with the matching device with the highest Device ID.
    - *Disabled*. SL1 will search the text string in the incoming email for a match for the device name. The text string must include an exact match to the regular expression (defined in the Events from Email policy), including any text following a period in the device name. If SL1 does not find an exact match in the incoming email, SL1 creates an entry in the system log.

- ***Inbound Email Alert Message***. In each event policy, the ***First Match String*** and ***Second Match String*** fields specify the string or regular expression used to correlate the event with a log message. To trigger an event, the text of a log message must match the value in the ***First Match String*** and ***Second Match String*** fields in that event's policy. For Events from Email policies, this field specifies whether only the email message body will be written to the device log or whether both the email message subject and email message body will be written to the device log. Choices are:
  - *Email Message Body Only*. Only the email message body is written to the device log. The ***First Match String*** and ***Second Match String*** fields can examine and match only the email message body.
  - *Email Message Subject and Body*. Both the email message body and the email message subject are written to the device log. The ***First Match String*** and ***Second Match String*** fields can examine and match against both the email message body.

NOTE: The global setting ***Inbound Email Alert Message*** affects how events are triggered. This field does not affect the ***Regex Pattern*** field in the Event from Email policy. The ***Regex Pattern*** field in an Event from Email policy specifies which device log to write to.

- ***Event Console Ticket Life Ring Button Behavior***. Specifies how the life-ring icon ( ) in the **Event Console** will behave. Choices are:
  - *Create/View EM7 Ticket*. When you click the life-ring icon ( ) for an event in the **Event Console**, SL1 will display the **Ticket Editor** page, where you can define a ticket and automatically associate it with the selected event. This is the default behavior.
  - *Create/View External Ticket*. If an external ticket is aligned with an event, when you click the life-ring icon ( ) for that event (from the **Event Console**), SL1 spawns a new window and displays the external ticket (as specified in the ***force_ticket_uri*** field). If an external ticket is not yet aligned with an event, when you click the life-ring icon ( ) for that event, SL1 sets a "request" flag for the ticket and displays an acknowledgment that a new ticket has been requested. You can then use the "request" in run book logic, to create the ticket on the external system.

CAUTION: If you select *Create/View External Ticket* in the ***Event Console Ticket Life Ring Button Behavior*** field, you can no longer create tickets from the **Event Console**.

- ***Automatic Ticketing Emails***. Specifies whether ticket watchers will automatically receive email notification when a ticket is created or changes status. Choices are:
  - *Enabled*. This is the default value. When you select this option, SL1 automatically sends email notifications to all watchers when a ticket is created, assigned, or updated.
  - *Disabled*. When you select this option, SL1 does not automatically send email notifications to all watchers when a ticket is created, assigned, or updated.

- ***Prevent Browser Saved Credentials***. This checkbox specifies whether or not the user interface will allow the browser to cache login credentials and perform auto-complete in the login page. By default, the user interface will allow browsers to cache login credentials. Choices are:
  - *Selected*. The user interface will not allow browsers to cache credentials and use auto-complete in the login page. Use this setting to comply with PCI DSS and other security protocols.
  - *Not Selected*. This is the default setting. The user interface will allow browsers to cache credentials and use auto-complete in the login page. The implementation of this functionality varies between browsers.
- ***Prevent Loading Interface in External Frames***. If you select this checkbox, other pages cannot be loaded in external frames in the same browser session that includes SL1. This is a security measure, to prevent clickjacking attacks.
- ***Hide Perpetual License Count***. Specifies whether to display the device count graph in the **System Usage** page (System > Monitor > System Usage). The default behavior is to hide the graph in the **System Usage** page. Users might find this graph useful to troubleshoot licensing issues. For a description of the **System Usage** page, see the *Monitoring Overall System Usage and Statistics* section.
- ***Hide "New" button on the Ticket Editor***. If you select this checkbox, the **Ticket Editor** page will not display the **[New]** button. This field is unselected by default.
- ***Hide "other" filesystem types***. If you select this checkbox, file systems of type "other" (which includes XFS file systems) will not be discovered and monitored. This checkbox is selected by default.
- ***Display Previous Login In Footer***. If you select this checkbox, the user interface will display information about the last successful login to the user interface and the last failed login (if applicable). The user interface will display the following in the lower right of the page:

  Previous Login: `yyyy-mm-dd hh-mm-ss from user's IP address.`
  Failed Login: `yyyy-mm-dd hh-mm-ss from user's IP address.`

- ***Ignore trap agent-addr varbind***. If you select this checkbox, SL1 will align incoming SNMP trap messages with the forwarding device (last hop) instead of searching for the IP address of the originator of the trap.
- ***Enable Selective PowerPack Field Protection***. If you select this checkbox, the following fields will ***not*** be updated when you update a PowerPack:
  - Event Policy > ***Operational State***
  - Event Policy > ***Event Severity***
  - Event Policy > ***Event Message***
  - Event Policy > ***Occurrence Count***
  - Event Policy > ***Occurrence Time***
  - Event Policy > ***Expiry Delay***
  - Event Policy > ***Detection Weight***
  - Event Policy > ***External Event ID***

- Event Policy > ***External Category***
- Event Policy > ***Use multi-match***
- Event Policy > ***Use message-match***
- Event Policy > ***Topology Suppression***
- Dynamic Application > Properties > ***Operational State***
- Dynamic Application > Properties > ***Poll Frequency***
- Dynamic Application > Properties > ***Disable Data Rollup***
- Dynamic Application > Collection > ***Custom Attribute***
- Dynamic Application > Collection > ***Asset / Formlink***
- Dynamic Application > Collection > ***Change Alerting***
- Dynamic Application > Collection > ***Hide Object***
- Dynamic Application > Presentation > ***Active State***
- Dynamic Application > Threshold > ***Override Threshold Value***
- Dynamic Application > Threshold > ***Numeric Range: High***
- Dynamic Application > Threshold > ***Numeric Range: Low***
- Dynamic Application > Threshold > ***Threshold Value***
- Device Class > ***Device Dashboard***

- ***Hide "Create a Ticket" in Toolbox menu***. If you select this checkbox, the **Toolbox** menu (three stacked horizontal lines in the upper-left corner) will not display the *Create a Ticket* option. This field is unselected by default.
- ***Enable CDP Topology***. If selected, SL1 will use Cisco Discovery Protocol (CDP) for each device that supports CDP. SL1 will then generate topology maps from the discovered CDP relationships.

NOTE: CDP is a proprietary protocol developed by Cisco and is not supported by all network hardware. If your network includes both CDP enabled and non-CDP network switches and routers, the topology data reported by the CDP enabled devices might not be accurate. In SL1, if a conflict exists between the collected CDP topology data and the collected layer-2 topology data, the CDP topology data takes precedence. In some cases, the ScienceLogic layer-2 data might be more accurate. Therefore, if your network includes both CDP enabled and non-CDP network switches and routers, you might want to disable CDP topology collection. For details, see the ***Views*** manual.

- ***Enable LLDP Topology***. If selected, SL1 will use Link Layer Discovery Protocol (LLDP) for each device that supports LLDP. SL1 will then generate topology maps from the discovered LLDP relationships.
- ***Enable Community String Indexing (VLAN Topology)***. If selected, SL1 will perform discovery of VLANs during topology collection. By default, this option is not selected because the SNMP requests used to discover VLANs might cause some types of hardware to erroneously reboot.
- ***Default Country***. Specifies the country that will be selected by default in each page where the user specifies a country. The user can override this default value in each page.

- ***System Timezone***. Specifies the default timezone for SL1. In each page where the user can select a timezone, this value will be selected by default. The user can override this default value in each page. SL1 also uses this default value to perform timezone conversions when no user timezone setting is available. For example, if SL1 sends an email to an address not associated with a user, any timestamps contained in the email will use the value from the ***System Timezone*** field. You can select from a list of all timezones. The default value is "UTC".
- ***NFS Detection Disable***. If selected, this checkbox prevents SL1 from monitoring and reporting on NFS "shared" file systems. SL1 will monitor and report only on local file systems.
- ***Port Polling Type***. Specifies how SL1 should poll devices to discover open ports. The choices are:
    - *Half Open*. Uses a faster TCP/IP connection method and does not appear on the device's logs.
    - *Full Connect*. Uses the standard TCP/IP connection to detect open ports.
- ***Initial Discovery Scan Level***. Specifies the data to be gathered during the initial discovery session. The options are:
    - *0. Model Device Only*. Discover if device is up and running and if so, discover device's make and model.
    - *1. Discover Dynamic Apps*. Discovery tool will search for Dynamic Applications associated with the device. Discovery will also perform *0. Model Device Only* discovery.
    - *2. Initial Population of Apps*. Discovery tool will retrieve subset of data from Dynamic Applications, to save time. Discovery tool will later retrieve full sets of data from each Dynamic Application. Discovery tool will also perform *1. Discover Dynamic Apps* and *0. Model Device Only*.
    - *3. Discover SSL Certificates*. Discovery tool will search for SSL certificates and retrieve SSL data. Discovery tool will also perform *2. Initial Population of Apps*, *1. Discover Dynamic Apps*, and *0. Model Device Only*.
    - *4. Discover Open Ports*. Discovery tool will search for open ports. Discovery tool will also perform 3. *Discover SSL Certificates*, *2. Initial Population of Apps*, *1. Discover Dynamic Apps*, and *0. Model Device Only*.

NOTE: If your system includes a firewall and you select option *4: Discover Open Ports*, discovery may be blocked and/or may be taxing to your network.

    - *5. Advanced Port Discovery*. Discovery tool will search for open ports, using a faster TCP/IP connection method. Discovery tool will also perform *3. Discover SSL Certificates*, *2. Initial Population of Apps*, *1. Discover Dynamic Apps*, and *0. Model Device Only*.

NOTE: If your system includes a firewall and you select option *5: Advanced Port Discovery*, some auto-discovered devices may remain in a pending state for some time after discovery. These devices will achieve a healthy status, but this might take several hours.

- ***Rediscovery Scan Level (Nightly)***. Specifies the data to be gathered/updated each day during the nightly discovery process. The nightly discovery process will find any changes to previously discovered

devices. The ***Rediscovery Scan Level (Nightly)*** field contains the same options as the ***Initial Discovery Scan Level*** field.

- ***Discovery Scan Throttle***. Specifies the amount of time a discovery process should pause between each IP address in a discovery session. Pausing discovery processes between IP addresses spreads the amount of network traffic generated by discovery over a longer period of time. The choices are:
  - *Disabled*. Discovery processes will not pause.
  - *1000 Msec to 10000 Msec*. A discovery process will pause for a random amount of time between half the selected value and the selected value.

NOTE: The ***Discovery Scan Throttle*** setting does not affect nightly auto discovery.

- ***Port Scan All IPs***. Specifies whether SL1 should scan all IP addresses on a device for open ports. The choices are:
  - *0. Disabled*. SL1 will scan only the Admin Primary IP address (the IP address SL1 uses to communicate with the device) for open ports.
  - *1. Enabled*. SL1 will scan all discovered IP addresses for open ports.

NOTE: The ***Port Scan All IPs*** setting affects initial discovery, nightly auto discovery, and re-discovery.

- ***Port Scan Timeout***. Length of time, in milliseconds, after which SL1 should stop trying to scan an IP address for open ports and begin scanning the next IP address (if applicable). Choices are between 60,000 and 1,800,000 milliseconds.

NOTE: The ***Port Scan Timeout*** setting affects initial discovery, nightly auto discovery, and re-discovery.

- ***Restart Windows Services (Agent required)***. Specifies whether SL1 should automatically restart failed Windows services that have been defined on the device with a startup type of "automatic". The choices are:
  - *0. Disabled*. SL1 will not automatically restart failed Windows services that have been defined on the device with a startup type of "automatic".
  - *1. Enabled*. SL1 will automatically restart failed Windows services that have been defined on the device with a startup type of "automatic".

NOTE: To use this feature, the managed device must be running the agent SNMP Informant, WMI Edition. For assistance or information on purchasing and installing this agent, please contact ScienceLogic. Users must also supply a value in the ***SNMP Write*** field in the **Device Properties** page for the device.

- ***Hostname Precedence***. Specifies which name SL1 will use for each discovered device. Choices are:
    - *SNMP System Name*. Use the device name specified in the device's SNMP System MIB.
    - *DNS Reverse Lookup*. Use the device name specified in the device's reverse-lookup record.

NOTE: If *SNMP System Name* is selected, and SL1 cannot find an SNMP name for the device, SL1 will assign the name returned by the DNS Reverse Lookup. If SL1 cannot find a DNS Reverse Lookup name for the device, SL1 will use the device's Admin Primary IP address as the device name in SL1.

- ***Event Interface Name Format***. Specifies the format of the network interface name that you want to appear in events. If you selected *Interface Alias* for the deprecated ***Interface Name Precedence*** field in a previous release of SL1, the format for existing interfaces is set to {alias}. If you selected *Interface Name* for the deprecated ***Interface Name Precedence*** field in a previous release of SL1, the format for existing interfaces is set to {name}. The default format is {name}. You can use a combination of string text and the following tokens to define the interface name format for events, such as string_{name}, string_{alias}, {name}{alias}, or {ifdesc}:
    - {alias}
    - {name}
    - {state}
    - {ifdescr}
    - {if_id}
    - {did}
    - {ifindex}
    - {ifphysaddress}
    - {iftype}
    - {ifspeed}
    - {ifhighspeed}
    - {ifoperstatus}
    - {ifadminstatus}
- ***DNS Hostnames***. If SL1 will use the DNS Reverse Lookup name as the device name (see the description of the field ***Hostname Precedence***), this field specifies whether SL1 will use the fully-qualified domain name or only the hostname for each discovered device. Choices are:
    - *Strip Device Name (Hostname)*. SL1 will use only the device name as the DNS hostname for each device.
    - *Use Full Domain Name (FQDN)*. SL1 will use the fully-qualified domain name as the device name for each device.

- ***Event Clearing Mode***. Describes how clearing an event will affect correlated events. Choices are:
  - *Clear Selected Only*. Clear only the selected events. If a parent event is cleared, the previously suppressed child events will appear in the **Event Console**.
  - *Clear All in Group*. When parent event is cleared, all child events correlated with parent event will be cleared. This is the default behavior.
- ***Maintenance Minimum Severity***. Specifies the minimum severity required for an event to be suppressed during device maintenance and user maintenance for devices. The default value is *Healthy*, which causes all events to be suppressed. Choices are *Healthy*, *Notice*, *Minor*, *Major*, or *Critical*.
- ***Patch Maintenance Minimum Severity***. If you schedule Device Maintenance and have defined a ***Patch Window*** within the larger maintenance interval, this field allows you to specify the event severity that will trigger the beginning of the ***Patch Window***. The first event that both matches the severity in this field and occurs within the larger maintenance window triggers the start of the ***Patch Window***. Choices are *Healthy*, *Notice*, *Minor*, *Major*, or *Critical*.
- ***SSL Certificate Expiry Soon***. Specifies, in number of days, when SL1 should generate an event for an SSL Certificate that is about to expire. The choices range from 1 day to 9 months.
- ***SSL Certificate Expiry Imminent***. Specifies, in number of days, when SL1 should generate a more urgent event for an SSL Certificate that is about to expire. The choices range from 1 day to 9 months.
- ***Asset Warranty Expiry***. Specifies, in number of days, when SL1 should generate an event for an asset warranty that is about to expire. The choices range from 1 day to 9 months.
- ***Domain Name Expiry***. Specifies, in number of days, when SL1 should generate an event for a domain's registration that is about to expire. The choices range from 1 day to 9 months.
- ***Validate Phone Number***. Specifies whether or not phone numbers entered into the user interface must be in US format. Choices are:
  - *Disabled*. Phone numbers are not required to be in US format.
  - *Enabled*. Phone numbers must be in US format.
- ***Dashboard Maximum Series Count Per Widget***. This field allows you to select the maximum number of time-series lines that can appear in a single ***Multi-series Performance*** widget. Choices are 8–25. Increasing this setting might cause longer load times in the **[Dashboards tab]** page.
- ***Prefer Global Device Summary Dashboard Over Category/Class***. If you select this checkbox, the global default device dashboard will be displayed as the default in the **Device Summary** page instead of the device dashboard assigned to the device category or device class of the device. For more information about device dashboards, see the ***Dashboards*** manual.
- ***Enable CBQoS Collection***. If selected, SL1 will collect configuration data about Class-Based Quality-of-Service (CBQoS) from interfaces that are configured for CBQoS. If selected, you can enable collection of CBQoS metrics per-interface. The collected CBQoS metrics are displayed in Device Performance reports associated with the device that contains those interfaces. This setting is disabled by default. (For more information about Device Performance reports, see the ***Device Management*** manual.)

- ***Enable Variable Rate Interface Counters***. If selected, enables more accurate collection of data from interfaces. If enabled, when SL1 retrieves data from an interface, that data is stored in the ScienceLogic database along with the timestamp associated with the exact collection time. Before normalization occurs, SL1 applies an interpolation function that spaces the data at regular time intervals. For example, suppose you have specified that SL1 should collect interface data every five minutes. However, due to network traffic across the Data Collectors, SL1 might collect data from an interface at 13:01 and then 13:05. Because the ScienceLogic normalization process expects data that has been collected every five minutes, SL1 first applies an interpolation to the data to prepare the data for normalization.

3. Click the **[Save]** button to save changes in this page.

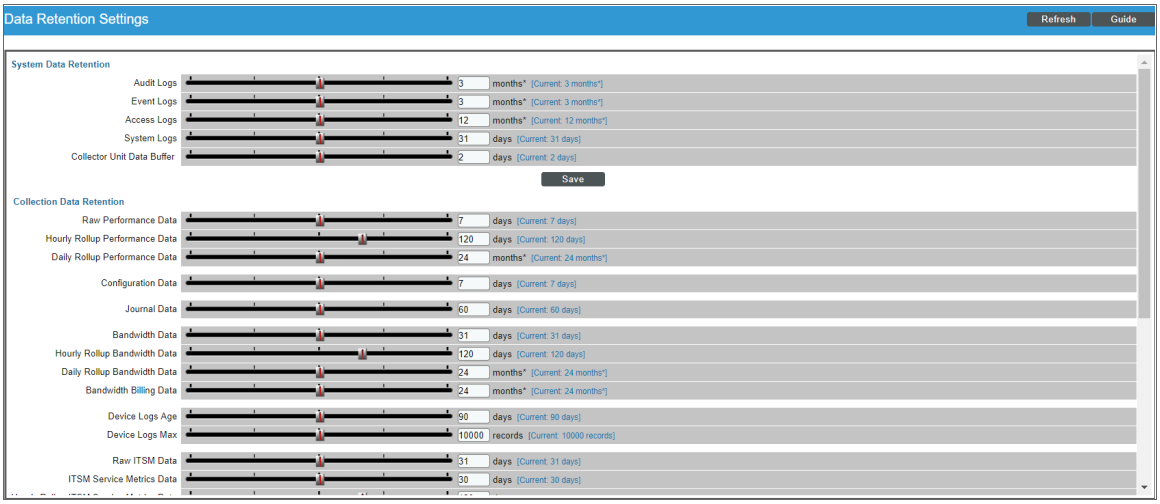
Global Settings for Data Retention

The **Data Retention Settings** page (System > Settings > Data Retention) allows you to define parameters for log and data retention.

These settings apply to all logs and all collected data. However, you can override these system settings on a case-by-case basis. For example, you can define data-retention thresholds for a device in the **Device Thresholds** page. The settings you define for the specific device override the settings in the **Data Retention Settings** page.

From the **Data Retention Settings** page, you can edit how long the platform stores log entries and collected data. To edit the settings for data retention:

1. Go to the **Data Retention Settings** page (System > Settings > Data Retention).



2. In the **Data Retention Settings** page, you can drag sliders to change the value of each field or manually enter values in the fields to the right of the sliders. You can edit the value for one or more of the following fields:

   - ***Audit Logs***. Number of months to retain log entries in the **Audit Logs** page (System > Monitor > Audit Logs). Log entries that are older than the specified number of months are automatically deleted. The default value is 3 months.

- ***Event Logs***. Number of days to retain event logs. Event history data is used to generate the **Event Overview** page (System > Monitor > Event Overview). Log entries that are older than the specified number of months are automatically deleted. The default value is 3 months.
- ***Access Logs***. Number of months to retain log entries in the **Access Sessions** page (System > Monitor > Access Logs). Log entries that are older than the specified number of months are automatically deleted. The default value is 12 months.
- ***System Logs***. Number of days to retain log entries in the **System Logs** page (System > Monitor > System Logs). Log entries that are older than the specified number of days are automatically deleted. The default value is 31 days.
- ***Collection Unit Data Buffer***. Number of days each Data Collector and Message Collector should store collected data. Choices are 1-4 days. Data that has been retrieved by the Database Server will be stored on the Data Collector(s) and optional Message Collector(s) for the specified number of days and then automatically deleted from the server(s). This setting does not apply to All-In-One Appliances. The default value is 2 days.
- ***Raw Performance Data***. Number of days to retain performance data collected from devices. This setting applies to all performance data types, except for bandwidth data. Performance data that is older than the specified number of days is automatically deleted. This is the default system-wide value. The value in the **Device Thresholds** page for each device can override this value. The default value is 7 days.
- ***Hourly Rollup Performance Data***. Number of days to retain hourly normalized performance data for devices. This setting applies to all performance data types, except for bandwidth data. Hourly normalized performance data that is older than the specified number of days is automatically deleted. This is the default system-wide value. The value in the **Device Thresholds** page for each device can override this value. The default value is 90 days.
- ***Daily Rollup Performance Data***. Number of months to retain daily normalized performance data for devices. This setting applies to all performance data types, except for bandwidth data. Daily normalized performance data that is older than the specified number of months is automatically deleted. This is the default system-wide value. The value in the **Device Thresholds** page for each device can override this value. The default value is 24 months.
- ***Configuration Data***. Number of days to retain data from Dynamic Applications of type "configuration". The value in the **Device Thresholds** page for each device can override this value. The default value is 7 days.
- ***Journal Data***. Number of days to retain collected data from Dynamic Applications of type "journal". The value in the **Device Thresholds** page for each device can override this value. The default value is 60 days.
- ***Bandwidth Data***. Number of days to retain bandwidth data and CBQoS data collected from each interface on a device. Bandwidth data that is older than the specified number of days is automatically deleted. The value in the **Device Thresholds** page for each device can override this value. The default value is 31 days.
- ***Hourly Rollup Bandwidth Data***. Number of days to retain hourly normalized data and hourly normalized CBQoS data for each interface on a device. Hourly normalized data that is older than the specified number of days is automatically deleted. The value in the **Device Thresholds** page for each device can override this value. The default value is 90 days.

- ***Daily Rollup Bandwidth Data***. Number of months to retain daily normalized data and daily normalized CBQoS data for each interface on a device. Daily normalized data that is older than the specified number of months is automatically deleted. The value in the **Device Thresholds** page for each device can override this value. The default value is 24 months.
- ***Bandwidth Billing Data***. Number of months to retain data collected by each bandwidth billing policy. Bandwidth billing data that is older than the specified number of months is automatically deleted. The default value is 24 months.
- ***Device Logs Age***. Number of days to retain each device log. Log records that are older than the specified number of days are automatically deleted. The value in the **Device Thresholds** page for each device can override this value. The default value is 90 days.
- ***Device Logs Max***. Maximum number of records to store in each device log. When this number is exceeded, the oldest entries will be deleted. The value in the **Device Thresholds** page for each device can override this value. The default value is 10,000 records.
- ***Raw ITSM Data***. Before the value for a metric in an IT Service policy is calculated, a copy of all the device data that will be aggregated is saved. This setting is the number of days to retain the un-aggregated copies of device data associated with each IT Service. The default value is 31 days.
- ***ITSM Service Metrics Data***. Number of days to retain values for metrics in IT Service policies. The default value is 30 days.
- ***Hourly Rollup ITSM Service Metrics Data***. Number of days to retain hourly normalized values for metrics in IT Service policies. The default value is 90 days.
- ***Daily Rollup ITSM Service Metrics Data***. Number of months to retain daily normalized values for metrics in IT Service policies. The default value is 12 months.
- ***ITSM Key Metrics Data***. Number of days to retain values for key metrics in IT Service policies (Health, Availability, and Risk). The default value is 30 days.
- ***Hourly Rollup ITSM Key Metrics Data***. Number of days to retain hourly normalized values for key metrics in IT Service policies (Health, Availability, and Risk). The default value is 90 days.
- ***Daily Rollup ITS Key Metrics Data***. Number of months to retain daily normalized values for key metrics in IT Service policies (Health, Availability, and Risk). The default value is 24 months.
- ***Subscriber Device Configuration Data***. For users with a subscriber license. Number of months to retain the files and database tables that contain configuration information for a device. Default value is 6 months.
- ***Subscriber Device Usage Data***. For users with a subscriber license. Number of months to retain the files and database tables that contain usage information for a device. Default value is 6 months.
- ***Subscriber System Configuration Data***. For users with a subscriber license. Number of months to retain the files and database tables that contain configuration information for the SL1 system. Default value is 3 months.
- ***Subscriber System Usage Data***. For users with a subscriber license. Number of months to retain the files and database tables that contain usage information for the SL1 system. Default value is 3 months.
- ***Subscriber Device Type Data***. For users with a subscriber license. Number of months to retain the files and database tables that map each device to a device category, as per your subscriber license. Default value is 3 months.

- ***Subscriber Daily Delivery Data***. For users with a subscriber license. Number of months to retain the "crunched" license usage data that is calculated each day using the Subscriber Device Configuration Data, Subscriber System Configuration Data, Subscriber System Usage Data, and Subscriber Device Type Data. SL1 will not prune data that has not yet been delivered to the ScienceLogic Licensing and Billing server. Default value is 3 months.

3. Click the **[Save]** button to save any changes to the data-retention settings.

NOTE: In SL1, normalized data does not include polling sessions that were missed or skipped. So for normalized data, null values are not included when calculating maximum values, minimum values, or average values.

TIP: You might want to retain normalized data for longer periods of time and non-normalized data for shorter periods of time. This allows you to save space and still create historical reports.

Global Settings for Inbound Email and Outbound Email

The **Email Settings** page (System > Settings > Email) allows you to define how SL1 will send and receive email. SL1 automatically sends email when tickets are updated, when automation actions are triggered, and to monitor email round-trip time. Email can be sent to the platform to create tickets and/or events.

From the **Email Settings** page, you can edit the global email parameters. To do so:

1. Go to the **Email Settings** page (System > Settings > Email).

2. In the **Email Settings** page, you can edit the value for one or more of the following fields:

   - ***Authorized Email Domains***. One or more SMTP domains that will be used by SL1. SL1 will use these domains to receive incoming email. This list of domains should include:

     - All domains used for loopback addresses in email round-trip monitoring policies.
     - All domains used to generate tickets from emails.

- All domains used to receive event messages from third-party monitoring systems.
- Each entry in this field must be a fully-qualified email domain and cannot exceed 64 characters. If you include a list of domains, separate the list with commas.
- Each domain in this field must be managed by the Database Server. This means that a DNS MX record must already exist or be created for each domain specified in this field. Each DNS MX record must map the domain to the Database Server. When creating the DNS MX record, use the fully-qualified name of the Database Server as the name of the email server.

- ***System From Email Address***. The email address from which SL1 will send all outbound email.
- ***Email Formal Name***. Name that will appear in the "from" field in email messages sent from SL1. This value can be any alphanumeric value, up to 64 characters in length.
- ***Email Gateway***. IP address or fully-qualified name of SL1's SMTP Relay server. If SL1 is to send outgoing messages, this field must be defined. Examples of when SL1 sends outgoing email messages are:
  - Automatically in response to Tickets from Email policies.
  - Automatically in response to changes in a ticket (ticket is assigned, edited, or resolved).
  - Automatically based on Ticket Escalation policies.
  - Automatically when executing Email Round-Trip Monitoring policies.
  - Automatically when executing Run Book policies that include email actions.
  - Automatically based on Report Jobs policies.
  - Manually, when a user selects the **Send Message** page from the ticket panel pages.

  Each Database Server and All-In-One Appliance includes a built-in SMTP Relay server. The fully-qualified name of SL1 SMTP Relay server is the same as the fully-qualified name of the Database Server or All-In-One Appliance.

  If SL1 cannot use its built-in SMTP relay server to route email messages directly to their destination server (for example, due to firewall rules or DNS limitations), SL1 can use another relay server. You can specify the IP address or fully-qualified name of the relay server in this field. Make sure you have configured your network to allow the Database Server or All-In-One Appliance to access this SMTP Relay server.

- ***Email Gateway Alt***. IP address or fully-qualified name of the secondary SMTP Relay server. If the SMTP Relay server specified in the previous field fails or is unavailable, SL1 will use the secondary SMTP Relay server. Make sure you have configured your network to allow the Database Server or All-In-One Appliance to access this SMTP Relay server.
- ***Escalation Notify Subject***. Default "Subject" text in emails generated by Ticket Escalation policies. This field can include any combination of variables and text. The field can include up to 64 characters, including one or more variables:

The ***Escalation Notify Subject*** field can include one or more of the following variables:

Variable	Source	Description
%1 (one)	Event	Entity type.
%2	Event	Sub-entity type.
%3	Event Policy	Event policy ID.
%4	Event	Text string of the user name that cleared the event.
%5	Event	Timestamp of when event was deleted.
%6	Event	Timestamp for event becoming active.
%7	Event	Event severity (1-5), for compatibility with previous versions of the platform. 1=critical, 2=major, 3=minor, 4=notify, 5=healthy.
%A	Account	Username.
%a	Entity	IP address.
%B	Organization	Organization billing ID.
%b	Organization	Impacted organization.
%C	Organization	Organization CRM ID.
%c	Event	Event counter.
%D	Event	Timestamp of first event occurrence.
%d	Event	Timestamp of last event occurrence.
%E	Event Policy	External ID from event policy.
%e	Event	Event ID.
%F	Dynamic Alert	Dynamic Application alert id.
%f	Event Policy	Specifies whether event is stateful, that is, has an associated event that will clear the current event. 1 (one) = stateful; 0 (zero) = not stateful.
%G	Event Policy	Event Category.
%g	Asset	Asset serial.
%H	Event	URL link to event.
%h	Asset	Device ID associated with the asset.
%I (uppercase "eye")	Dynamic Alert	Table index for a Dynamic Application.

Variable	Source	Description
%i (lowercase "eye")	Asset	Asset Location.
%7	Ticket	Ticket subject.
%K	Asset	Asset Floor.
%k	Asset	Asset Room.
%M	Event	Event message.
%m	Automation	Automation policy note.
%N	Action	Automation action name.
%n	Automation	Automation policy name.
%O (uppercase "oh")	Organization	Organization name.
%o (lowercase "oh")	Organization	Organization ID.
%P	Asset	Asset plate.
%p	Asset	Asset panel.
%Q	Asset	Asset punch.
%q	Asset	Asset zone.
%R	Event Policy	Event policy cause/action text.
%r	System	Unique ID / name for the current SL1 system.
%S	Event	Severity (Healthy - Critical).
%s	Event	Severity (0 - 4). 0=healthy, 1=notify, 2=minor, 3=major, 4=critical.
%T	Dynamic Alert	Dynamic Application alert threshold value.
%t	Ticket	Ticket ID.
%U	Asset	Asset rack.
%u	Asset	Asset shelf.
%V	Dynamic Alert	Dynamic Application alert result value.
%v	Asset	Asset tag.
%W	Asset	Asset make.
%w	Asset	Asset model.

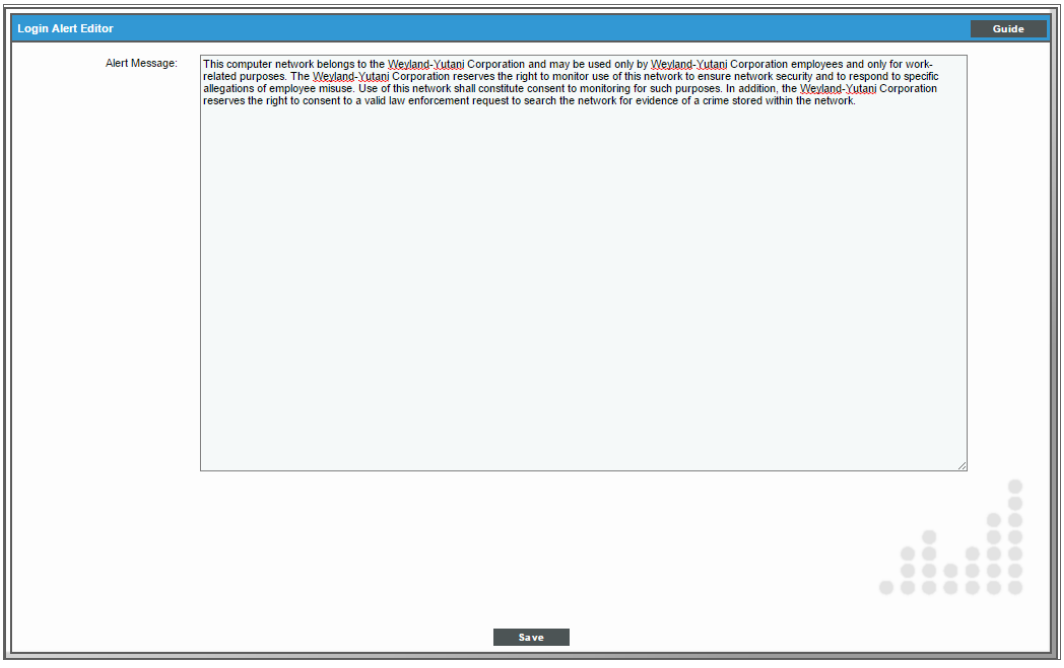
Variable	Source	Description
%X	Event	Entity name.
%x	Event	Entity ID.
%Y	Event	Sub-entity name.
%y	Event	Sub-entity ID.
%Z	Event	Event source (1 - 8).
%z	Event	Event source (Syslog - Group).

Global Settings for Login Alert Messages

In SL1, administrators can add a customizable click-through alert message as a security measure at logon. Users will not be able to access the system until the user click the **[OK]** button to agree to the terms and conditions of use for that system.

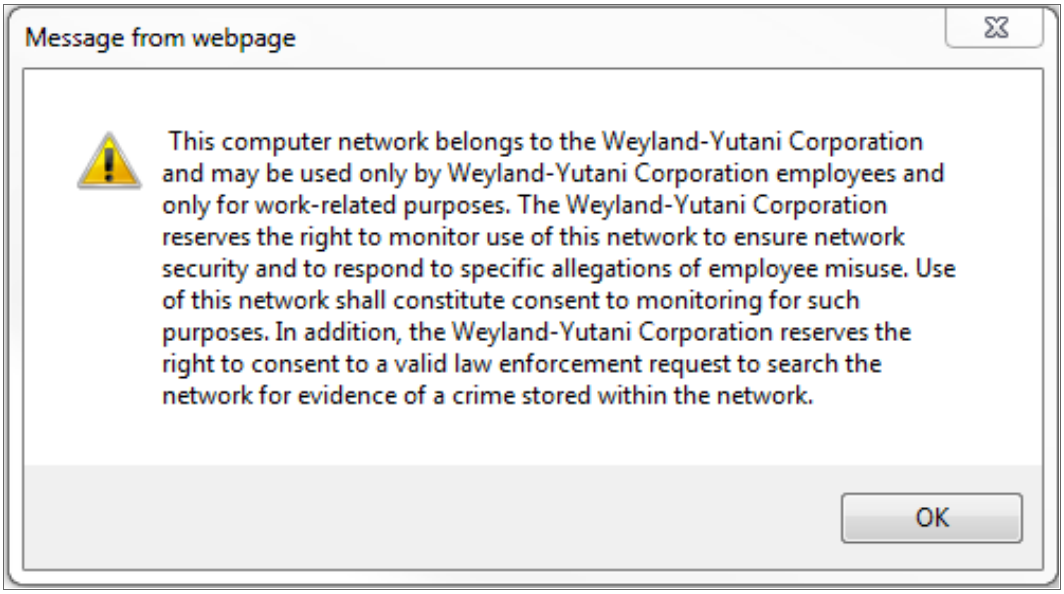
To add a custom login alert message to SL1:

1. Go to the **Login Alert Editor** page (System > Settings > Login Alert Message).
2. In the ***Alert Message*** field, type the text of your login alert message:



3. After entering the login alert text, click the **[Save]** button.

4. When a user logs in, the alert message will display:



Global Settings for Password Reset Emails

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

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

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

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

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

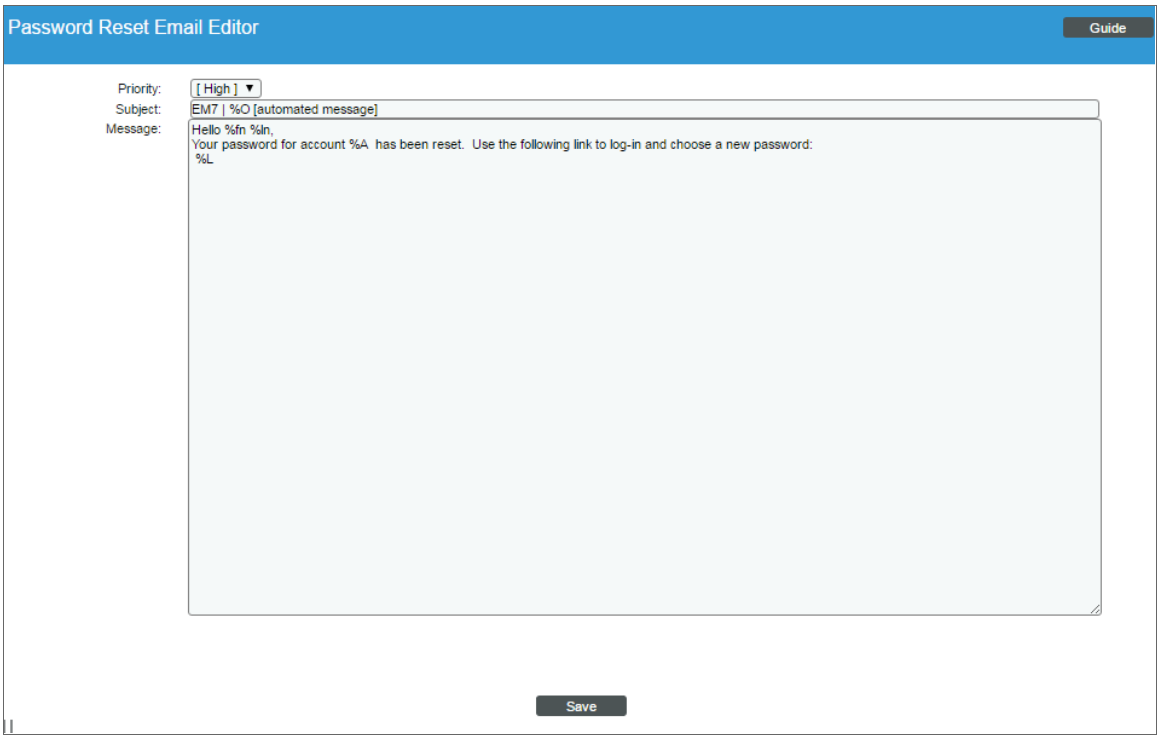
If the user exceeds the number of login tries (defined in the **Behavior Settings** page), the "I forgot my password" option is not displayed in the **Login** page.

Defining the Email Message for "I forgot my password"

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

To define the email message sent by SL1:

1. Go to the **Password Reset Email Editor** page (System > Settings > Password Reset Email).



2. Supply a value in each of the following fields:
   - ***Priority***. This will be the priority of the email message. Choices are:
     - *High*. Emails will be marked as high priority.
     - *Normal*. Emails will be marked as normal priority.
     - *Low*. Emails will be marked as low priority.
   - ***Subject***. This will be the subject of the email message.
   - ***Message***. This will be the body of the email message. ***The body must include the variable %L***. This variable inserts the link to the page that allows the user to reset their ScienceLogic password.
3. You can include the following variables in the ***Subject*** field and the ***Message*** field:

- *%L (uppercase "el")*. The link to the page that allows the user to reset their password.
- *%O (uppercase "oh")*. The user's primary organization, as defined in the **Account Permissions** page for the user.
- *%fn (lowercase "eff" "en")*. The user's first name, as defined in the **Account Permissions** page for the user.
- *%ln (lowercase "el "en"*. The user's last name, as defined in the **Account Permissions** page for the user.

4. Click the **[Save]** button to save the email template.
5. When a user follows the link in the email, SL1 displays the **Login** page, with the message "Your account has been reset. Please create a new password." The user must then enter their new password twice. The new password is recorded in SL1 and replaces the previous (forgotten) password.

For example, you could define the following:

Subject. ScienceLogic | %O (automated message)

Message. Hello %fn %ln,

Your password for account %A has been reset.

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

%L.

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

Subject: ScienceLogic | System (automated message).

Hello Keyser Soze,

Your password for account ksoze has been reset.

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

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

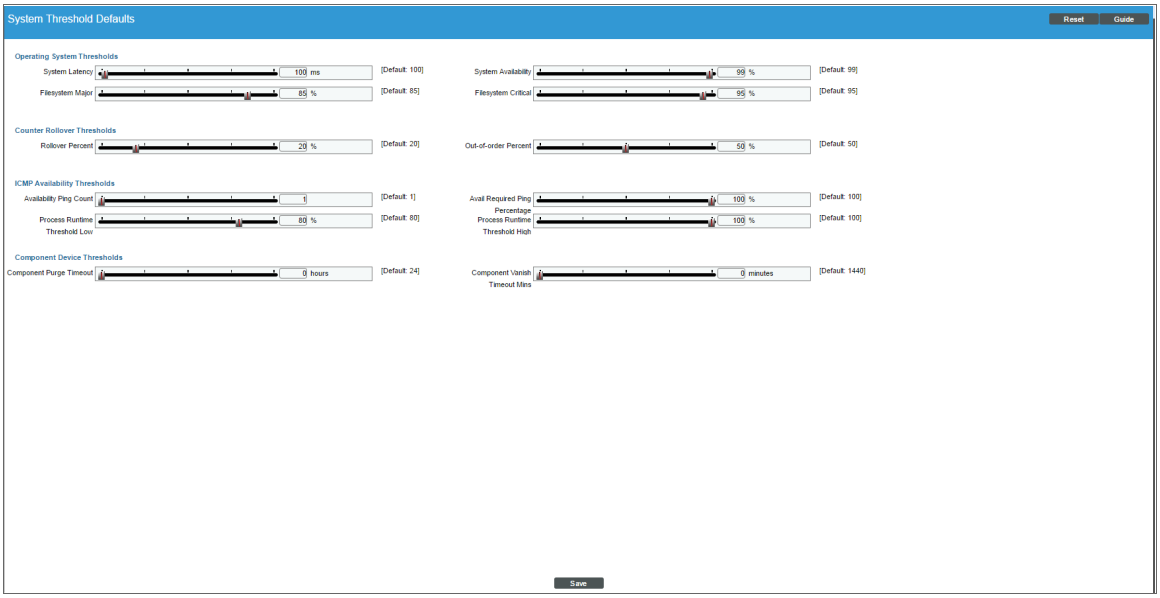
Global Settings for System Thresholds

The **System Threshold Defaults** page (System > Settings > Thresholds > System) allows you to define global thresholds for system latency, file system usage, counter rollovers, ICMP availability, and number of component devices.

These settings apply to all devices. However, you can override these system settings on a case-by-case basis. For example, you can define thresholds for a device's file systems in the **Device Thresholds** page (Devices > Device Manager > wrench icon > Thresholds). The settings you define for the specific device override the settings in the **System Threshold Defaults** page.

To edit the global settings for system thresholds:

1. Go to the **System Threshold Defaults** page (System > Settings > Thresholds > System).



2. In the **System Threshold Defaults** page, you can drag sliders to change to value of each field or edit a field manually. You can edit the value for one or more of the following fields:

    - ***Interface Inventory Timeout***. Specifies the maximum amount of time that the discovery processes will spend polling a device for the list of interfaces. After the specified time, SL1 will stop polling the device, will not model the device, and will continue with discovery. The default value is 600,000 ms (10 minutes).
        - During *initial discovery*, initiated from the Discovery Session Editor page (System > Manage > Classic Discovery > Create), SL1 uses the value in this field if there is no differing value specified in the **Discovery Session Editor** page.

- During *re-discovery* (clicking the binocular icon () in the Device Properties page), SL1 will use the value in this field if there no value is specified in the **Device Thresholds** page (Devices > Device Manager > wrench icon > Thresholds) for the device.
- During *nightly auto-discovery* (run automatically by SL1 every night, to update device information), SL1 uses the value in this field if no differing value is specified in the **Device Thresholds** page (Devices > Device Manager > wrench icon > Thresholds) for a device.

- ***Maximum Allowed Interfaces***. Specifies the maximum number of interfaces per device. If a device exceeds this number of interfaces, SL1 will stop scanning the device, will not model the device, and will continue with discovery. The default value is 10,000.
  - During *initial discovery*, initiated from the **Discovery Session Editor** page (System > Manage > Classic Discovery > Create), SL1 uses the value in this field if there is no differing value specified in the **Discovery Session Editor** page.
  - During *re-discovery* (clicking the binocular icon () in the Device Properties page), SL1 will use the value in this field if there is no differing value is specified in the **Device Thresholds** page (Devices > Device Manager > wrench icon > Thresholds) for the device.
  - During *nightly auto-discovery* (run automatically by SL1 every night, to update device information), SL1 uses the value in this field if no differing value is specified in the **Device Thresholds** page (Devices > Device Manager > wrench icon > Thresholds) for a device.
- ***System Latency***. During polling, the platform initially pings monitored devices. The value in this field is the maximum number of milliseconds for the device to respond to SL1's ping (round-trip time divided by 2). The default value is 100 ms. When the latency threshold is exceeded, SL1 generates an event for that device.
- ***System Availability***. During polling, SL1 monitors devices for availability. Availability means the device's ability to accept connections and data from the network. The value in this field is the percent availability required of each device. The default value is 99%. When a device falls below this level of availability, SL1 generates an event for that device.

  During polling, a device has two possible availability values:
  - 100%. Device is up and running.
  - 0%. Device is not accepting connections and data from the network.

NOTE: Component devices use a Dynamic Application collection object to measure availability. SL1 polls component devices for availability at the frequency defined in the Dynamic ApplicationFor details, see the chapter on *Monitoring Device Availability and Device Latency* in the ***Device Management*** manual.

NOTE: The ***Ping & Poll Timeout (Msec)*** setting in the **Behavior Settings** page (System > Settings > Behavior) affects how SL1 monitors device availability. This field specifies the number of milliseconds the discovery tool and availability polls will wait for a response after pinging a device. After the specified number of milliseconds have elapsed, the poll will timeout.

- ***File System Major***. Threshold that will trigger a "low disk space" event. The default threshold is 85%. When a device has used more disk space than the specified percentage, SL1 will generate a "file system usage exceeded threshold" event with a status of "major".
- ***File System Critical***. Threshold that will trigger a "low disk space" event. The default threshold is 95%. When a device has used more disk-space than the specified percentage, SL1 will generate a "file system usage exceeded threshold" event with a status of "critical".

NOTE: If you hide a file system in the **Device Hardware** page (Devices > Hardware), SL1 does not generate events for that file system.

- ***Rollover Percent***. For any collected data that uses a 32-bit counter, you can specify how SL1 determines that the counter has "rolled over", that is, has reached its maximum value, is reset to zero, and restarts counting. When this happens, the collected values go from the maximum value to a lower value. However, there are multiple circumstances under which a counter value can go from a higher value to a lower value:
    - Maximum value has been exceeded and counter was reset to zero.
    - Retrieved value was manually reset to zero on the external device.
    - Data was collected out-of-order, that is, due to a slowdown somewhere in the network, two counter values were stored out of sequence.

NOTE: For 64-bit counters, when the counter values go from a higher value to a lower value, SL1 assumes that the counter has been manually reset or that the two values were collected out of order. SL1 does not assume that the counter has rolled over.

The ***Rollover Percent*** field allows you to specify a threshold that indicates that a 32-bit counter has reached its maximum value and restarted counting. The default value is 20%. When SL1 records a counter value that is lower than the previously collected value, the platform:

- Calculates the difference between the two counter values (the delta):

  2^{32} - Last Collected Value + Current Collected Value

- Examines the value of the ***Rollover Percent*** threshold. If the delta is less than the specified percentage of the maximum possible value (2^{32}), SL1 concludes that the 32-bit counter rolled over.
- For example, if you specified "25" in this field, SL1 would determine if the delta is less than 25% of the maximum possible value. If the delta is less than 25% of the maximum possible value, SL1 concludes that the 32-bit counter rolled over.
- When SL1 determines a counter has rolled over, SL1 uses the delta value when displaying the data point for this poll period.

NOTE: The ***Rollover Percent*** field applies only to 32-bit counters. If a 64-bit counter value goes from a higher value to a lower value, the change is treated as either a manual reset or an out-of-order collection.

- ***Out-of-order Percent***. For any collected data that uses a counter, you can specify how SL1 determines that data has been collected out of order. When this data is collected out of order, the collected values go from a higher value to a lower value. However, there are multiple circumstances under which a counter value can go from a higher value to a lower value:
    - Maximum value has been exceeded and counter was reset to zero (for 32-bit counters only).
    - Data was collected out-of-order, that is, due to a slowdown somewhere in the network, two counter values were stored out of sequence.
    - Retrieved value was manually reset to zero on the external device.

  The ***Out-of-order Percent*** field allows you to specify a threshold that indicates that data has been collected out of order. The default value is 50%. When SL1 records a counter value that is lower than the previously collected value and the platform has determined that the value is not a rollover, SL1:

    - Compares the current value to the last collected value:

      current value / last collected value

    - If the ratio of current value / last collected value is greater than the percent specified in the ***Out-of-order Percent*** field, SL1 concludes that the data was collected out of order.
    - When SL1 determines a data point has been collected out of order, SL1 uses the following value as the current value of the data point:

      last collected value - current collected value

NOTE: If a 32-bit counter value goes from the maximum value to a lower value, and the current collected value does not meet the criteria for a rollover AND the current collected value does not meet the criteria for out-of-order, SL1 concludes that the 32-bit counter was manually reset to zero (0). SL1 uses the current collected value for this data point.

NOTE: If a 64-bit counter value goes from a higher value to a lower value, and the current collected value does not meet the criteria for out-of-order, SL1 concludes that the 64-bit counter was manually reset to zero (0). SL1 uses the current collected value for this data point.

- ***Availability Ping Count***. If you select *ICMP* in the ***Availability Port*** field in the **Device Properties** page (Devices> Device Manager > wrench icon) for a device, this field specifies the number of packets that should be sent during each availability check. The default value is "1".

- ***Avail Required Ping Percentage***. If you select *ICMP* in the ***Availability Port*** field in the **Device Properties** page (Devices> Device Manager > wrench icon) for a device, this field specifies the percentage of packets that must be returned during an availability check for SL1 to consider the device available. The default value is "100%".
- ***Process Runtime Threshold Low***. Threshold that will trigger a "process time exceeded" event. The default threshold is 80%. When a process has used more than 80% of its allowed ***Run Length***, SL1 will generate a "process time exceeded threshold" event with a status of "minor".
- ***Process Runtime Threshold High***. Threshold that will trigger a "process time exceeded" event. The default threshold is 100%. When a process has used 100% of its allowed ***Run Length***, SL1 will generate a "process time exceeded threshold" event with a status of "major".

NOTE: ***Run Length*** is defined in the **Process Manager** page (System > Settings > Admin Processes).

- ***Component Purge Timeout***. If SL1 cannot retrieve information from a root device about a component device, this field specifies how many hours to wait until purging the component device. When a device is purged, SL1 stops trying to collect data about the component device. The purged device will not appear in reports or views on in any pages in the user interface. When a device is purged, all of its configuration data and collected data is deleted from the Database Server. If you set this value to "0", component devices are never purged. You can override this threshold for a specific device in the **Device Thresholds** page for the device.

NOTE: When a device is set to "vanished", all children of that device are also set to "vanished". When a device is purged, all children of that device are also purged.

- ***Component Vanish Timeout Mins***. If SL1 cannot retrieve information from a root device about a component device, this field specifies how many minutes to wait until putting the component device into "vanish" mode. When a device is set to "vanished", SL1 stops trying to collect data about the component device. The vanished device will not appear in reports or views. The vanished device will appear in the **Vanished Device Manager** page. If you set this value to "0", component devices are never set to "vanished". You can override this threshold for a specific device in the **Device Thresholds** page for the device.

3. Click the **[Save]** button to save changes in this page.

Global Settings for Interface Thresholds

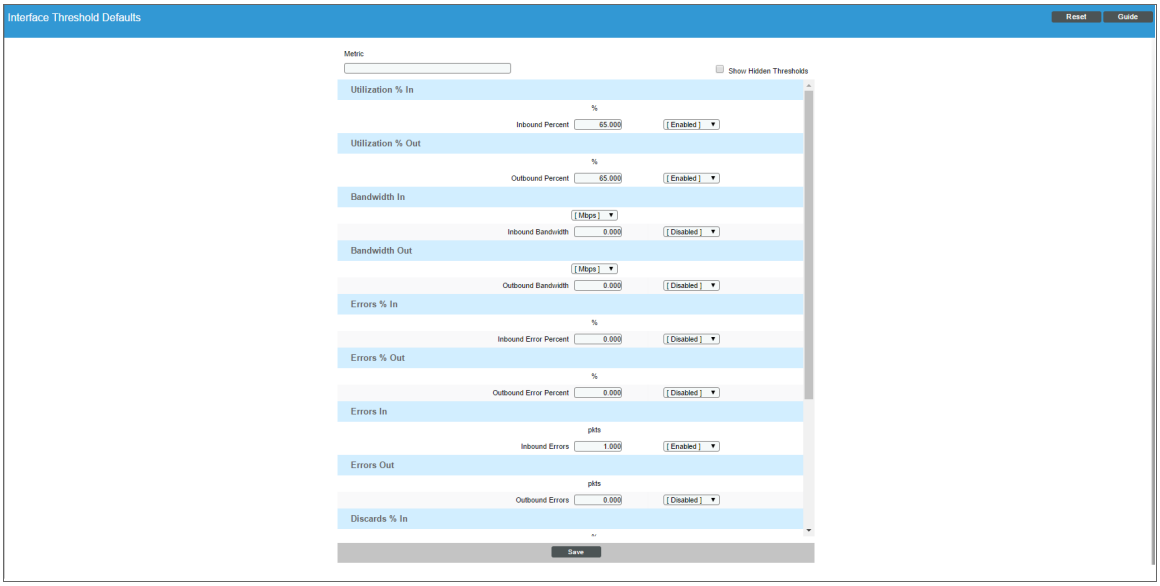
The **Interface Thresholds Defaults** page (System > Settings > Thresholds > Interface) allows you to define global thresholds for interfaces.

The settings in the **Interface Thresholds Defaults** page apply to all interfaces. However, you can override these system settings on a case-by-case basis for each interface in the **Thresholds** tab on the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon).

If you have specified that SL1 should monitor an interface, SL1 will collect data about the interface and also monitor performance thresholds for the interface. SL1 will use either the default thresholds defined in the **Interface Thresholds Defaults** page (System > Settings > Thresholds > Interface or the custom threshold you define in the **Thresholds** tab on the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon). When the values for an interface exceed one or more thresholds, SL1 will generate an event.

To define global thresholds for interfaces:

1. Go to **Interface Thresholds Defaults** page (System > Settings > Thresholds > Interface.



2. The following global thresholds are defined by default in the **Interface Thresholds Defaults** page:

NOTE: You can specify the unit of measure for all the metrics in **Bandwidth In** and **Bandwidth Out**. You can select ***bps***, ***kbps***, ***Mbps*** (the default), or ***Gbps***.

Threshold	Default Value	Default Status
Utilization % In > Inbound Percent	65.000	Enabled
Utilization % Out > Outbound Percent	65.000	Enabled
Bandwidth In > Inbound Bandwidth	0.000	Disabled
Bandwidth Out > Outbound Bandwidth	0.000	Disabled
Errors % In > Inbound Error Percent	1.000	Enabled
Errors % Out > Outbound Error Percent	1.000	Enabled
Errors In > Inbound Errors	1000.000	Enabled

Threshold	Default Value	Default Status
Errors Out > Outbound Errors	1000.000	Enabled
Discard % In > Inbound Discard Percent	1.000	Enabled
Discards % Out > Outbound Discard Percent	1.000	Enabled
Discards In > Inbound Discards	1000.000	Enabled
Discards Out > Outbound Discards	1000.000	Enabled
Multicast % In > Rising Medium	30.000	Disabled
Multicast % In > Rising Low	20.000	Disabled
Broadcast % Out > Rising Medium	30.000	Disabled
Broadcast % Out > Rising Low	20.000	Disabled

3. Selecting the ***Show Hidden Thresholds*** checkbox displays the following default thresholds:

NOTE: You can specify the unit of measure for all the metrics in **Bandwidth In** and **Bandwidth Out**. You can select ***bps***, ***kbps***, ***Mbps*** (the default), or ***Gbps***.

Threshold	Default Value	Default Status
Utilization % In > Rising High	0.000	Hidden
Utilization % In > Rising Medium	0.000	Hidden
Utilization % In > Rising Low	0.000	Hidden
Utilization % In > Falling Low	0.000	Hidden
Utilization % In > Falling Medium	0.000	Hidden
Utilization % In > Falling High	0.000	Hidden
Utilization % In > Inbound Percent	65.000	Enabled
Utilization % Out> Rising High	0.000	Hidden
Utilization % Out > Rising Medium	0.000	Hidden
Utilization % Out > Rising Low	0.000	Hidden
Utilization % Out > Falling Low	0.000	Hidden
Utilization % Out > Falling Medium	0.000	Hidden
Utilization % Out > Falling High	0.000	Hidden
Utilization % Out > Outbound Percent	65.000	Enabled

Threshold	Default Value	Default Status
Bandwidth In > Rising High	0.000	Hidden
Bandwidth In > Rising Medium	0.000	Hidden
Bandwidth In > Rising Low	0.000	Hidden
Bandwidth In > Falling Low	0.000	Hidden
Bandwidth In > Falling Medium	0.000	Hidden
Bandwidth In > Falling High	0.000	Hidden
Bandwidth In > Inbound Bandwidth	0.000	Disabled
Bandwidth Out > Rising High	0.000	Hidden
Bandwidth Out > Rising Medium	0.000	Hidden
Bandwidth Out > Rising Low	0.000	Hidden
Bandwidth Out > Falling Low	0.000	Hidden
Bandwidth Out > Falling Medium	0.000	Hidden
Bandwidth Out > Falling High	0.000	Hidden
Bandwidth Out > Outbound Bandwidth	0.000	Disabled
Errors % In > Rising High	0.000	Hidden
Errors % In > Rising Medium	0.000	Hidden
Errors % In > Rising Low	0.000	Hidden
Errors % In > Falling Low	0.000	Hidden
Errors % In > Falling Medium	0.000	Hidden
Errors % In > Falling High	0.000	Hidden
Errors % In > Inbound Error Percent	1.000	Enabled
Errors % Out > Rising High	0.000	Hidden
Errors % Out > Rising Medium	0.000	Hidden
Errors % Out > Rising Low	0.000	Hidden
Errors % Out > Falling Low	0.000	Hidden
Errors % Out > Falling Medium	0.000	Hidden
Errors % Out > Falling High	0.000	Hidden
Errors % Out > Outbound Error Percent	1.000	Enabled
Errors In > Rising High	0.000	Hidden

Threshold	Default Value	Default Status
Errors In > Rising Medium	0.000	Hidden
Errors In > Rising Low	0.000	Hidden
Errors In > Falling Low	0.000	Hidden
Errors In > Falling Medium	0.000	Hidden
Errors In > Falling High	0.000	Hidden
Errors In > InboundErrors	1000.000	Enabled
Errors Out > Rising High	0.000	Hidden
Errors Out > Rising Medium	0.000	Hidden
Errors Out > Rising Low	0.000	Hidden
Errors Out > Falling Low	0.000	Hidden
Errors Out > Falling Medium	0.000	Hidden
Errors Out > Falling High	0.000	Hidden
Errors Out > Outbound Errors	1000.000	Enabled
Discards % In > Rising High	0.000	Hidden
Discards % In > Rising Medium	0.000	Hidden
Discards % In > Rising Low	0.000	Hidden
Discards % In > Falling Low	0.000	Hidden
Discards % In > Falling Medium	0.000	Hidden
Discards % In > Falling High	0.000	Hidden
Discards % In > Inbound Discard Percent	1.000	Enabled
Discards % Out > Rising High	0.000	Hidden
Discards % Out > Rising Medium	0.000	Hidden
Discards % Out > Rising Low	0.000	Hidden
Discards % Out > Falling Low	0.000	Hidden
Discards % Out > Falling Medium	0.000	Hidden
Discards % Out > Falling High	0.000	Hidden
Discards % Out > Outbound Discard Percent	1.000	Enabled
Discards In > Rising High	0.000	Hidden
Discards In > Rising Medium	0.000	Hidden

Threshold	Default Value	Default Status
Discards In > Rising Low	0.000	Hidden
Discards In > Falling Low	0.000	Hidden
Discards In > Falling Medium	0.000	Hidden
Discards In > Falling High	0.000	Hidden
Discards In > Inbound Discards	1000.000	Enabled
Discards Out > Rising High	0.000	Hidden
Discards Out > Rising Medium	0.000	Hidden
Discards Out > Rising Low	0.000	Hidden
Discards Out > Falling Low	0.000	Hidden
Discards Out > Falling Medium	0.000	Hidden
Discards Out > Falling High	0.000	Hidden
Discards Out > Outbound Discards	1000.000	Enabled
Broadcast % In > Rising High	0.000	Hidden
Broadcast % In > Rising Medium	30.000	Disabled
Broadcast % In > Rising Low	20.000	Disabled
Broadcast % In > Falling Low	0.000	Hidden
Broadcast % In > Falling Medium	0.000	Hidden
Broadcast % In > Falling High	0.000	Hidden
Broadcast % Out > Rising High	0.000	Hidden
Broadcast % Out > Rising Medium	30.000	Disabled
Broadcast % Out > Rising Low	20.000	Disabled
Broadcast % Out > Falling Low	0.000	Hidden
Broadcast % Out > Falling Medium	0.000	Hidden
Broadcast % Out > Falling High	0.000	Hidden
Broadcast In > Rising High	0.000	Hidden
Broadcast In > Rising Medium	0.000	Hidden
Broadcast In > Rising Low	0.000	Hidden
Broadcast In > Falling Low	0.000	Hidden
Broadcast In > Falling Medium	0.000	Hidden

Threshold	Default Value	Default Status
Broadcast In > Falling High	0.000	Hidden
Broadcast Out > Rising High	0.000	Hidden
Broadcast Out > Rising Medium	0.000	Hidden
Broadcast Out > Rising Low	0.000	Hidden
Broadcast Out > Falling Low	0.000	Hidden
Broadcast Out > Falling Medium	0.000	Hidden
Broadcast Out > Falling High	0.000	Hidden
Multicast % In > Rising High	0.000	Hidden
Multicast % In > Rising Medium	00.000	Hidden
Multicast % In > Rising Low	00.000	Hidden
Multicast % In > Falling Low	0.000	Hidden
Multicast % In > Falling Medium	0.000	Hidden
Multicast % In > Falling High	0.000	Hidden
Multicast % Out > Rising High	0.000	Hidden
Multicast % Out > Rising Medium	00.000	Hidden
Multicast % Out > Rising Low	00.000	Hidden
Multicast % Out > Falling Low	0.000	Hidden
Multicast % Out > Falling Medium	0.000	Hidden
Multicast % Out > Falling High	0.000	Hidden
Multicast In > Rising High	0.000	Hidden
Multicast In > Rising Medium	0.000	Hidden
Multicast In > Rising Low	0.000	Hidden
Multicast In > Falling Low	0.000	Hidden
Multicast In > Falling Medium	0.000	Hidden
Multicast In > Falling High	0.000	Hidden
Multicast Out > Rising High	0.000	Hidden
Multicast Out > Rising Medium	0.000	Hidden
Multicast Out > Rising Low	0.000	Hidden
Multicast Out > Falling Low	0.000	Hidden

Threshold	Default Value	Default Status
Multicast Out > Falling Medium	0.000	Hidden
Multicast Out > Falling High	0.000	Hidden
Unicast % In > Rising High	0.000	Hidden
Unicast % In > Rising Medium	00.000	Hidden
Unicast % In > Rising Low	00.000	Hidden
Unicast % In > Falling Low	0.000	Hidden
Unicast % In > Falling Medium	0.000	Hidden
Unicast % In > Falling High	0.000	Hidden
Unicast % Out > Rising High	0.000	Hidden
Unicast % Out > Rising Medium	00.000	Hidden
Unicast % Out > Rising Low	00.000	Hidden
Unicast % Out > Falling Low	0.000	Hidden
Unicast % Out > Falling Medium	0.000	Hidden
Unicast % Out > Falling High	0.000	Hidden
Unicast In > Rising High	0.000	Hidden
Unicast In > Rising Medium	0.000	Hidden
Unicast In > Rising Low	0.000	Hidden
Unicast In > Falling Low	0.000	Hidden
Unicast In > Falling Medium	0.000	Hidden
Unicast In > Falling High	0.000	Hidden
Unicast Out > Rising High	0.000	Hidden
Unicast Out > Rising Medium	0.000	Hidden
Unicast Out > Rising Low	0.000	Hidden
Unicast Out > Falling Low	0.000	Hidden
Unicast Out > Falling Medium	0.000	Hidden
Unicast Out > Falling High	0.000	Hidden

4. For each threshold, you can edit the following:

    - ***Value***. The value at which the threshold will trigger an event.

        - For thresholds that include the word *Rising*, when a value exceeds the specified value, SL1 triggers an event.

- For thresholds that include the word *Falling*, when a value falls below the specified value, SL1 triggers an event.
- For thresholds that do not include the word *Rising* or *Falling*, when a value exceeds the specified value, SL1 triggers an event.

- ***Status***. Specifies whether the threshold is active and whether the threshold will appear in the **Thresholds** tab on the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon). Choices are:
  - *Enabled*. The threshold is applied to all interfaces and is monitored by SL1. The threshold appears in the **Thresholds** tab on the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon). Users can edit the ***Value*** and ***Status*** of the threshold.
  - *Disabled*. The threshold is applied to all interfaces but is not monitored by SL1. The threshold appears in the **Thresholds** tab on the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon) with a status of *Disabled*. In the **Thresholds** tab on the **Interface Properties** page, users can edit the ***Value*** and ***Status*** of the threshold.
  - *Hidden*. The threshold is not applied to all interfaces, and is not monitored by SL1. The threshold does not appear in the **Thresholds** tab on the **Interface Properties** page (Registry > Networks > Interfaces > interface wrench icon).

- ***Unit of Measure***. For all the metrics under ***Bandwidth In*** and ***Bandwidth Out***, you can select the unit of measure. Choices are:
  - bps
  - kbps
  - Mbps
  - Gbps

Settings in Silo.Conf

Every SL1 appliance has a configuration file called **silo.conf**, which contains configuration information about the appliance itself, such as the IP address, licensing information, and directory locations. The default settings in silo.conf are configured automatically when the appliance is installed. The following section describes how you can add additional, non-default settings to silo.conf.

CAUTION: ScienceLogic recommends that you do not edit the values in these files without first consulting ScienceLogic. Incorrect values can severely disrupt platform operations.

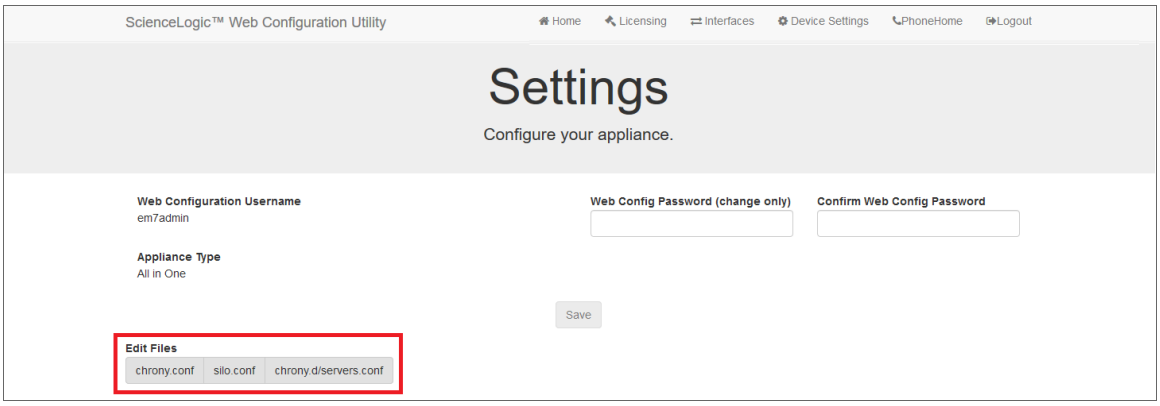
From the **Device Settings** page of the Web Configuration Utility, you can edit the **silo.conf** file and the following files:

- **chrony.conf**. This configuration file contains settings related to the time server (chrony.d) used by SL1.
- **chrony.d/servers.conf**. This configuration file contains additional settings for the various chrony time servers.

NOTE: All settings in these .conf files are case-sensitive.

To edit the silo.conf file:

1. *Log in to the Web Configuration Utility.* The **Configuration Utilities** page appears.
2. Click the **[Device Settings]** button. The **Settings** page appears.



3. In the Edit Files section, click **silo.conf**. The Silo.conf Editor modal page appears:

4. You can add or edit one or more of the following settings:

   - ***store_timeout***. You can edit this setting in the silo.conf file on each Database Server. When the Database Server pulls collected data back from Data Collectors and Message Collectors, each piece of data (called a storage object) must be stored within a set amount of time. The default timeout for a storage object is ten seconds.

     To change the timeout for all storage objects, add the following line to the silo.conf file on the Database Server:

     ```
     store_timeout=xx
     > >
     ```

     where:

     - *xx* is the timeout in seconds.

     If you change this setting (for example, change the value to 30 seconds), you must stop and restart the high frequency, medium frequency, and low frequency data pull processes for the change to be applied.

NOTE: The *store_timeout* setting does not apply to All-In-One Appliances.

   - ***eventmanager***. You can edit this setting in the silo.conf file on each SL1 appliance. You can modify this default setting to allow API events to be processed on a Data Collector. The default configuration is:

     ```
     eventmanager = internal,dynamic,syslog,trap
     ```

     To allow a Data Collector to process API events, change this line to:

     ```
     eventmanager = internal,dynamic,syslog,trap,api
     ```

WARNING: Do not make any other changes to this setting or modify this setting on a Database Server or Data Collector.

- ***report_memory_limit***. You can edit this setting in the silo.conf file on each SL1 appliance that provides the user interface (an Administration Portal, Database Server, or All-In-One Appliance). If *report_memory_limit* is not defined in silo.conf, the default value is three gigabytes (3G). If reports are failing to be generated due to a lack of memory, you can increase this value.

  To increase report memory, add the following line to the [LOCAL] section of silo.conf on each SL1 appliance the provides the user interface for your system. In most cases, this will be the Administration Portal (for distributed system) or the All-In-One Appliance:

  ```
  report_memory_limit=XY
  ```

  where:

  - *X* is a positive integer
  - *Y* represents units. Value can be ***K*** (kilobytes), ***M*** (megabytes), or ***G*** (gigabytes),

  For example, if reports are failing to be generated due to a lack of memory, you could add the following line to silo.conf:

  ```
  report_memory_limit=4G
  ```

NOTE: You should add the *report_memory_limit* option to the silo.conf file on a Database Server only if there are no Administration Portals configured in your system.

NOTE: You must add the same *report_memory_limit* setting to every Administration Portal configured in your system.

- ***use_v1trap_envelope_addr***. You can edit this setting in the silo.conf file on each Data Collectors, Data Collectors that perform message collection, and All-In-One Appliances. In environments where Network Address Translation is performed on SNMP v1 trap messages sent to SL1, you can configure the platform to read the envelope address (the address of the host sending the trap) instead of the agent address (the IP address variable sent as part of the trap). If ***use_v1trap_envelope_addr*** is not defined in silo.conf, SL1 will use the agent address for SNMP v1 trap messages.

  - To use the envelope address instead of the agent address for SNMP v1 trap messages, add the following line to the [LOCAL] section of silo.conf on Data Collectors, Data Collectors that perform message collection, and All-In-One Appliances

  ```
  use_v1trap_envelope_addr=1
  ```

  - To use the agent address for SNMP v1 trap messages, you can either omit the ***use_v1_trap_envelope_addr*** setting or add the following line to the [LOCAL] section of silo.conf on Data Collectors, Data Collectors that perform message collection, and All-In-One Appliances

  ```
  use_v1trap_envelope_addr=0
  ```

- ***disable_itil_compliance***. You can edit this setting in the silo.conf file on each If you enable this setting on an appliance that provides the user interface (an Administration Portal, Database Server, or All-In-One Appliance), the **Ticket Console** page on that appliance will include an option to delete tickets. The option to delete tickets will appear only to users that have been granted the Ticket: Delete access hook and users of type "administrator".

  To enable this setting, add the following line to the [LOCAL] section of silo.conf on the appliance that provides the user interface (Administration Portal, Database Server, or All-In-One Appliance):

  ```
  disable_itil_compliance=1
  ```

- ***suppress_ticket_link***. You can edit this setting in the silo.conf file on each SL1 appliance that provides the user interface (an Administration Portal, Database Server, or All-In-One Appliance). If you enable this setting, automatic notifications that are generated when a ticket is created or updated will not include a hyperlink to the ticket.

  To enable this setting, add the following line to the [LOCAL] section of silo.conf on SL1 appliance that provides the user interface (Administration Portal, Database Server, or All-In-One Appliance):

  ```
  suppress_ticket_link=1
  ```

- ***mailparse_interval***. You can edit this setting in the silo.conf file on each Database Server or All-In-One Appliance. The ***mailparse_interval*** setting defines how frequently the mail parsing process reads email messages from the mailbox. If the mailparse_interval setting is not defined in silo.conf, the default value is 60 seconds. When an email is received by SL1, the mail parsing process on the primary Database Server or All-In-One Appliance reads the email message from the mailbox file and sends it to one of the three processes responsible for acting on that email: the event engine (for events from email), the tickets from email process, or the round-trip email collection process.

  To enable this setting, add the following line to the [LOCAL] section of silo.conf on each Database Server or All-In-One Appliance:

  ```
  mailparse_interval=X
  ```

  where:

  - *X* is the frequency at which the mailbox will be read, in seconds. Valid values are 15 seconds to 60 seconds.

- ***dynamic_collect_num_chunk_workers***. You can edit this setting in the silo.conf file on each Database Server or All-In-One Appliance. This setting represents the number of workers that handle collection requests. SL1 first sorts collection requests into groups by execution environment and sends each group of collection requests (called a chunk) to a worker process. This worker process is called a chunk worker. For each chunk, a chunk worker creates the execution environment and creates a pool of request workers to process the collection requests. The number of chunk workers generally represents the number of PowerPacks that can be processed in parallel. The default value for this parameter is "2".

  To change this setting, add the following line to the [LOCAL] section of silo.conf on each Database Server or All-In-One Appliance:

  ```
  dynamic_collect_num_chunk_workers = [X]
  ```

  where:

  - *X* is the number of chunk workers

NOTE: For more information about using ***dynamic_collect_num_chunk_workers***, see the section on *Tuning the Collector Load Balancing Process in the Silo.Conf File*.

- ***dynamic_collect_num_request_workers***. You can edit this setting in the silo.conf file on each Database Server or All-In-One Appliance. This setting represents the maximum number of request workers in each worker pool and generally represents the number of collections within a PowerPack that can be processed in parallel. The default value for this parameter is "2" or the number of cores on the Data Collector, whichever is greater.

  To change this setting, add the following line to the [LOCAL] section of silo.conf on each Database Server or All-In-One Appliance:

  ```
  dynamic_collect_num_request_workers = [X]
  ```

  where:

  - *X* is the maximum number of request workers in each worker pool.

NOTE: For more information about using ***dynamic_collect_num_request_workers***, see the section on *Tuning the Collector Load Balancing Process in the Silo.Conf File*.

- ***dynamic_collect_request_chunk_size***. You can edit this setting in the silo.conf file on each Database Server or All-In-One Appliance. This setting represents the maximum number of collection requests in a chunk and controls how many collections are processed by a single pool or request workers. The default value for this parameter is "200".

  To change this setting, add the following line to the [LOCAL] section of silo.conf on each Database Server or All-In-One Appliance:

  ```
  dynamic_collect_request_chunk_size = [X]
  ```

  where:

  - *X* is the maximum number of collection requests in a chunk.

NOTE: For more information about using ***dynamic_collect_request_chunk_size***, see the section on *Tuning the Collector Load Balancing Process in the Silo.Conf File*.

- ***read_timeout***. You can edit this setting in the silo.conf file on each Database Server. This setting controls the client read timeout for database connections to the collectors. This setting applies only to the ***Enterprise Database: Collector Config Push*** process (config_push.py) that runs on the primary Database Server.

WARNING: Change this value only if you are instructed to do so by ScienceLogic.

  To change this setting, add the following line to the [CONFIG_PUSH] section of silo.conf on all Database Servers in your system.

  ```
  read_timeout=X
  ```

  where:

  - *X* is the read timeout, in seconds.

- ***wait_timeout***. You can edit this setting in the silo.conf file on each Database Server. This setting controls the server wait timeout for database connections to the collectors. This setting applies only to the ***Enterprise Database: Collector Config Push*** process (config_push.py) that runs on the primary Database Server

WARNING: Change this value only if you are instructed to do so by ScienceLogic.

  To change this setting, add the following line to the [CONFIG_PUSH] section of silo.conf on all Database Servers in your system.

  ```
  wait_timeout=X
  ```

  where:

- *X* is the wait timeout, in seconds.

- ***write_timeout***. You can edit this setting in the silo.conf file on each Database Server. This setting controls the client write timeout for database connections to the collectors. This setting applies only to the ***Enterprise Database: Collector Config Push*** process (config_push.py) that runs on the primary Database Server

WARNING: Change this value only if you are instructed to do so by ScienceLogic.

To change this setting, add the following line to the [CONFIG_PUSH] section of silo.conf on all Database Servers in your system.

```
write_timeout=X
```

where:

- *X* is the write timeout, in seconds.

- ***memory_limit***. You can edit this setting in the silo.conf file on each Database Server. This setting controls the memory limit for the ***Enterprise Database: Collector Config Push*** process. This setting applies only to the ***Enterprise Database: Collector Config Push*** process (config_push.py) that runs on the primary Database Server

WARNING: Change this value only if you are instructed to do so by ScienceLogic.

To change this setting, add the following line to the [CONFIG_PUSH] section of silo.conf on all Database Servers in your system.

```
memory_limit=XY
```

where:

- *X* is a positive integer.
- *Y* represents units. Value can be ***KB*** (kilobytes), ***MB*** (megabytes), or ***GB*** (gigabytes).

- ***message_timeout***. You can edit this setting in the silo.conf file on each Database Server. This setting controls the amount of time the parent ***Enterprise Database: Collector Config Push*** process will wait for a message from a child process before abandoning that process. This setting applies only to the ***Enterprise Database: Collector Config Push*** process (config_push.py) that runs on the primary Database Server

WARNING: Change this value only if you are instructed to do so by ScienceLogic.

To change this setting, add the following line to the [CONFIG_PUSH] section of silo.conf on all Database Servers in your system.

```
message_timeout=X
```

where:

- *X* is the write timeout, in seconds.

- ***shutdown_timeout***. You can edit this setting in the silo.conf file on each Database Server. If the ***Enterprise Database: Collector Config Push*** process is terminated, this setting controls the amount of time the parent configuration process will wait for its child processes to stop before terminating itself and allowing the child processes to be inherited by init. This setting applies only to the ***Enterprise Database: Collector Config Push*** process (config_push.py) that runs on the primary Database Server.

WARNING: Change this value only if you are instructed to do so by ScienceLogic.

To change this setting, add the following line to the [CONFIG_PUSH] section of silo.conf on all Database Servers in your system.

```
shutdown_timeout=X
```

where:

- *X* is the write timeout, in seconds.

- ***[PROC_VIRTUAL_MEM_LIMIT]***. By default, processes in SL1 have a virtual memory limit of 1 GB. You can edit this section in the silo.conf file to overwrite the existing virtual memory limit for a given process in SL1 to ensure that it does not fail by crossing its virtual memory limit.

  To change this setting, add the [PROC_VIRTUAL_MEM_LIMIT] section to the silo.conf file. Below that section heading, specify the process you want to update and the new virtual memory limit for that process. Use the following format for each setting:

  ```
  [process ID]=X
  ```

  where:

  - *[process ID]* is the ID of the process you want to update, as found in master.system_settings_procs.aid
  - *X* is the new virtual memory limit, in bytes

  For example, if you wanted to update a process with an ID of "12" with a new 2 GB memory limit, you would write the following under [PROC_VIRTUAL_MEM_LIMIT]:

  ```
  12=2147483648
  ```

- ***[ADHOC_REPORT_IN_BATCH]***. Adhoc reports are processed in a batch process. You can edit this section in the silo.conf file to overwrite the default timing values for certain adhoc reporting settings.

  To change these settings, under the [ADHOC_REPORT_IN_BATCH] section heading in the silo.conf file, specify the time value (in seconds) for each setting. The following settings are included in the [ADHOC_REPORT_IN_BATCH] section:

  - *report_execution_delay*. This setting controls the amount of time between when a report is scheduled to start running and when it actually begins running. Its default value is 10.
  - *ajax_start_delay*. This setting controls the amount of time elapsed before jQuery triggers the ajaxStart event. Its default value is 20.
  - *ajax_stop_time*. This setting controls the amount of time elapsed before jQuery triggers the ajaxStop event after all AJAX requests have completed. Its default value is 1800.
  - *ajax_frequency*. This setting controls the frequency with which jQuery fires AJAX requests. Its default value is 10.
  - *ajax_frequency_decreased_after*. This setting controls the amount of time elapsed after which jQuery will fire AJAX requests less frequently than in the *ajax_frequency* setting. Its default value is 300.
  - *ajax_decreased_frequency*. This setting controls the decreased frequency with which jQuery fires AJAX requests after the amount of time listed in the *ajax_frequency_decreased_after* setting has elapsed. Its default value is 60.
  - *report_fail_check_time*. This setting controls the amount of time elapsed after which a running report will be considered to have failed. Its default value is 10800.
  - *auto_page_refresh*. This setting controls the amount of time elapsed after which the **Scheduled Report Jobs** page (Report > Create Report > Scheduled Job / Report Archive) automatically refreshes. Its default value is 10.
  - *about_to_start_time_check*. This setting controls the amount of time before a report job is scheduled to start that it will be labeled as "About to start" on the **Scheduled Report Jobs** page (Report > Create Report > Scheduled Job / Report Archive). Its default value is 30.
  - *time_unit*. This setting controls the unit of time measurement for the adhoc report settings. Its default value is "second".
  - *ui_php_timeout*. This setting controls the amount of time elapsed after which an inactive SL1 reports session will time out. Its default value is 1800.

5. To save your changes, click **Save** and then close the modal window.

NOTE: All changes to the silo.conf file are logged in the SL1Database Server.

Disabling the User Interface on a Database Server

Database Servers are automatically configured to provide the user interface. If your SL1 system includes an Administration Portal, you might want to disable the user interface capability on your Database Server(s). Perform the following steps to disable the user interface capability on a Database Server:

NOTE: To complete these steps, you must be familiar with how to edit a file using the vi text editor. If you need assistance with these steps, please contact ScienceLogic Support.

1. Log in to the console of the Database Server or use SSH to access the server as the ***em7admin*** user with the appropriate password.
2. Execute the following command to open the firewall rules file:

```
sudo vi /etc/siteconfig/firewalld-rich-rules.siteconfig
```

3. Add following lines:

```
rule port port="443" protocol="tcp" reject
rule port port="80" protocol="tcp" reject
```

4. Save the file and exit the vi editor.
5. Execute the following commands to update and restart the firewall:

```
sudo /opt/em7/share/scripts/update-firewalld-conf.py
```

Chapter 3

Collector Groups

Overview

A Collector Group is a group of SL1 Data Collectors. Data Collectors retrieve data from managed devices and applications. This collection occurs during initial discovery, during nightly updates, and in response to policies defined for each managed device. The collected data is used to trigger events, display data in the user interface, and generate graphs and reports.

Grouping multiple Data Collectors allows you to:

- Create a load-balanced collection system, where you can manage more devices without loss of performance. At any given time, the Data Collector with the lightest load manages the next discovered device.
- Optionally, create a redundant, high-availability system that minimizes downtime should a failure occur. If a Data Collector fails, one or more Collection servers in the Collector Group will handle collection until the problem is solved.

This chapter will describe how to create and manage Collector Groups.

NOTE: If you are using a SL1 All-In-One Appliance, most of the sections in this chapter do not apply to your system. For an All-In-One Appliance, a single, default Collector Group is included with the appliance; you cannot create any additional Collector Groups. However, you can *view information about the default Collector Group*. You can also *create a virtual Collector Group*, for data storage only. However, the other tasks described in this section do not apply to an All-In-One Appliance.

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

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

This chapter includes the following topics:

Installing, Configuring, and Licensing Data Collectors

Before you can create a Collector Group, you must install and license at least one Data Collector. For details on installation and licensing of a Data Collector, see the ***Installation*** manual.

After you have successfully installed, configured, and licensed a Data Collector, the platform automatically adds information about the Data Collector to the Database Server.

Technical Information About Data Collectors

You might find the following technical information about Data Collectors helpful when creating Collector Groups.

Duplicate IP Addresses

A single Collector Group ***cannot*** include multiple devices that use the same Admin Primary IP Address (this is the IP address the platform uses to communicate with a device). If a single Collector Group includes multiple devices that use the same Primary IP Address or use the same Secondary IP Address, the platform will generate an event. Best practice is to ensure that within a single Collector Group, all IP addresses on all devices are unique.

- During initial discovery, if a device is discovered with the same Admin Primary IP Address as a previously discovered device in the Collector Group, the later discovered device will appear in the discovery log, but will not be modeled in the platform. That is, the device will not be assigned a device ID and will not be created in the platform. The platform will generate an event specifying that a duplicate Admin Primary IP was discovered within the Collector Group.
- If you try to assign a device to a Collector Group, and the device's Admin Primary IP Address already exists in the Collector Group, the platform will display an error message, and the device will not be aligned with the Collector Group.

Open Ports

By default, Data Collectors accept connections only to the following ports:

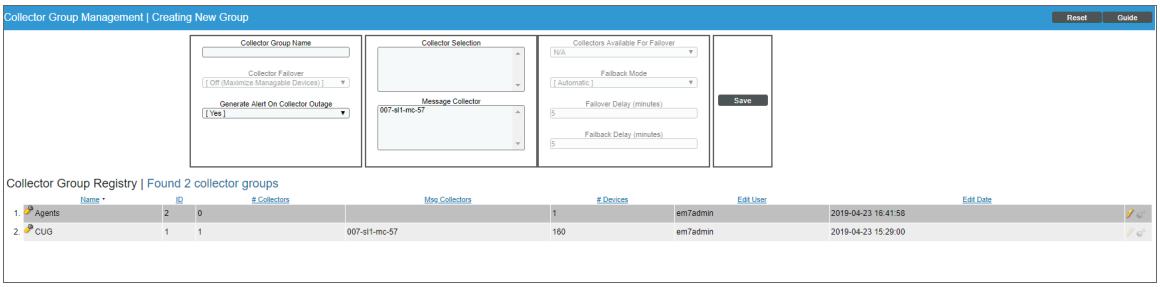
- TCP 22 (SSH)
- TCP 53 (DNS)
- TCP 123 (NTP)
- UDP 161 (SNMP)
- UDP 162 (Inbound SNMP Trap)
- UDP 514 (Inbound Syslog)
- TCP 7700 (Web Configuration Utility)
- TCP 7707 (one-way communication from the Database Server)

For increased security, all other ports are closed.

Viewing the List of Collector Groups

To view the list of already-defined Collector Groups in your SL1 system:

1. Go to the **Collector Group Management** page (System > Settings > Collector Groups).



2. The **Collector Group Registry** pane displays a list of all Collector Groups in your SL1 system. For each Collector Group, the **Collector Group Management** page displays the following:

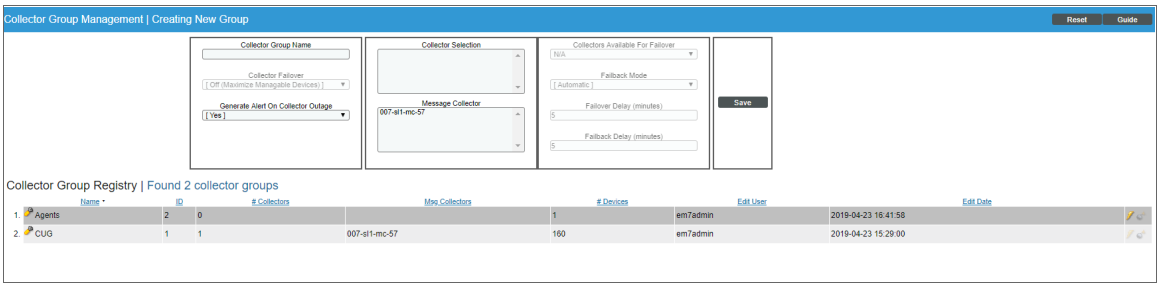
   - ***Name***. Name of the Collector Group.
   - ***ID***. Unique numeric identifier automatically assigned by SL1 to each Collector Group.
   - ***# Collectors***. Number of Data Collectors in the Collector Group.
   - ***Msg Collector***. Name of the Message Collector(s) (if any) associated with the Collector Group.
   - ***# Devices***. Number of devices currently using the Collector Group for data collection.
   - ***Edit User***. User who created or last edited the Collector Group.
   - ***Edit Date***. Date and time the Collector Group was created or last edited.

Creating a Collector Group

You can group multiple Data Collectors into a Collector Group. Depending on the number of Data Collectors in your SL1 system, you can define one or more Collector Groups. Each Collector Group must include at least one Data Collector.

To define a new Collector Group:

1. Go to the **Collector Group Management** page (System > Settings > Collector Groups).
2. In the **Collector Group Management** page, click the **[Reset]** button to clear the values from the fields in the top pane.



3. Go to the top pane and enter values in the following fields:

- ***Collector Group Name***. Name of the Collector Group.
- ***Collector Failover***. Specifies whether you want to maximize the number of devices to be managed or whether you want to maximize reliability. Your choices are:
  - *Off (Maximize Manageable Devices)*. The Collector Group will be load-balanced only. At any given time, the Data Collector with the lightest load handles the next discovered device. If a Data Collector fails, no data will be collected from the devices aligned with the failed Data Collector until the failure is fixed.
  - *On (Maximize Reliability)*. The Collector Group will be load-balanced and configured as a high-availability system that minimizes downtime. If one or more Data Collectors should fail, the tasks from the failed Data Collector will be distributed among the other Data Collectors in the Collector Group.
- ***Generate Alert on Collector Outage***. Specifies whether or not the platform should generate an event if a Data Collector has an outage.
- ***Collector Selection***. Displays a list of available Data Collectors.
  - To assign an available Data Collector server to the Collector Group, simply highlight it. You can assign one or more Data Collectors to a Collector Group.
  - To assign multiple Data Collectors to the Collector Group, hold down the **<Ctrl>** key and click multiple Data Collectors.
- ***Message Collector***. Displays a list of available Message Collectors.
  - To assign an available Message Collector to the Collector Group, simply highlight it. You can assign one or more Message Collectors to a Collector Group.
  - To assign multiple Message Collectors to the Collector Group, hold down the **<Ctrl>** key and click multiple Message Collectors.
  - Note that a single Message Collector can be used by multiple Collector Groups.

NOTE: When you align a single Message Collector with multiple Collector Groups, the single Message Collector might then be aligned with two devices (each in a separate Collector Group) that use the same primary IP address or the same secondary IP address. If this happens, SL1 will generate an event.

- ***Collectors Available for Failover***. Applies only if you selected "On (Maximize Reliability)" in the ***Collector Failover*** field. Specifies the minimum number of Data Collectors that must be available (i.e. with a status of "Available [0]") before a Data Collector failover may occur.
  - For collector groups with only two Data Collectors, this field will contain the value "1 collector".
  - For collector groups with more than two Data Collectors, the field will contain values from a minimum of one half of the total number of Data Collectors up to a maximum of one less than the total number of Data Collectors.
  - For example, for a collector group with eight Data Collectors, the possible values in this field would be 4, 5, 6, and 7.

- SL1 will never automatically increase the maximum number of Data Collectors that can fail in a Collector Group. For example, suppose you have a collector group with three Data Collectors. Suppose ***Collectors Available For Failover*** field is set to "2". If you add a fourth Data Collector to the collector group, SL1 will automatically set the ***Collectors Available For Failover*** field to to "3" to maintain the maximum number of Data Collectors that can fail as "one". However, you can override this automatic setting by manually changing the value in the ***Collectors Available For Failover*** field.

CAUTION: If the number of available Data Collectors is less than the value in the ***Collectors Available For Failover*** field, SL1 will not failover within the Collector Group. ***SL1 will not collect any data from the devices aligned with the failed Data Collector(s) until the failure is fixed on enough Data Collector(s) to equal the value in the Collectors Available For Failover field.*** EM7 will generate a critical event.

- ***Failback Mode***. Applies only if you selected *On (Maximize Reliability)* in the ***Collector Failover*** field. Specifies how you want collection to behave when the outage is fixed. You can specify one of the following:
  - *Automatic*. After the failed Data Collector is restored, SL1 will automatically redistribute data-collection tasks among the Collector Group, including the previously failed Data Collector.
  - *Manual*. After the failed Data Collector is restored, you will manually prompt Data Collector to redistribute data-collection tasks by clicking the lightning bolt icon ( ) for the Collector Group.
- ***Failover Delay (minutes)***. Applies only if you selected *On (Maximize Reliability)* in the ***Collector Failover*** field. Specifies the number of minutes SL1 should wait after the outage of a Data Collector before redistributing the data-collection tasks among the other Data Collectors in the group. During this time, data will not be collected from the devices aligned with the failed Data Collector(s). The default minimum value for this field is 5 minutes.
- ***Failback Delay (minutes)***. Applies only if you selected *On (Maximize Reliability)* in the ***Collector Failover*** field and *Automatic* in the ***Failback Mode*** field. Specifies the number of minutes SL1 should wait after the failed Data Collector is restored before redistributing data-collection tasks among the Collector Group, including the previously failed Data Collector. The default minimum value for this field is 5 minutes.

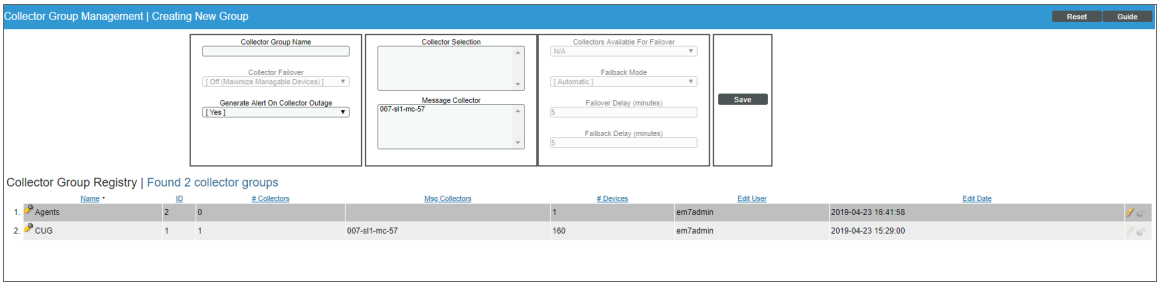
4. Click the **[Save]** button to save the new Collector Group.
5. To assign devices to the Collector group, see the section on *aligning single devices with a Collector Group* and the section on *aligning a device group with a Collector Group*.

Editing a Collector Group

From the **Collector Group Management** page, you can edit an existing Collector Group. You can add or remove Data Collectors and change the configuration from load-balanced to failover (high availability). To edit a Collector Group:

1. Go to the **Collector Group Management** page (System > Settings > Collector Groups).

2. In the **Collector Group Management** page, go to the **Collector Group Registry** pane at the bottom of the page.



3. Find the Collector Group you want to edit. Click its wrench icon ( ).
4. The fields in the top pane are populated with values from the selected Collector Group. You can edit one or more of the fields. For a description of each field, see the section on *Creating a Collector Group*.
5. Click the **[Save]** button to save any changes to the Collector Group.

Collector Groups and Load Balancing

To perform initial discovery, SL1 uses a single, selected Data Collector from the Collector Group. This allows you to easily troubleshoot discovery if there are any problems.

After each discovered device is modeled (that is, after SL1 assigns a device ID and creates the device in the database), SL1 distributes devices among the Data Collectors in the Collector Group. The newest device is assigned to the Data Collector currently managing the lightest load.

This process is known as ***Collector load balancing***, and it ensures that the work performed by the Dynamic Applications aligned to the devices is evenly distributed across the Data Collectors in the Collector Group.

SL1 performs Collector load balancing in the following circumstances:

- A new Data Collector is added to a Collector Group.
- New devices are discovered
- Failover or failback occurs within a Collector Group (if failover is enabled).
- A user clicks the lightning bolt icon ( ) for a Collector Group to manually force redistribution.

NOTE: The lightning bolt icon ( ) appears only for Collector Groups that contain more than one Data Collector. For Collector Groups with only one Data Collector, this icon is grayed out. This icon does not appear for All-In-One Appliances.

When all of the devices in a Collector Group are redistributed, SL1 will assign the devices to Data Collectors so that all Data Collectors in the collector group will spend approximately the same amount of time collecting data from devices.

Collector load balancing uses two metrics:

- ***Device Rating***. The total elapsed time per hour that SL1 has spent collecting data for the device.
- ***Collector Load***. The sum of the device ratings for all of the devices assigned to a collector.

SL1 peforms the following steps during Collector load balancing:

1. Searches for all devices that are not yet assigned to a Collector Group.
2. Determines the load on each Data Collector by calculating the device rating for each device on a Data Collector and then summing the device ratings.
3. Determines the number of new devices (less than one day old) and old devices on each Data Collector.
4. On each Data Collector, calculates the average device rating for old devices (sum of the device ratings for all old devices divided by the number of old devices). If there are no old devices, sets the average device rating to "1" (one).
5. On each Data Collector, assigns the average device rating to all new devices (devices less than one day old).
6. Assigns each unassigned device (either devices that are not yet assigned or devices on a failed Data Collector) to the Data Collector with the lightest load. Add each newly assigned device rating to the total load for the Data Collector.

Tuning Collector Groups in the silo.conf File

With the addition of execution environments to SL1, SL1 sorts data collections in to a two-process-pool model.

SL1 sorts collection requests into groups by execution environment. These groups of collection requests are called "chunks". Each chunk contains a maximum of 200 collection requests, all of which use the same execution environment. SL1 sends each chunk to a chunk worker.

The chunk worker determines the appropriate execution environment for the chunk, deploys the execution environment, and starts a pool of request workers in the execution environment.

The request workers then process the actual collection requests contained in the chunks and perform the actual data collection.

> **NOTE:** For more information about ScienceLogic Libraries and execution environments, see the manual ***ScienceLogic Libraries and Execution Environments***.

The following settings are available in the master.system_settings_core database table for tuning globally in a stack, or *in the Silo.Conf file* for tuning locally on a single Data Collector:

Parameter Name	Description	Runtime Default
dynamic_ collect_num_ chunk_ workers	The number of chunk workers. In general, this value controls the number of PowerPacks that can be processed in parallel.	2
dynamic_ collect_num_ request_ workers	The maximum number of request workers in each worker pool. In general, this value controls the number of collections within a PowerPack that can be processed in parallel.	"2" or the number of cores on the Data Collector, whichever is greater
dynamic_ collect_ request_ chunk_size	The maximum number of collection requests in a chunk. This value controls how many collections are processed by each pool of requests workers.	200

NOTE: The database values for these parameters are "Null" by default, which specifies that SL1 should use the runtime defaults.

The maximum total number of worker processes used during a scheduled collection is generally `dynamic_ collect_num_chunk_workers X dynamic_collect_num_request_workers`.

There might be circumstances where adjustment is necessary to improve the performance of collection.

Example 1: Additional Environments Required

You might need to adjust the values of the collection processes when scheduled collection requires more than two environments.

Because the default number of chunk workers is "2", SL1 can simultaneously process chunks of collection requests for a maximum of two virtual environments. If the collection requests require more than two virtual environments, you can increase parallelism by setting `dynamic_collect_num_chunk_workers` to match the number of environments.

If you increase `dynamic_collect_num_chunk_workers`, you might want to decrease `dynamic_collect_num_ request_workers` to avoid performance problems caused by too many request workers.

If you cannot increase `dynamic_collect_num_chunk_workers` because doing so would result in too many request workers, you can decrease `dynamic_collect_request_chunk_size` to give collection requests for each environment a "fairer share" of the chunk workers.

NOTE: Smaller chunk sizes require more resources to establish the virtual environments and establish more polls of request workers to process the chunks. Conversely, if you want to use fewer resources for establishing virtual environments and creating pools of request worker pools, and you want to use more resources for collection itself, increasing `dynamic_collect_request_chunk_size` allows more collection requests to be processed by each pool of request workers.

Example 2: Input/Output Bound Collections

You might need to adjust the values of the collection processes when collection requests are input/output (I/O) bound with relatively large latencies.

In this scenario, you can increase `dynamic_collect_num_request_workers` to improve parallelism. If you increase `dynamic_collect_num_request_workers`, you might want to decrease `dynamic_collect_num_chunk_workers` to avoid performance problems caused by too many request workers.

CAUTION: Increasing the number of collection processes will increase CPU and memory utilization on the Data Collector, so be careful when increasing the values dramatically.

Before adjusting `dynamic_collect_num_request_workers`, you need to know the following information:

- The number of CPU cores in the Data Collector
- The current CPU utilization of Data Collector
- The current memory utilization of Data Collector

Start by setting `dynamic_collect_num_request_workers` to equal the number of CPUs plus 50%. For example: with 8 cores, start by setting `dynamic_collect_num_request_workers` to 12. If that is insufficient, you can then try 16, 20, 24, and so forth.

If data collections are terminating early, it means that collections are not completed within the 15-minute limit. If this is the case, wait 30 minutes to see results after adjusting the collection values.

Collector Affinity

Collector Affinity specifies the Data Collectors that are allowed to run collection for Dynamic Applications aligned to component devices. You can define Collector Affinity for each Dynamic Application. Choices are:

- ***Default***. If the Dynamic Application is auto-aligned to a component device during discovery, then the Data Collector assigned to the root device will collect data for this Dynamic Application as well. For devices that are not component devices, the Data Collector assigned to the device running the Dynamic Application will collect data for the Dynamic Application.

- ***Root Device Collector***. The Data Collector assigned to the root device will collect data for the Dynamic Application. This guarantees that Dynamic Applications for an entire DCM tree will be collected by a single Data Collector. You might select this option if:
    - The Dynamic Application has a cache dependency with one or more other Dynamic Applications.
    - You are unable to collect data for devices and Dynamic Applications within the same Device Component Map on multiple Data Collectors in a collector group.
    - If the Dynamic Application will consume cache produced by a Dynamic Application aligned to a non-root device (for instance, a cluster device).
- ***Assigned Collector***. The Dynamic Application will use the Data Collector assigned to the device running the Dynamic Application. This allows Dynamic Applications that are auto-aligned to component devices during discovery to run on multiple Data Collectors. You might select this option if:
    - The Dynamic Application has no cache dependencies with any other Dynamic Applications.
    - You want the Dynamic Application to be able to make parallel data requests across multiple Data Collectors in a collector group.
    - The Dynamic Application can be aligned using mechanisms other than auto-alignment during discovery (for instance, manual alignment or alignment via Device Class Templates or Run Book Actions).

Failover for Collector Groups for Component Devices

If you specified ***Default*** or ***Root Device Collector*** for Dynamic Applications, and the single Data Collector in the Collector Group for component devices fails, users must create a new Collector Group with a single Data Collector and manually move the devices from the failed Collector Group to the new Collector Group. For details on manually moving devices to a new Collector Group, see the section on *Changing the Collector Group for One or More Devices*.

Collector Groups for Merged Devices

You can merge a physical device and a component device. There are two ways to do this:

- From the Actions menu in the **Device Properties** page (Devices> Device Manager > wrench icon) for either the physical device or the component device.
- From the ***Actions*** menu in the **Device Manager** page (Devices > Device Manager), select *Merge Devices* to merge devices in bulk.

You can unmerge a component device from a physical device. You can do this in two ways:

- From the ***Actions*** menu in the **Device Properties** page (Devices> Device Manager > wrench icon) for either the physical device or the component device, , select *Unmerge Devices* to unmerge devices.
- From the ***Actions*** menu in the the **Device Manager** page Devices > Device Manager), select *Unmerge Devices* to unmerge devices in bulk.

When you merge a physical device and a component device, the device record for the component device is no longer displayed in the user interface; the device record for the physical device is displayed in user interface pages that previously displayed the component device. For example, the physical device is displayed instead of the component device in the **Device Components** page (Devices > Device Components) and the **Component Map** page (Device Component Map). All existing and future data for both devices will be associated with the physical device.

If you manually merge a component device with a physical device, SL1 allows data for the merged component device and data from the physical device to be collected on different Data Collectors. Data that was aligned with the component device can be collected by the Collector Group for its root device. Data aligned with the physical device can be collected by a different Collector Group.

NOTE: You can merge a component device with only one physical device.

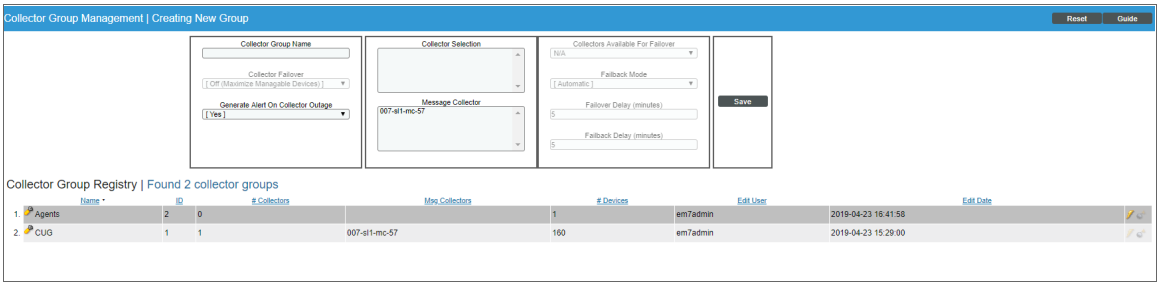
Creating a Collector Group for Data Storage Only

From the **Collector Group Management** page, you can create a ***Virtual Collector Group*** that serves as a storage area for all historical data from decommissioned devices.

The Virtual Collector Group will store all existing historical data from all aligned devices, but will not perform collection on those devices. The Virtual Collector Group will not contain any Data Collectors or any Message Collectors. ***SL1 will stop collecting data from devices aligned with a Virtual Collector Group***.

To define a Virtual Collector Group:

1. Go to the **Collector Group Management** page (System > Settings > Collector Groups).



2. In the **Collector Group Management** page, click the **[Reset]** button to clear values from the fields in the top pane.
3. Go to the top pane and enter a name for the virtual Collector Group in the ***Collector Group Name*** field.
4. Leave all other fields set to the default values. Do not include any Data Collectors or Message Collectors in the Collector Group.
5. Click the **[Save]** button to save the new Collector Group.
6. To assign devices to the virtual Collector Group, see the section on *aligning single devices with a Collector Group* and the section on *aligning a device group with a Collector Group*.

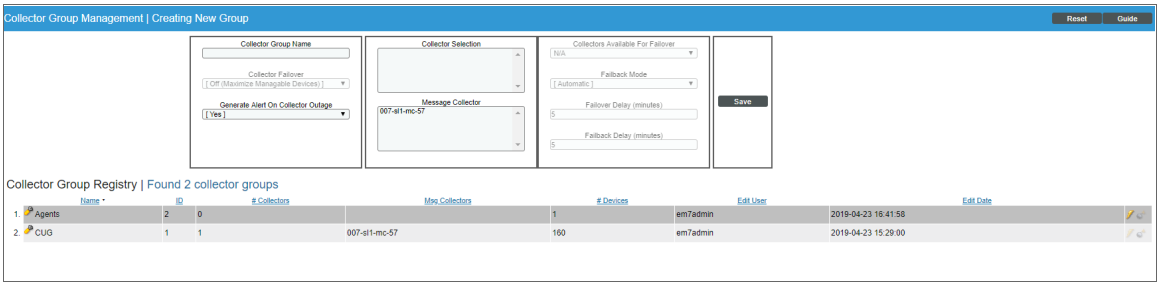
Deleting a Collector Group

From the **Collector Group Management** page, you can delete a Collector Group. When you delete a Collector Group, those Data Collectors become available for use in other Collector Groups.

NOTE: Before you can delete a Collector Group, you must move all aligned devices to another Collector Group. For details on how to do this, see the section *Changing the Collector Group for One or More Devices*.

To delete a Collector Group:

1. Go to the **Collector Group Management** page (System > Settings > Collector Groups).



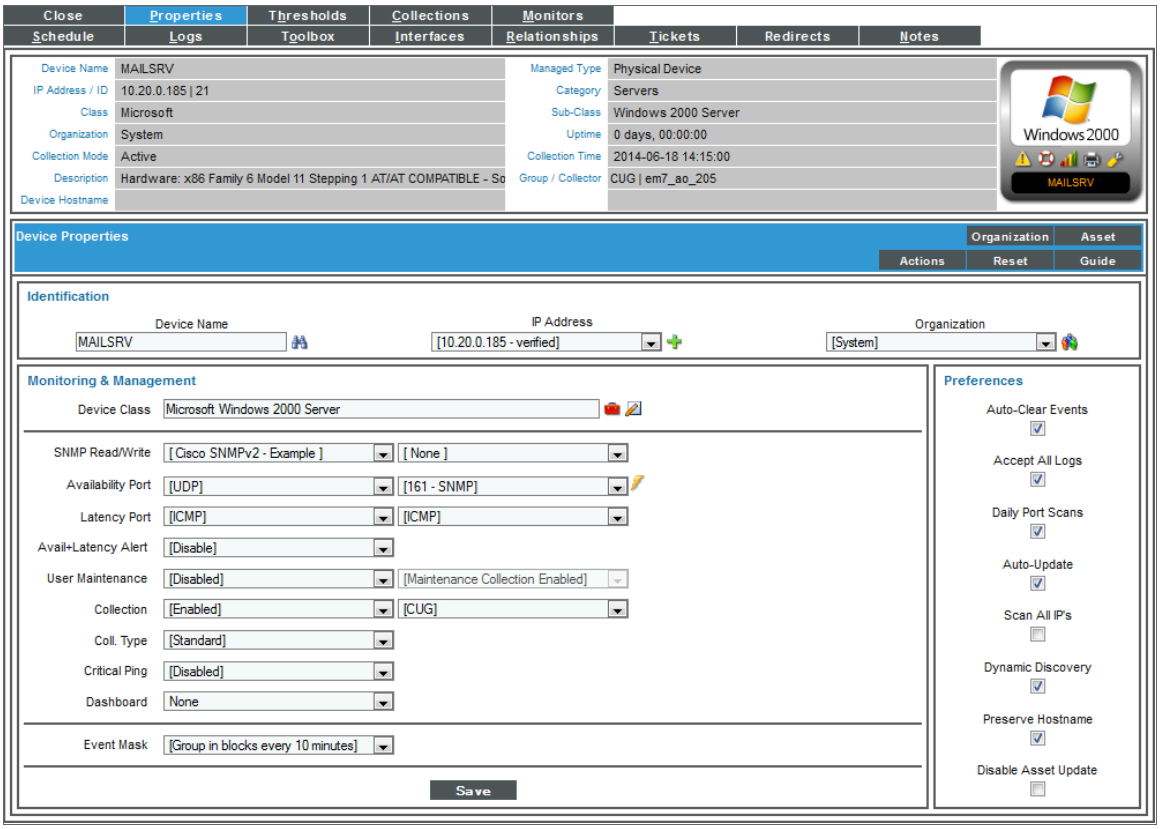
2. In the **Collector Group Management** page, go to the **Collector Group Registry** pane at the bottom of the page.
3. Find the Collector Group you want to delete. Click its bomb icon ( ).

Aligning the Collector Group for A Single Device

After you have defined a Collector Group, you can align devices with that Collector Group. To assign a Collector Group to a device:

1. Go to the **Device Manager** page (Devices > Device Manager).

2. In the **Device Manager** page, find the device you want to edit. Click its wrench icon ( ). The **Device Properties** page appears:



3. In the **Device Properties** page, you can select a Collector Group from the ***Collection*** fields.
4. Click the **[Save]** button to save the change to the device.

Aligning the Collector Group in a Device Template

You can specify a Collector Group in a device template. Then, when you apply the device template to a device, either through discovery or when you apply the device template to a device group or selection of devices, the specified Collector Group is automatically associated with the device(s). Optionally, you can later edit the Collector Group for each device.

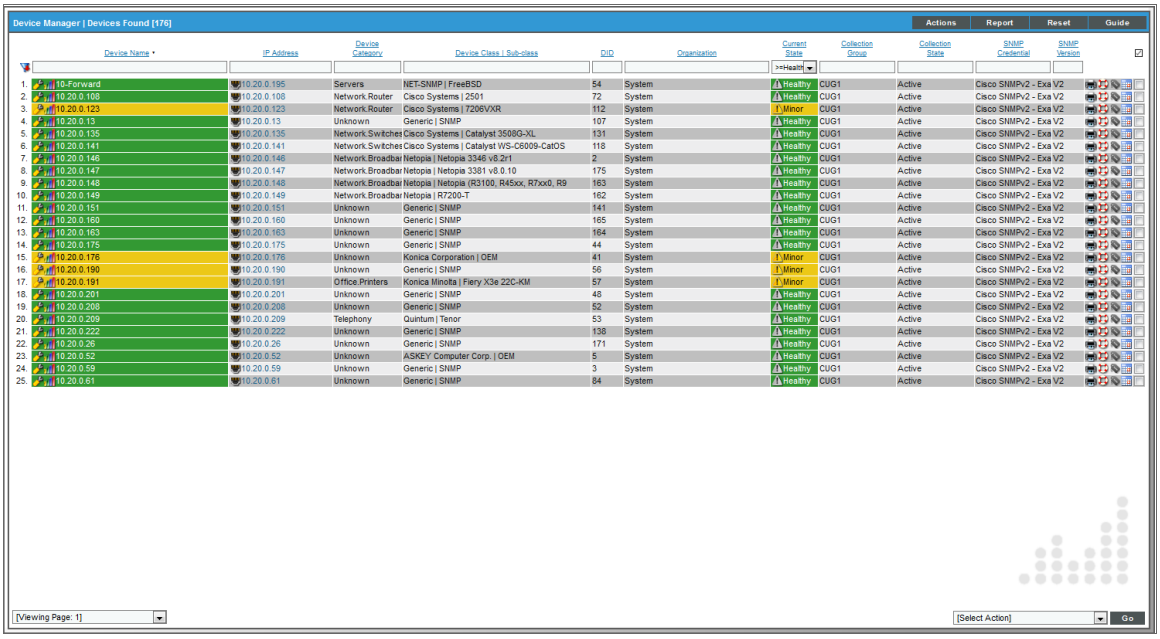
For more details on device templates and device groups, see the manual ***Device Groups and Device Templates***.

Changing the Collector Group for One or More Devices

You can change the Collector Group for multiple devices simultaneously. This is helpful if you want to reorganize devices or Collector Groups. If you want to delete a Collector Group, you first must first move each aligned device to another Collector Group. In this situation, you might want to change the Collector Group for multiple devices simultaneously.

To change the Collector Group for multiple device simultaneously:

1. Go to the **Device Manager** page (Devices > Device Manager).



2. In the **Device Manager** page, click on the heading for the ***Collection Group*** column to sort the list of devices by Collector Group.
3. Select the checkbox for each device that you want to move to a different Collector Group.
4. In the ***Select Action*** field (in the lower right), go to ***Change Collector Group*** and select a Collector Group.
5. Click the **[Go]** button. The selected devices will now be aligned with the selected Collector Group.

Managing the Host Files for a Collector Group

The **Host File Entry Manager** page allows you to edit and manage host files for all of your Data Collectors from a single page in the SL1 system. When you create or edit an entry in the **Host File Entry Manager** page, SL1 automatically sends an update to every Data Collector in the specified Collector Group.

The **Host File Entry Manager** page is helpful when:

- The SL1 system does not reside in the end-customer's domain
- The SL1 system does not have line-of-sight to an end-customer's DNS service
- A customer's DNS service cannot resolve a host name for a device that the SL1 system monitors

For details, see the section on *Managing Host Files*.

Processes for Collector Groups

For troubleshooting and debugging purposes, you might find it helpful to understand the ScienceLogic processes that affect a Collector Group.

NOTE: You can view the list of all processes and details for each process in the **Process Manager** page (System > Settings > Admin Processes).

- The ***Enterprise Database: Collector Task Manager process (em7_ctaskman)*** process distributes devices between Data Collectors in a Collector Group, to load-balance the collection tasks. The process runs every 60 seconds and also checks the license on each Data Collector. The Enterprise Database: Collector Task Manager process (em7_ctaskman.py) redistributes devices between collectors when:
  - A Collector Group is created.
  - A new Data Collector is added to a Collector Group.
  - Failover or failback occurs within a Collector Group.
  - A user clicks on the lightning bolt icon () for a Collector Group, to manually force redistribution.
- ***The Enterprise Database: Collector Data Pull processes*** retrieves information from each Data Collector in a Collector Group. The process pulls data from the in_storage tables on each Data Collector. The retrieved information is stored in the Database Server.
  - *Enterprise Database: Collector Data Pull, High F (em7_hfpulld)*. Retrieves data from each Data Collector every 15 seconds (configurable).
  - *Enterprise Database: Collector Data Pull, Low F (em7_lfpulld)*. Retrieves data from each Data Collector every five minutes.
  - *Enterprise Database: Collector Data Pull, Medium (em7_mfpulld)*. Retrieves data from each Data Collector every 60 seconds.
- ***The Enterprise Database: Collector Config Push process (config_push.py)*** updates each Data Collector with information on system configuration, configuration of Dynamic Applications, and any new or changed policies. This process runs once every 60 seconds and checks for differences between the configuration tables on the Database Server and the configuration tables on each Data Collector. The list of tables to be synchronized is stored in master.definitions_collector_config_tables on the Database Server.
- ***Asynchronous Processes*** (for example, discovery or programs run from the **Device Toolbox** page). Asynchronous processes need to be run immediately and cannot wait until the Enterprise Database: Collector Config Push process (config_push.py) runs and tells the Data Collector to run the asynchronous process. Therefore, SL1 uses a stored procedure and the EM7 Core: Task Manager process (em7) to trigger asynchronous processes on both the Database Server and Data Collector.

- If a user requests an asynchronous process, a stored procedure on the Database Server inserts a new row in the table master_logs.spool_process on the Database Server.
- Every three seconds, the EM7 Core: Task Manager process (proc_mgr.py) checks the table master_logs.spool_process on the Database Server for new rows.
- If the asynchronous process needs to be started on a Data Collector, a stored procedure on the Database Server inserts the same row into the table master_logs.spool_process on the Data Collector.
- Every three seconds, the EM7 Core: Task Manager process (em7) checks the table master_logs.spool_process on the Data Collector for new rows.
- If the EM7 Core: Task Manager process (em7) on the Data Collector finds a new row, the specified asynchronous process is executed on the Data Collector.

Chapter 4

Daily Health Tasks

Overview

The tasks in this chapter help you monitor the health of your SL1 system. You can perform these tasks daily (or more frequently, if you require) to gather information about the overall status of your SL1 system.

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

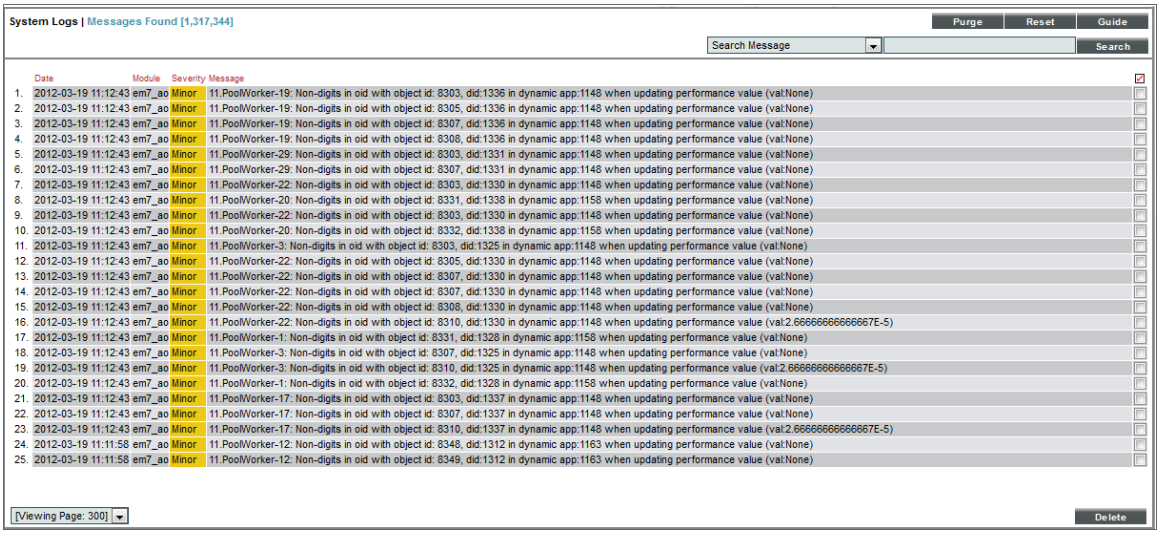
- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon ( ).

This chapter includes the following topics:

Monitoring System Events

To view the entries in the **System Logs**:

1. Go to the **System Logs** page (System > Monitor > System Logs).



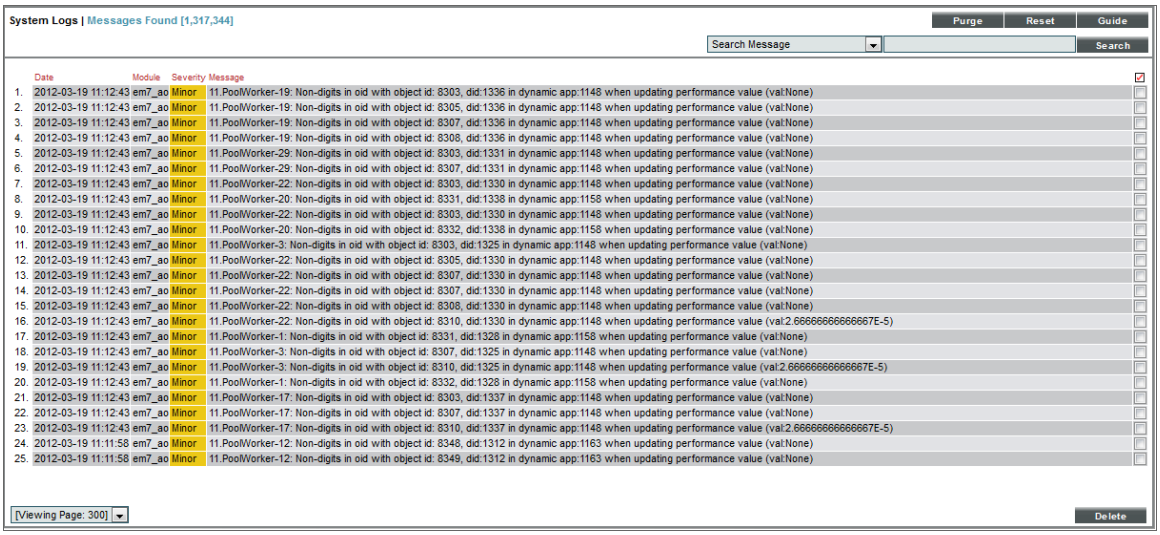
2. In the **System Logs** page, pay special attention to any log entry tagged as Critical or Major. These entries might require additional diagnostics.
3. For each log entry, the **System Logs** page displays:

   - ***Date***. Date and time the log entry was generated.
   - ***Module***. Name of the appliance that generated the log entry.
   - ***Severity***. Specifies the severity assigned to the log entry. The choices are:
     - Healthy
     - Notice
     - Minor
     - Major
     - Critical
   - ***Message***. Descriptive text included in the log entry.

Searching the System Logs

When viewing the **System Logs**, you might want to sort the entries by date or by log message. This is helpful when you want to view information about a specific occurrence of a system event. To search the **System Logs**:

1. Go to the **System Logs** page (System > Monitor > System Logs).



2. The search fields at the top of the **System Logs** page allows you to search for log entries by message, date, or module.

   - ***Search where.*** Specifies the parameter you want to search by. You can select from the following:

     - *Search Message*. Searches all log entries for those that match the text that you enter in the regular expression field.
     - *Search Module ID*. Searches all log entries for those that have the same module ID text as that entered in the regular expression field.
     - *Search Date = (Y-m-d H:i:s)*. Searches all log entries for those that have a date and time that is equal to the date entered in the regular expression field.
     - *Search Date > (Y-m-d H:i:s)*. Searches all log entries for those that have a date and time that is later than the date entered in the regular expression field.
     - *Search Date Like (Y-m-d H:i:s)*. Searches all log entries for those that have a date and time that is similar to the date entered in the regular expression field.
     - *Search Date Like != (Y-m-d H:i:s)*. Searches all log entries for those that have a date and time that is **not** similar to the date entered in the regular expression field.

   - ***regular expression***. In this field you manually enter the text to search for. You can use the following special characters in this field:

     - * Match zero or more characters preceding the asterisk. For example:

       "dell*" would match "dell", "dell2650", "dell7250" and "dell1700N".

       "*dell*" would match "mydell", "dell", "dell2650", "dell7250" and "dell1700N".

     - % Match zero or more characters preceding the asterisk. This special character behaves in the same way as the asterisk.

3. When you click the **[Search]** button, the **System Logs** page will be refreshed and will display only the log entries that match the search parameters.

Deleting Entries from the System Logs

To save space, you might want to remove some or all log entries from the system log.

There are two ways to delete entries from the **System Logs** page:

1. Go to the **System Logs** page (System > Monitor > System Logs).
2. In the **System Logs** page, click the **[Purge]** button to delete all entries from the System Logs.

Or:

1. Go to the **System Logs** page (System > Monitor > System Logs).
2. In the **System Logs** page, highlight each entry you want to delete. To select multiple entries, right-click while holding down the **[<Ctrl>]** key.
3. Click the **[Delete]** button to delete all the selected entries from the System Logs.

Monitoring System Processes

The **System Processes** page (System > Monitor > Admin System Processes) allows you to view read-only information about the execution of SL1's system processes. System Processes gather, manipulate, and publish the data used in SL1. These system processes can be configured and debugged in the **Process Manager** page (System > Settings > Admin Processes).

Viewing the List of System Processes

To view the list of system processes for all appliances:

1. Go to the **System Processes** page (System > Monitor > Admin System Processes).
2. The **System Processes** page displays the following for each process:

    - ***Appliance***. The appliance where the process ran or is currently running. This field will contain the device name of the appliance.
    - ***Process***. Name of the process.
    - ***ID***. Unique numeric ID automatically assigned to the process by SL1.
    - ***Start Time***. Date and time at which the process started running.
    - ***End Time***. Date and time at which the process stopped running.
    - ***Duration***. Amount of time, in hours, minutes, and seconds, for which the process ran.
    - ***Frequency***. Frequency with which SL1 launches the process. Possible values are:

- *Asynchronous*. The process is launched in response to a system event or user request. Asynchronous events display a value of "-1" (negative one) in this column.
- *Always*. The process always runs while SL1 is running. Always running processes display a value of "0" (zero) in this column.
- The process runs at intervals in minutes ranging from *1 Minute* to *1440 Minutes (Daily)*.

- ***Percent***. Percent of ***Run Length*** (defined in the **Process Manager** page) currently in use by the process.
- ***Instances***. This field is not currently in use.
- ***Max Instances***. Maximum number of instances of the process that have run in parallel.
- ***Processed***. Number of records processed by this run of the process.
- ***Errors***. Number of errors encountered by this run of the process.

Searching and Filtering the List of System Processes

The **System Processes** page includes ten filters. You can filter the list of processes by one or multiple of the following parameters: appliance, process name, start time, end time, duration, frequency, percent, max instances, processed, and errors. Only processes that meet all the filter criteria will be displayed in the **System Processes** page.

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

- For eight of the filters, you must enter text to match against. The user interface will search for processes that match the text, including partial matches. Text matches are not case sensitive. You can use the following special characters in each filter:
  - **,** Specifies an "or" operation. For example:

    "dell, micro" would match all values that contain the string "dell" OR the string "micro".
  - **!** Specifies a "not" operation. For example:

    "!dell" would match all values that do not contain the string "dell".
- ***Appliance***. You can enter text to match, including special characters, and the **System Processes** page will display only processes that have a matching appliance name.
- ***Process***. You can enter text to match, including special characters, and the **System Processes** page will display only processes that have a matching process name.
- ***ID***. You can enter text to match, and the **System Processes** page will display only processes that have a matching ID.
- ***Start Time***. Only those processes that match all the previously selected fields and have the specified start date and time will be displayed. The choices are:
  - *All*. Display processes with all start dates and times.
  - *Last Minute*. Display only processes that started within the last minute.
  - *Last Hour*. Display only processes that started within the last hour.

- *Last Day*. Display only processes that started within the last day.
- *Last Week*. Display only processes that started within the last week.
- *Last Month*. Display only processes that started within the last month.
- *Last Year*. Display only processes that started within the last year.

- ***End Time***. Only those processes that match all the previously selected fields and have the specified end date and time will be displayed. The choices are:
  - *All*. Display processes with all end dates and times.
  - *Last Minute*. Display only processes that ended within the last minute.
  - *Last Hour*. Display only processes that ended within the last hour.
  - *Last Day*. Display only processes that ended within the last day.
  - *Last Week*. Display only processes that ended within the last week.
  - *Last Month*. Display only processes that ended within the last month.
  - *Last Year*. Display only processes that ended within the last year.
- ***Duration***. You can enter text to match, including special characters, and the **System Processes** page will display only processes that have a matching duration.
- ***Frequency***. You can enter text to match, including special characters, and the **System Processes** page will display only processes that have a matching frequency.
- ***Percent***. You can enter text to match, including special characters, and the **System Processes** page will display only processes that have a matching percent.
- ***Instances***. This field is not currently in use. It is not recommended to filter the System Processes by this field.
- ***Max Instances***. You can enter text to match, including special characters, and the **System Processes** page will display only processes that have a matching number of Max Instances.
- ***Processed***. You can enter text to match, including special characters, and the **System Processes** page will display only processes that have a matching number of records processed.
- ***Errors***. You can enter text to match, including special characters, and the **System Processes** page will display only processes that have a matching number of errors.

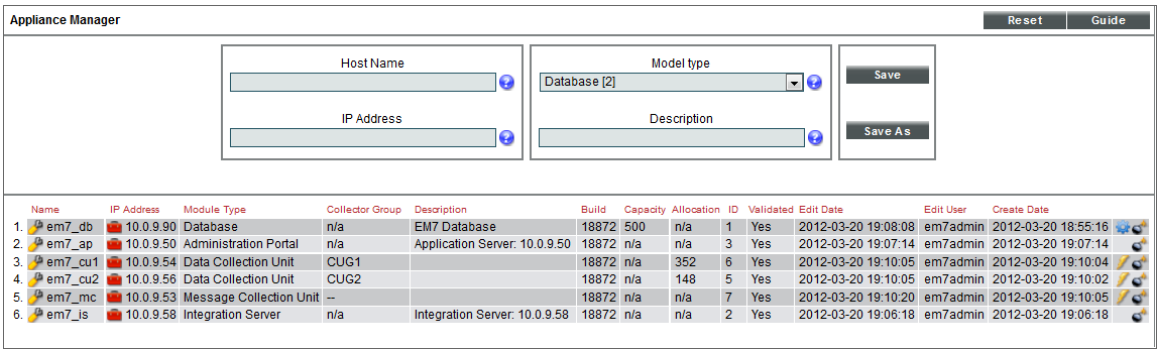
Monitoring the Status of Each Appliance

The **Appliance Manager** page allows you to view information, including license status, about each appliance in your system.

From the **Appliance Manager** page, you can also access the Web Configuration Utility for each appliance and the database administration tool for the Database Server.

To view the **Appliance Manager** page:

1. Go to the **Appliance Manager** page (System > Settings > Appliances).



	Name	IP Address	Module Type	Collector Group	Description	Build	Capacity	Allocation	ID	Validated	Edit Date	Edit User	Create Date
1.	em7_db	10.0.9.90	Database	n/a	EM7 Database	18872	500	n/a	1	Yes	2012-03-20 19:08:08	em7admin	2012-03-20 18:55:16
2.	em7_ap	10.0.9.50	Administration Portal	n/a	Application Server: 10.0.9.50	18872	n/a	n/a	3	Yes	2012-03-20 19:07:14	em7admin	2012-03-20 19:07:14
3.	em7_cu1	10.0.9.54	Data Collection Unit	CUG1		18872	n/a	352	6	Yes	2012-03-20 19:10:05	em7admin	2012-03-20 19:10:04
4.	em7_cu2	10.0.9.56	Data Collection Unit	CUG2		18872	n/a	148	5	Yes	2012-03-20 19:10:05	em7admin	2012-03-20 19:10:02
5.	em7_mc	10.0.9.53	Message Collection Unit	--		18872	n/a	n/a	7	Yes	2012-03-20 19:10:20	em7admin	2012-03-20 19:10:05
6.	em7_is	10.0.9.58	Integration Server	n/a	Integration Server: 10.0.9.58	18872	n/a	n/a	2	Yes	2012-03-20 19:06:18	em7admin	2012-03-20 19:06:18

2. The **Appliance Manager** page displays the following about each appliance:

   - ***Name***. Name of the appliance.
   - ***IP Address***. Primary IP address for the appliance.
   - ***Module Type***. Type of appliance. Choices are:
     - All-In-One Appliance
     - Database Server
     - Administration Portal
     - Data Collector
     - Message Collector
     - Integration Server
   - ***Collector Group***. For Data Collectors and All-In-One Appliances, specifies the Collector Group associated with the appliance.
   - ***Description***. Description of the appliance.
   - ***Build***. Specifies the latest build installed on the appliance.
   - ***Capacity***. For Database Servers, specifies the licensed capacity of the appliance.
   - ***Allocation***. For Data Collectors, specifies the number of devices aligned with the appliance.
   - ***ID***. Unique numeric ID, automatically assigned by the platform to each appliance in the **Appliance Manager** page.
   - ***Validated***. Specifies whether the license is valid.
   - ***Edit Date***. Date the appliance's information was discovered or last edited.
   - ***Edit User***. User who last edited the appliance's information.
   - ***Create Date***. Date and time the appliance was registered and licensed.

3. For Database Servers, you can click the gear icon ( ) to access the phpMyAdmin interface for the Database Server. In this interface, you can view all the database tables on the Database Server.

4. For Data Collectors and Message Collectors, you can click the lightning bolt icon () to manually force the Database Server to send the latest configuration information.

Monitoring User Actions and Events

The **Audit Logs** page provides an audit trail for SL1. The **Audit Logs** page displays a record of actions in SL1 that are generated by ***users*** or by ***managed elements***. These actions are organized by organization.

Some of the actions that are logged in the **Audit Logs** page include:

- User logins to SL1
- Organization name changes
- The addition, editing, or deletion of elements in SL1

> **NOTE:** Entries for the addition, editing, and deletion of elements includes the affected device ID, when applicable.

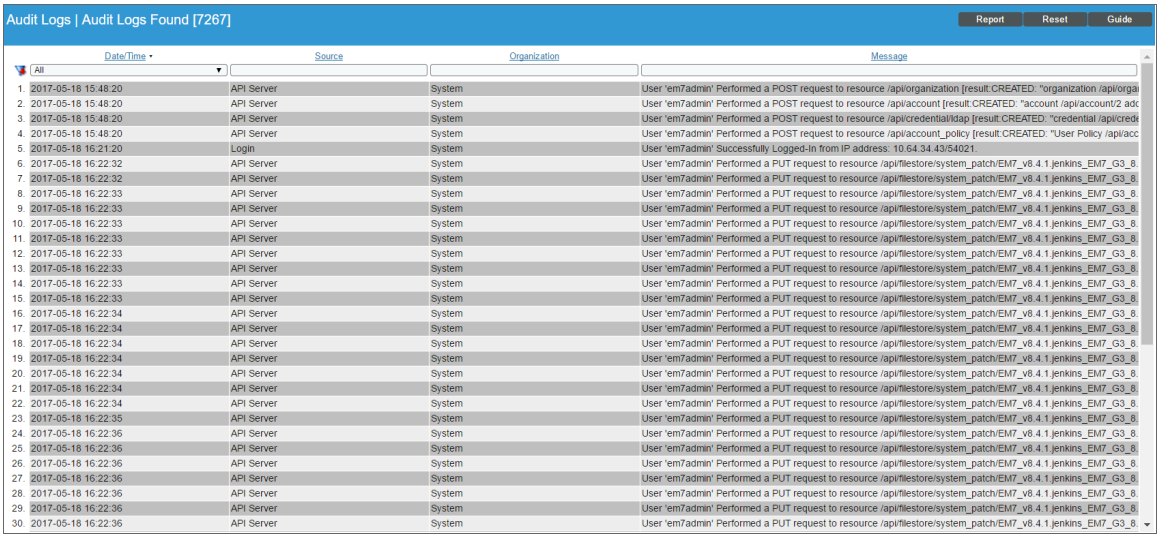
- The installation, editing, or uninstallation of PowerPacks, including when a PowerPack is imported or installed from Global Manager to a Stack
- Manually triggered discovery sessions
- Events and cleared events
- Devices being set to maintenance mode or devices no longer being in maintenance mode
- The unalignment of Dynamic Applications from devices and the deletion of that data
- The creation, editing, or deletion of Run Book Automation policies
- The addition or deletion of Reports
- Asset Record changes
- User-defined changes to settings on the **Data Retention Settings** page (System > Settings > Data Retention)
- API requests that use a PUT, POST, or DELETE method

> **NOTE**: By default, the **Audit Logs** page displays a list of actions associated with all organizations.

Viewing the List of Audit Logs

To view the list of log entries in the **Audit Logs** page:

1. Go to the **Audit Logs** page (System > Monitor > Audit Logs).



2. The **Audit Logs** page displays all actions that are performed by users or managed elements in SL1. For each action, the **Audit Logs** page displays:

   - ***Date/Time***. Date and time the action occurred and the log entry was created.
   - ***Source***. Source of the log entry. This usually describes where the action took place. For example, if you change the contact information for your account, an entry will be made in the audit log, and the source will be "Contact Information."
   - ***Organization***. Organization associated with the action.
   - ***Message***. Text of the log entry.

Searching and Filtering the List of Audit Logs

The Filter-While-You-Type fields appear as a row of blank fields at the top of the list. These fields allow you to filter the items that appear in the list.

The list is dynamically updated as you select each filter. For each filter, you must make a selection from a drop-down menu or type text to match against. SL1 will search for entries that match the text, including partial matches. Text matches are not case-sensitive, and you can use special characters in each text field.

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.

You can filter by one or more of the following parameters. Only items that meet all of the filter criteria are displayed on the page.

The following describes each filter on the **Audit Logs** page:

- ***Date/Time***. Only those audit logs that have the specified creation date will be displayed. The choices are:
    - *All*. Display all audit logs that match the other filters.
    - *Last Minute*. Display only audit logs that have been created within the last minute.
    - *Last Hour*. Display only audit logs that have been created within the last hour.
    - *Last Day*. Display only audit logs that have been created within the last day.
    - *Last Week*. Display only audit logs that have been created within the last week.
    - *Last Month*. Display only audit logs that have been created within the last month.
    - *Last Year*. Display only audit logs that have been created within the last year.
- ***Source***. You can enter text to match, including special characters, and the Audit Logs page will display only audit logs that have a matching source.
- ***Organization***. You can enter text to match, including special characters, and the Audit Logs page will display only audit logs that have a matching organization.
- ***Message***. You can enter text to match, including special characters, and the Audit Logs page will display only audit logs that have a matching message.

Special Characters

You can include the following special characters to filter by each column except those that display date and time:

> **NOTE**: When searching for a string, SL1 will match substrings by default, even if you do not include any special characters. For example, searching for "hel" will match both "hello" and "helicopter". When searching for a numeric value, SL1 will not match a substring unless you use a special character.

String and Numeric

- , (comma). Specifies an "OR" operation. Works for string and numeric values. For example:

  "dell, micro" matches all values that contain the string "dell" OR the string "micro".

- & (ampersand). Specifies an "AND " operation. Works for string and numeric values. For example:

  "dell & micro" matches all values that contain both the string "dell" AND the string "micro", in any order.

- ! (exclamation point). Specifies a "not" operation. Works for string and numeric values. For example:

  "!dell" matches all values that do not contain the string "dell".

  "!^micro" would match all values that do not start with "micro".

  "!fer$" would match all values that do not end with "fer".

  "!^$" would match all values that are not null.

  "!^" would match null values.

  "!$" would match null values.

  "!*" would match null values.

  "happy, !dell" would match values that contain "happy" OR values that do not contain "dell".

NOTE: You can also use the "!" character in combination with the arithmetic special characters (min-max, >, <, >=, <=, =) described below.

- * (asterisk). Specifies a "match zero or more" operation. Works for string and numeric values. For a string, matches any string that matches the text before and after the asterisk. For a number, matches any number that contains the text. For example:

  "hel*er" would match "helpers" and "helicopter" but not "hello".

  "325*" would match "325", "32561", and "325000".

  "*000" would match "1000", "25000", and "10500000".

- ? (question mark). Specifies "match any one character". Works for string and numeric values. For example:

  "l?ver" would match the strings "oliver", "levers", and "lover", but not "believer".

  "135?" would match the numbers "1350", "1354", and "1359", but not "135" or "13502"

String

- ^ (caret). For strings only. Specifies "match the beginning". Matches any string that begins with the specified string. For example:

  "^sci" would match "scientific" and "sciencelogic", but not "conscious".

  "^happy$" would match only the string "happy", with no characters before or after.

  "!^micro" would match all values that do not start with "micro".

  "!^$" would match all values that are not null.

  "!^" would match null values.

- $ (dollar sign). For strings only. Specifies "match the ending". Matches any string that ends with the specified string. For example:

  "ter$" would match the string "renter" but not the string "terrific".

  "^happy$" would match only the string "happy", with no characters before or after.

  "!fer$" would match all values that do not end with "fer".

  "!^$" would match all values that are not null.

  "!$" would match null values.

NOTE: You can use both ^ and $ if you want to match an entire string and only that string. For example, "^tern$" would match the strings "tern" or "Tern" or "TERN"; it would not match the strings "terne" or "cistern".

Numeric

- min-max. Matches numeric values only. Specifies any value between the minimum value and the maximum value, including the minimum and the maximum. For example:

  "1-5 "would match 1, 2, 3, 4, and 5.

- - (dash). Matches numeric values only. A "half open" range. Specifies values including the minimum and greater or including the maximum and lesser. For example:

  "1-" matches 1 and greater. So would match 1, 2, 6, 345, etc.

  "-5" matches 5 and less. So would match 5, 3, 1, 0, etc.

- > (greater than). Matches numeric values only. Specifies any value "greater than". For example:

  ">7" would match all values greater than 7.

- < (less than). Matches numeric values only. Specifies any value "less than". For example:

  "<12" would match all values less than 12.

- >= (greater than or equal to). Matches numeric values only. Specifies any value "greater than or equal to". For example:

  "=>7" would match all values 7 and greater.

- <= (less than or equal to). Matches numeric values only. Specifies any value "less than or equal to". For example:

  "=<12" would match all values 12 and less.

- = (equal). Matches numeric values only. For numeric values, allows you to match a negative value. For example:

  "=-5 " would match "-5" instead of being evaluated as the "half open range" as described above.

Additional Examples

- "aio$". Matches only text that ends with "aio".
- "^shu". Matches only text that begins with "shu".
- "^silo$". Matches only the text "silo", with no characters before or after.
- "!silo". Matches only text that does not contains the characters "silo".
- "!^silo". Matches only text that does not start with "silo".
- "!0$". Matches only text that does not end with "0".
- "!^silo$". Matches only text that is not the exact text "silo", with no characters before or after.
- "!^". Matches null values, typically represented as "--" in most pages.
- "!$". Matches null values, typically represented as "--" in most pages.
- "!^$". Matches all text that is not null.
- silo, !aggr". Matches text that contains the characters "silo" and also text that does not contain "aggr".
- "silo, 02, !aggr". Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr".
- "silo, 02, !aggr, !01". Matches text that contains "silo" and also text that contains "02" and also text that does not contain "aggr" and also text that does not contain "01".
- "^s*i*l*o$". Matches text that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXlXo" would match.
- "!^s*i*l*o$". Matches all text that does not that contains the letter "s", "i", "l", "o", in that order. Other letters might lie between these letters. For example "sXiXlXo" would not match.
- "!vol&!silo". Matches text that does not contain "vol" AND also does not contain "silo". For example, "volume" would match, because it contains "vol" but not "silo".
- "!vol&02". Matches text that does not contain "vol" AND also contains "02". For example, "happy02" would match, because it does not contain "vol' and it does contain "02".
- "aggr,!vol&02". Matches text that contains "aggr" OR text that does not contain "vol" AND also contains "02".
- "aggr,!vol&!infra". Matches text that contains "aggr" OR text that does not contain "vol" AND does not contain "infra".
- "*". Matches all text.
- "!*". Matches null values, typically represented as "--" in most pages.
- "silo". Matches text that contains "silo".
- " !silo ". Matches text that does not contain "silo".
- " !^silo$ ". Matches all text except the text "silo", with no characters before or after.
- "-3,7-8,11,24,50-". Matches numbers 1, 2, 3, 7, 8, 11, 24, 50, and all numbers greater than 50.

- "-3,7-8,11,24,50-,a". Matches numbers 1, 2, 3, 7, 8, 11, 24, 50, and all numbers greater than 50, and text that includes "a".
- "?n". Matches text that contains any single character and the character "n". For example, this string would match "an", "bn", "cn", "1n", and "2n".
- "n*SAN". Matches text the contains "n", zero or any number of any characters and then "SAN". For example, the string would match "nSAN", and "nhamburgerSAN".
- "^?n*SAN$". Matches text that begins with any single character, is following by "n", and then zero or any number of any characters, and ends in "SAN".

Generating Reports on Audit Logs

You can export the entries on the **Audit Logs** page as one of the following report types:

- Acrobat document (.pdf)
- Web page (.html)
- Excel spreadsheet (.xlsx)
- OpenDocument Spreadsheet (.ods)
- Comma-separated values (.csv)

When you create a report in the **Audit Logs** page, SL1 includes only those logs that appear in the current view of the page. If you filter the entries on the **Audit Logs** page, only those logs that meet the filter criteria and currently appear on the page will appear in the report.

To generate an audit logs report:

1. From the **Audit Logs** page, click the **[Report]** button. The **Export current view as a report** window appears.
2. In the ***Output Format*** field, select the report format type.
3. Click **[Generate]**.

Monitoring the Status of Data Collectors

The **Collector Status** page displays the status of each Data Collector and Message Collector in your system.

> **NOTE**: This page does not appear in All-In-One Appliances.

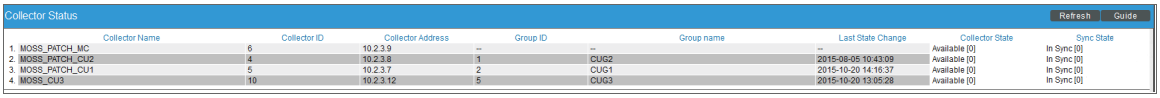
Data Collectors retrieve data from managed devices and applications. This collection occurs during initial discovery, during nightly updates, and in response to policies defined for each managed device. The collected data is used to trigger events, display data in the user interface, and generate graphs and reports.

Message Collectors receive and process inbound, asynchronous syslog and trap messages from monitored devices. In most distributed systems, dedicated ***Message Collector*** appliances perform message collection. A single ***Message Collector*** can handle syslog and trap messages from devices that are monitored by multiple ***Data Collectors***.

To perform collection, you must define a Collector Group and align it with at least one Data Collector. If your Collector Group includes multiple Data Collectors, you can configure the Collector Group for high-availability. For details, see the section on *Collector Groups*.

To ensure the health of your system, you should periodically check on the status of the Data Collectors and Message Collectors. To access the **Collector Status** page:

1. Go to the **Collector Status** page (System > Monitor > Collector Status).



2. For each Data Collector in your system, the **Collector Status** page displays the following:

   - ***Collector Name***. Name of the Data Collector or Message Collector.
   - ***Collector ID***. Unique numeric ID automatically assigned to the Data Collector or Message Collectorby SL1.
   - ***Collector Address***. IP address of the Data Collector or Message Collector.
   - ***Group ID***. Unique numeric ID of the *Collector Group* associated with the Data Collector or Message Collector.
   - ***Group Name***. Name of the *Collector Group* associated with the Data Collector or Message Collector.
   - ***Last State Change***. Date and time the platform last polled the status of the Data Collector or Message Collector.
   - ***Collector State***. Operating state of the Data Collector or Message Collector.
   - ***Sync State***. Specifies whether the Data Collector or Message Collector is in synch with the latest configuration data on the Database Server.

Chapter 5

Updating, Monitoring, and Maintaining SL1

Overview

The **System Updates** page allows you to update the software on your SL1 appliances. You must first download the update file to the local computer where you are running the browser. You can then load the software update through the user interface.

After you load a software update to your SL1 system, the SL1 system can automatically ***stage*** the software update. Staging is when the software is copied to each ScienceLogic appliance. Staging allows SL1 to simultaneously apply the software changes to each ScienceLogic appliance, regardless of the speed of the connection to each ScienceLogic appliance.

You can allow the SL1 system to automatically stage the software or you can manually stage the software.

After the software update is staged, you can install the software.

WARNING: To apply updates to an existing Data Collector, that Data Collector must be a member of a Collector Group. In some SL1 systems, users might have to create a Collector Group for a single Data Collector before applying updates.

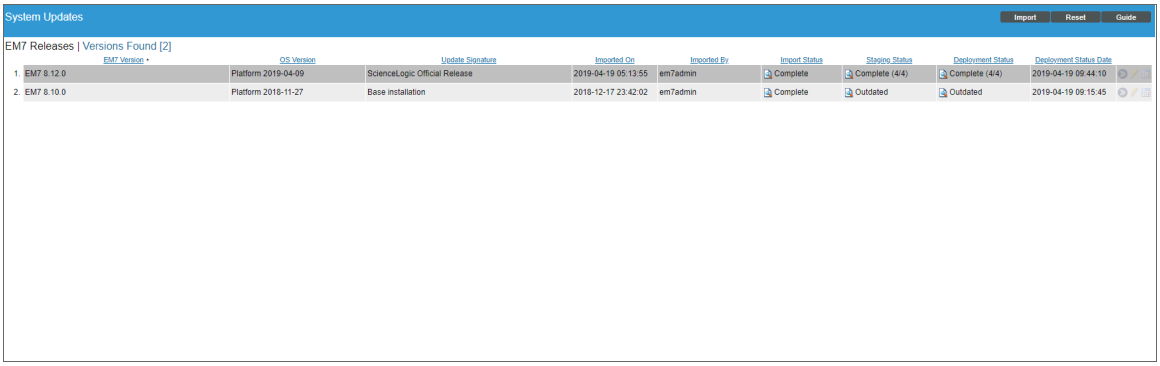
Use the following menu options to navigate the SL1 user interface:

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

This chapter includes the following topics:

Viewing the List of Updates

The **System Updates** page (System > Tools > Updates) displays the following about each update:



TIP: To sort the list of update files, click on a column heading. The list will be sorted by the column value, in ascending order. To sort by descending order, click the column heading again. The ***Deployed Status Date*** column sorts by descending order on the first click; to sort by ascending order, click the column heading again.

- ***EM7 Version***. Name and version number for the software update.
- ***OS Version***. Name and number of the platform OS update.
- ***Update Signature***. Name of the entity that released the update and type of update. Usually "ScienceLogic Official Release".
- ***Imported On***. Date and time the software update was loaded onto the SL1 system.
- ***Imported By***. Name of the ScienceLogic user who loaded the software update onto the SL1 system.
- ***Import Status***. Status of the import process. Clicking on the log icon displays the log file associated with importing the selected software. Possible values are:
    - *In Progress*. Software is currently being imported by the SL1 system.
    - *Complete*. Software has been imported successfully.
    - *Failed*. Software import has failed due to an unexpected condition. Contact ScienceLogic Support for assistance.

- *Missing Base*. The SL1 system cannot import this software until another software package has been imported. The dependency is for compression purposes. Check the log for a message stating which software package needs to be imported.

- ***Staging Status***. Status of the staging process. Clicking on the log icon displays the log file associated with staging the selected software. Possible values are:
  - --. No staging request is active and software has not been staged on any SL1 appliances.
  - *Scheduled*. The SL1 system is aware of the staging request and is preparing for staging.
  - *In Progress*. Staging is in progress but has not completed.
  - *Complete*. Staging has completed, and all appliances are ready to deploy the software.
  - *Incomplete*. Staging has completed, and one or more appliances are ready to deploy the software.
  - *Canceled*. User manually canceled the staging process.
  - *Outdated*. The current update is not the latest or has already been installed.
  - *Failed*. An unexpected error occurred in the staging process. Contact ScienceLogic Support.

NOTE: If you did not select ***Auto Stage*** during import, the ***Staging Status*** column will include an asterisk (*) until you manually stage the update..

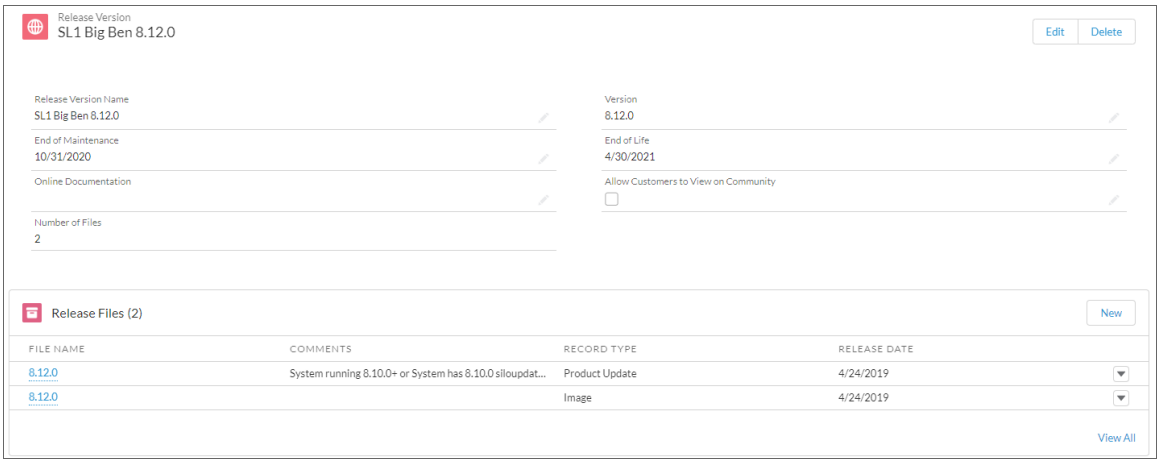
- ***Deployment Status***. Specifies the current deployment state. Possible values are:
  - --. No deployment request is active and software has not been deployed on any SL1 appliances.
  - *Scheduled*. The SL1 system is aware of the deployment request and is preparing for deployment.
  - *In Progress*. Deployment is in progress but has not completed.
  - *Complete*. Deployment has completed, and all appliances are updated.
  - *Incomplete*. Deployment has completed, and one or more appliances are updated.
  - *Canceled*. User manually canceled the deployment.
  - *Outdated*. The current update is not the latest or has already been installed.
  - *Failed*. An unexpected error occurred in the deployment process. Contact ScienceLogic Support.
- ***Deployment Status Date***. Specifies the date and time the software update was last deployed.

Downloading Patches and Updates

Before you can load a patch or update onto your instance of the SL1 system, you must first download the patch or update to your local computer. To do this:

1. Log in to https://support.sciencelogic.com. Use your ScienceLogic customer account and password to access this site.

2. Select the **[Product Downloads]** button, select the ***Product Downloads*** menu, and choose *Platform*.
3. Find the release you are interested in and click its name.

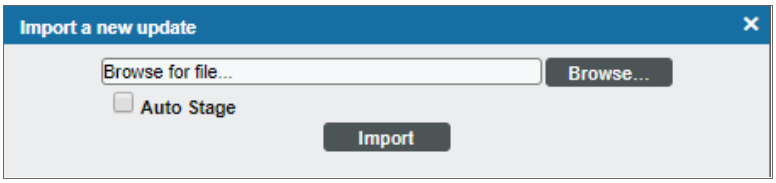


4. In the ***Release Version*** article, click on the link for the release image or release patch you want to download. Scroll to the bottom of the page.
5. Under **File**s, select the link for the file you want to download.
6. The file is then downloaded to your local computer.

Importing Updates on to the Platform

To import a product update on to your SL1 system:

1. Make sure that you can navigate to the patch file.
2. In SL1, go to the **System Updates** page (System > Tools > Updates).
3. In the **System Updates** page, click the **[Import]** button.



4. In the **Import a new update** modal page, browse to the product update file and select it.
   - If you select the ***Auto Stage*** button, the SL1 system will begin stating as soon as the import is completed.
   - If you do not select the ***Auto Stage*** button, you must click the staging button() after import is completed. You can do so at any time after import has completed.

- For more information on staging, see the section on "Automatic Staging" in the ***System Administration*** manual.

5. Click the **[Import]** button.
6. In the **System Updates** page, the *Import Status* column can have one of the following statuses:
    - *In Progress*. Software is currently being imported by the SL1 system.
    - *Complete*. Software has been imported successfully.
    - *Failed*. Software import has failed due to an unexpected condition. Contact ScienceLogic Support for assistance.
    - *Missing Base*. The SL1 system cannot import this software until another software package has been imported. The dependency is for compression purposes. Check the log for a message stating which software package needs to be imported.
7. The update file or patch file is imported to SL1 and appears in the **System Updates** page.

NOTE: For details on the import process, go to the **System Updates** page, find the entry for the software you are interested in, go to its ***Import Status*** column, and click the log icon ( ).

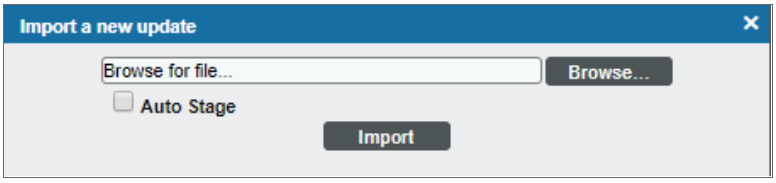
Automatic Staging

After you import a software update to your SL1 system, you must ***stage*** the software update. During staging, the SL1 system copies the software update to each ScienceLogic applianceGlobal Manager system. Staging allows SL1 to simultaneously apply the software changes to each ScienceLogic applianceGlobal Manager system, regardless of the speed of the connection to each ScienceLogic applianceGlobal Manager system.The SL1 system stages updates per import. You can choose to automatically stage imports or manually stage import.

After the software update is imported and staged, you can deploy the software.

To enable automatic staging:

1. In SL1, go to the **System Updates** page (System > Tools > Updates).
2. In the **System Updates** page, click the **[Import]** button.

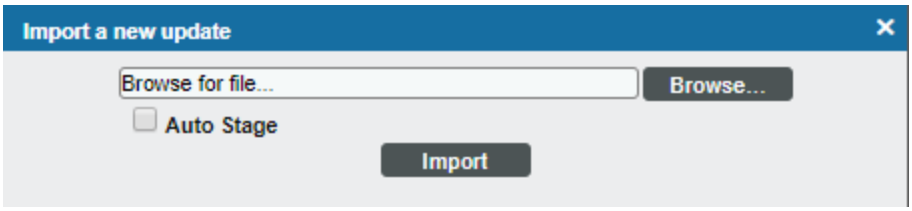


3. In the **Import a new update** modal page, browse to the product update file and select it.
    - If you select the ***Auto Stage*** button, the SL1 system will begin stating as soon as the import is completed.
4. After import, in the the **System Updates** page, the *Staging Status* column will display the number of ScienceLogic appliances that have been successfully stage compared to the total number of ScienceLogic appliances.
5. The *Staging Status* column can have one of the following statuses:
    - --. No staging request is active and software has not been staged on any SL1 appliances.
    - *Scheduled*. The SL1 system is aware of the staging request and is preparing for staging.
    - *In Progress*. Staging is in progress but has not completed.
    - *Complete*. Staging has completed, and all appliances are ready to deploy the software.
    - *Incomplete*. Staging has completed, and one or more appliances are ready to deploy the software.
    - *Canceled*. User manually canceled the staging process.
    - *Outdated*. The current update is not the latest or has already been installed.
    - *Failed*. An unexpected error occurred in the staging process. Contact ScienceLogic Support.

NOTE: For details on the staging process, go to the **System Updates** page, find the entry for the software you are interested in, go to its ***Staging Status*** column, and click the log icon ( ).

To disable automatic staging:

1. In SL1, go to the **System Updates** page (System > Tools > Updates).
2. In the **System Updates** page, click the **[Import]** button.



3. In the **Import a new update** modal page, browse to the product update file and select it.

    - If you do not select the ***Auto Stage*** button, you must click the staging button( ) after import is completed. You can do so at any time after import has completed.

NOTE: For details on the staging process, go to the **System Updates** page, find the entry for the software you are interested in, go to its ***Staging Status*** column, and click the log icon ( ).

Manually Staging an Update

You can manually stage a software update to one or more SL1 appliances.

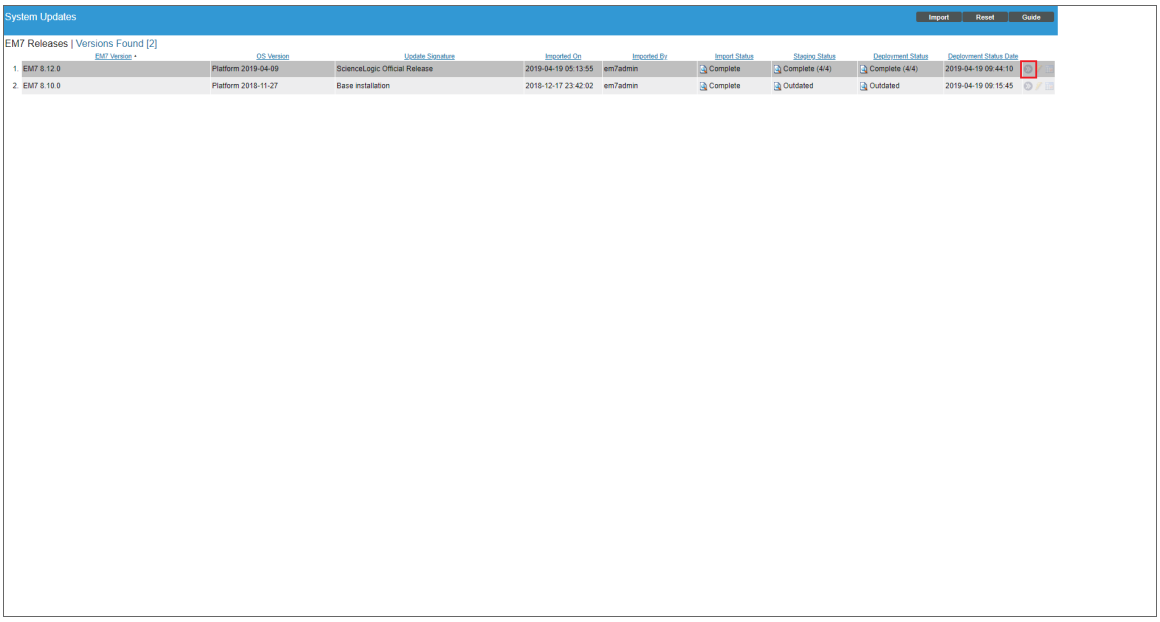
For example:

- If you imported an update but want to stage it at a later time.
- If you add another ScienceLogic appliance to your SL1 system and need to apply software updates, you can manually stage a software update.
- If staging failed on one or more ScienceLogic appliances, you can manually stage a software update.
- If you want to ensure that a previous staging process was successful, you can manually stage a software update.

When you manually stage a software update, SL1 checks the status of the software updated on each ScienceLogic appliance. SL1 then stages the software update ***only to those SL1 appliances that have not yet been staged*** for this software update.

To manually stage a software update:

1. Go to the **System Updates** page (System > Tools > Updates).



2. In the **System Updates** page, find the software update you want to stage. Select its staging icon ( ).
3. The software update will be copied to each ScienceLogic appliance that has not yet been staged.
4. The *Staging Status* column will display the number of ScienceLogic appliances that have been successfully stage compared to the total number of ScienceLogic appliances.
5. The *Staging Status* column can have one of the following statuses:

   - --. No staging request is active and software has not been staged on any SL1 appliances.
   - *Scheduled*. The SL1 system is aware of the staging request and is preparing for staging.
   - *In Progress*. Staging is in progress but has not completed.
   - *Complete*. Staging has completed, and all appliances are ready to deploy the software.
   - *Incomplete*. Staging has completed, and one or more appliances are ready to deploy the software.
   - *Canceled*. User manually canceled the staging process.
   - *Outdated*. The current update is not the latest or has already been installed.
   - *Failed*. An unexpected error occurred in the staging process. Contact ScienceLogic Support.

NOTE: For details on the staging process, go to the **System Updates** page, find the entry for the software you are interested in, go to its ***Staging Status*** column, and click the log icon ( ).

Deploying Updates

After you have imported and staged an update to SL1, you can either immediately deploy the update or deploy it at a later time..

When you deploy an update, the update is installed on all appliances that have already been staged.

NOTE: When you deploy an update, SL1 checks to ensure that you have already deployed all required updates. If you have not, SL1 will generate an error message specifying the updates you must deploy before continuing with the current update.

To deploy a software update on your appliances:

1. Make sure that you have imported and staged the update file.
2. Go to the **System Updates** page (System > Tools > Updates).
3. In the **System Updates** page, find the software update you want to deploy. Click the lightning bolt icon () to deploy the software.

NOTE: If SL1 is still staging the patch when you click the lightning-bolt icon (), SL1 will wait until staging has completed before deploying the updates to each ScienceLogic appliance.

2. The software update will be deployed to all appliances in your SL1 system that have already been staged. If one or more appliances in your SL1 system have been successfuolly staged, SL1 will deploy the update to those appliances.
3. During deployment the Deployment Status column can have one of the following statuses:
    - --. No deployment request is active and software has not been deployed on any SL1 appliances.
    - *Scheduled*. The SL1 system is aware of the deployment request and is preparing for deployment.
    - *In Progress*. Deployment is in progress but has not completed.
    - *Complete*. Deployment has completed, and all appliances are updated.
    - *Incomplete*. Deployment has completed, and one or more appliances are updated.
    - *Canceled*. User manually canceled the deployment.
    - *Outdated*. The current update is not the latest or has already been installed.
    - *Failed*. An unexpected error occurred in the deployment process. Contact ScienceLogic Support.

NOTE: For details on the deployment process, go to the **System Updates** page, find the entry for the software you are interested in, go to its ***Deployment Status*** column, and click the log icon ().

Viewing the Log Files for Updates

From the **System Updates** page, you can view a log file that displays the history of the software update. To view this log file:

1. Go to the **System Updates** page (System > Tools > Updates).
2. In the **System Updates** page, find the software update for which you want to view the log files. Go to its ***Import Status*** column, ***Staging Status*** column, or ***Deployment Status*** column and click the log icon ().
3. The appropriate log page appears. In this modal page, each log entry displays:
    - Information about the status of the software update and its related actions.
    - For each action, the name and IP address of the appliance where the action occurred
    - The date and time each action occurred.

Configuring Timeouts for Updates in Distributed Systems

In a distributed system, two timeout settings apply to the update process:

- The *Time Factor* setting for the ***EM7 Core: System Updater*** process, displayed in the **Process Manager** page (System > Settings > Admin Processes), defines the timeout for the process that applies the update to each appliance.
- In the silo.conf file, the *patcher_wait_timeout* setting defines how long the Database Server will wait for all other appliances to complete the update process. If the *patcher_wait_timeout* setting is not defined in silo.conf, the default value is 300 seconds (5 minutes).

NOTE: For help configuring these settings, please contact ScienceLogic Support.

Managing New Features on the Content Management Page

You can use the **Content Management** page to install and upgrade various features of SL1, such as new versions of the user interface (ap2) and new widget components for dashboards. These features are delivered in ***content packages***, which you can find on the **Content Management** page (Manage > Content Management).

NOTE: You might not be able to access the **Content Management** page if you do not have update and install privileges for SL1.

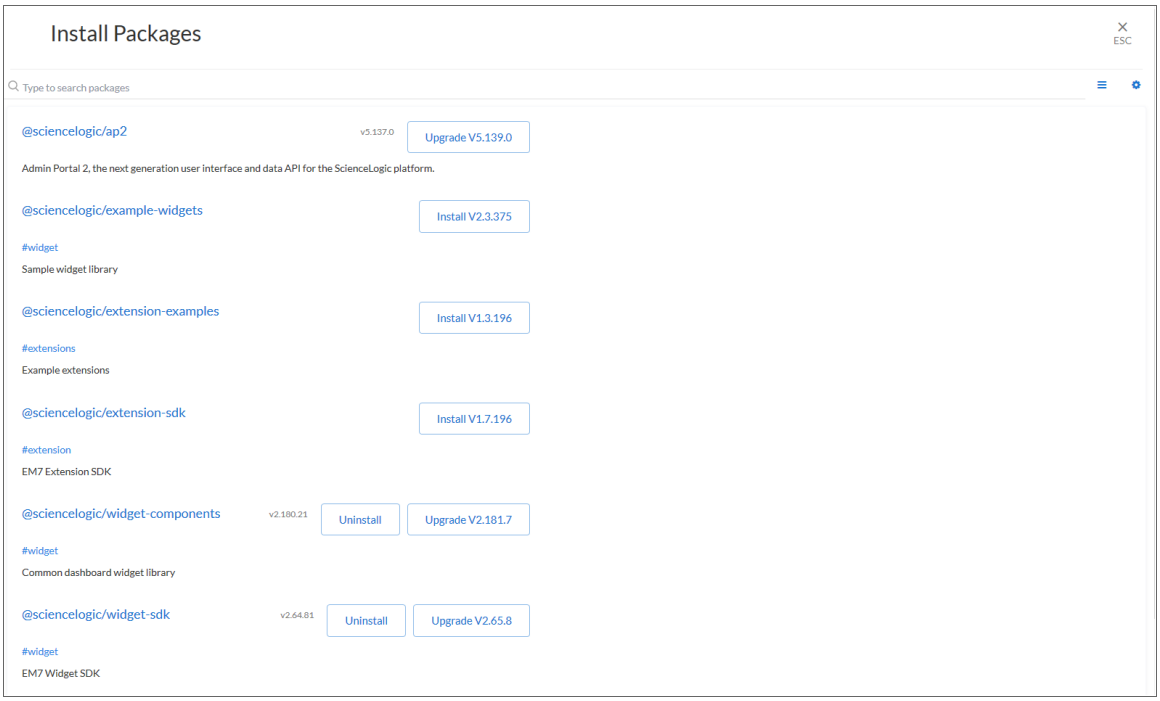
Content package names follow packaging rules for NPM, the package manager for JavaScript. Content packages created by ScienceLogic include **@sciencelogic** in the package name.

You can update more than one content package at a time, and you do not need to wait for one package to install before installing another package. Also, you can navigate away from this page and the package or packages will continue to install.

WARNING: If you use the **@sciencelogic/ap2** content package on the **Content Management** page to update your version of SL1, you will need to use the **Content Management** page for *all* future updates of SL1. If you do not want to use the **Content Management** page for SL1 updates, ScienceLogic recommends that you use the **System Updates** (System > Manage > Tools > Updates) page to upgrade the version of SL1.

To install or upgrade a content package:

1. Go to the **[Content Management]** page (Manage > Content Management).
2. Click the **[Install/Upgrade Packages]** button. The **Install Packages** page appears.



3. Click the **[Install]** button for the content package you want to install. The button changes to **[Installed]** when the package finishes installing. Larger content packages might take longer than usual to install.

NOTE: If you are updating the **@sciencelogic/ap2** content package, allow the package to run for a few minutes, and ignore any "Install Failed" messages.

NOTE: If the most recent **@sciencelogic/ap2** content package does not appear on the **Install Packages** page, reload the browser window.

4. As a best practice, clear the cache for your browser after the installation, and also clear the cache in the current or "classic" interface by clicking the **[Toolbox]** or "hamburger" button ( ) and selecting *Clear SL1 System Cache*.

TIP: To access the classic SL1 interface, type **/em7** at the end of the URL or IP address, such as **http://sl1.sciencelogic.com/em7**.

5. To view more information about a content package, including a short description and a Readme file, where relevant, click the name of the package.
6. Press the **[ESC]** button to return to the **[Content Management]** page. You can leave the **Install Packages** page before a content packages finishes installing.
7. To uninstall a content package, click the **[Uninstall]** button for that package.

Remote Reboot After an Update

If you need to reboot remote Administration Portals, Data Collectors, or Message Collectors, for example after installing an update to EM7, perform the following steps::

You can perform the reboot either from the command line of a Database Server or from the ScienceLogic user interface.

To perform remote reboot from the command line:

1. Either go to the console of the Database Server or use SSH to access the server.
2. Log in as ***em7admin*** with the appropriate password.
3. At the shell prompt, execute the following:

```
{code}python -m silo_common.admin_toolbox <mid> "/usr/bin/sudo /usr/sbin/shutdown -r
+1"{code}
```

where:

- `mid` is the appliance ID for the Data Collector, Message Collector, or Administration Portal.

To perform remote reboot from the ScienceLogic user interface:

1. Go to the **Appliance Manager** page (System > Settings > Appliances).
2. Select the checkboxes for the appliances you want to reboot.
3. In the **[Select Action]** menu, select ***Reboot*** and click the **[Go]** button.

4. Click the **[OK]** button when the "Are you sure you want to reboot the selected appliances?" message is displayed.
5. During the reboot, go to the **System Logs** page (System > Monitor > System Logs). You should see this message:

```
Major: Could not connect to module (5) database USING SSL=TRUE: Error attempting
to connect to database with SSL enabled True: (2003, 'Can't connect to MySQL
server on '10.2.12.77' (113 "No route to host")')
```

6. When the reboot has completed, the **Audit Logs** page (System > Monitor > Audit Logs) will include an entry for each appliance that was rebooted.

Upgrading Default PowerPacks

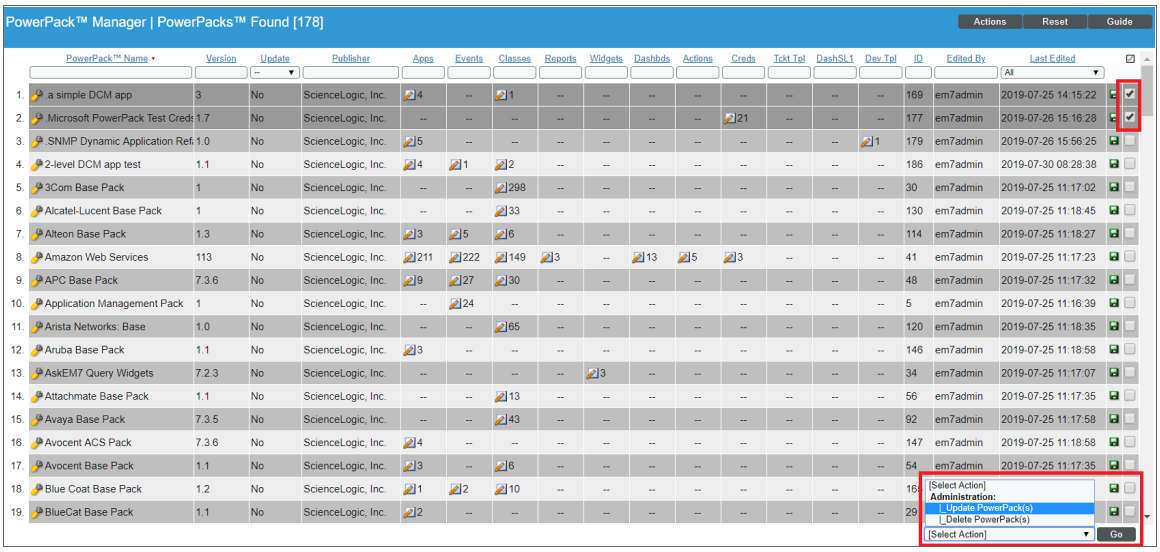
Every time you install a software update on your appliances, ScienceLogic recommends that you also install the updates for all the PowerPacks that were included in the software update.

ScienceLogic includes multiple PowerPacks in the default installation of SL1. When you apply an update to your system, new versions of the default PowerPacks will be automatically imported in to your system. If a PowerPack is included in an update and is not currently installed on your system, SL1 will automatically install the PowerPack. If a PowerPack is included in an update and is currently installed on your system, SL1 will automatically import (but not install) the PowerPack.

If PowerPacks have been imported into your system but have not been installed, the ***Update*** column appears in the **PowerPack Manager** page (System > Manage > PowerPacks). For each PowerPack that has been imported to your system but has not been installed, the lightning bolt icon ( ) appears in the ***Update*** field on the **PowerPack Manager** page.

To install the updates for multiple PowerPacks:

1. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).



2. In the **PowerPack Manager** page, select the checkbox for each PowerPack you want to install.
3. In the ***Select Action*** drop-down field (in the lower right), choose *Update PowerPack(s)*.
4. SL1 will display the following message before updating the PowerPack(s):

```
Update the selected PowerPacks?
NOTE: Any customizations to items contained in updated PowerPacks will be
overwritten by the version contained within the more recently imported PowerPack
file.
```

   Click the **[OK]** button to continue the installation. Click the **[Cancel]** button to quit the update.

5. Click the **[Go]** button. If you completed the update, updated information about the PowerPack will appear in the **PowerPack Manager** page. All the items in the PowerPack will be automatically installed in your SL1 system.

NOTE: You can install multiple PowerPacks with the ***Select Action*** drop-down list only if each selected PowerPack includes an embedded Installation Key. PowerPacks that do not include embedded Installation Keys will fail to install.

NOTE: The ***Enable Selective PowerPack Field Protection*** field on the *Behavior Settings* page (System > Settings > Behavior) affects how updates behave. If the ***Enable Selective PowerPack Field Protection*** checkbox is selected, certain fields in Event Policies, Dynamic Applications, and Device Classes will **not** be updated.

Monitoring and Managing User Access

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

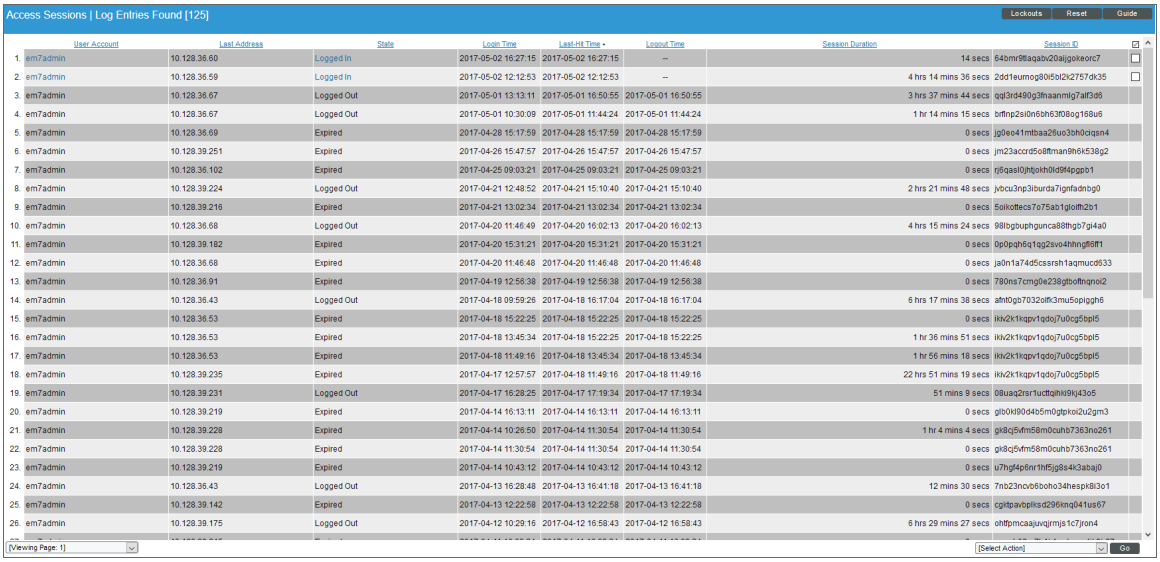
From this page, you can also:

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

Viewing Information about Each Access Session

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

1. Go to the **Access Sessions** page (System > Monitor > Access Logs).



2. For each session, the **Access Sessions** page displays:

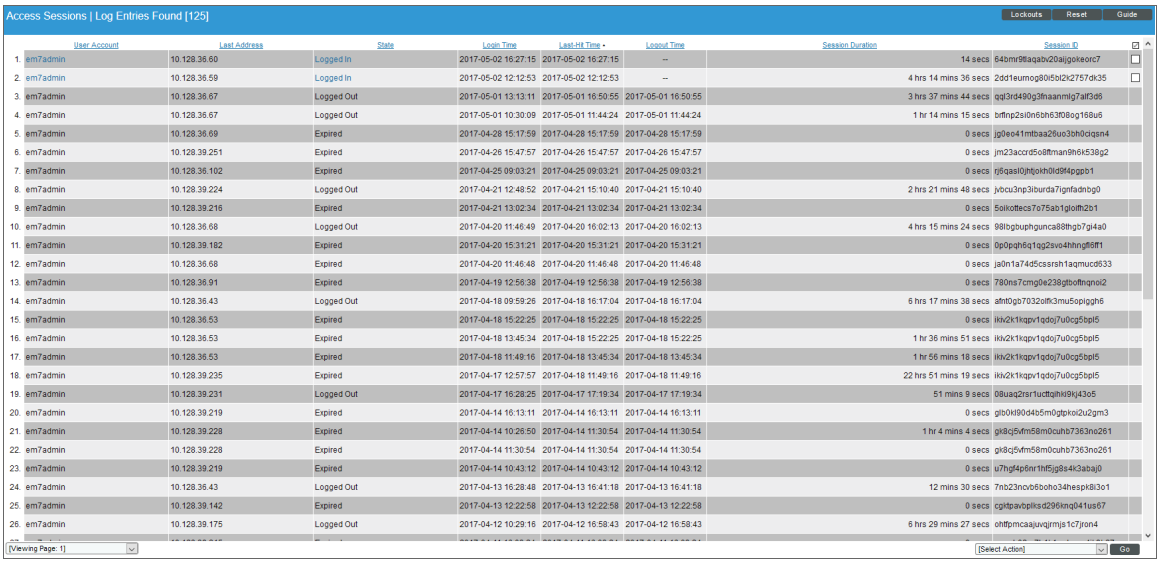
   - ***User Account***. Username of person logging in to the user interface.
   - ***Last Address***. IP address from which the user accessed the user interface.
   - ***State***. Current status of the user. The choices are:
     - *Active*. User is currently logged in to the user interface.
     - *Expired*. User's session in the user interface was killed.
     - *Logged Out*. User logged out of the user interface.
     - *Never Used*. User logged in to the user interface and did not perform any tasks before the session was killed.
   - ***Login Time***. Date and time at which the user logged in.
   - ***Last-Hit Time***. Date and time at which the user last loaded a page in the user interface.
   - ***Logout Time***. Date and time at which the user logged out.
   - ***Session Duration***. Length of time between login and logout.
   - ***Session ID***. Unique numeric ID assigned to each user session.

Deleting a User's Session

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

To end a user's session:

1. Go to the **Access Sessions** page (System > Monitor > Access Logs).



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

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

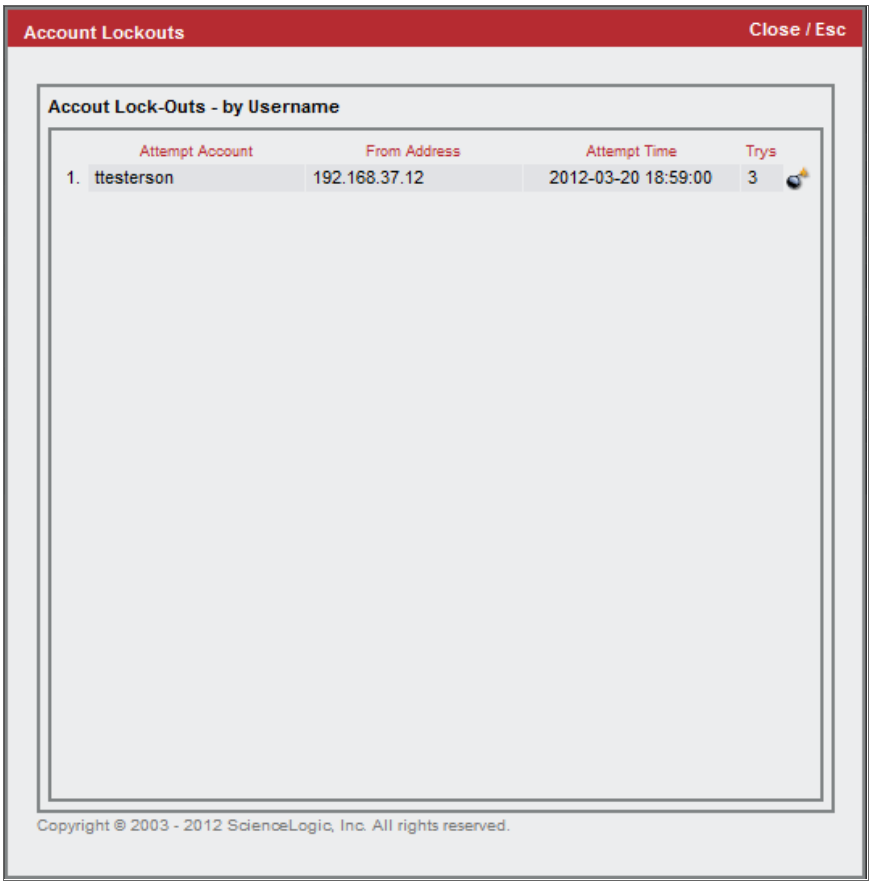
Viewing Lockouts and Unlocking Lockouts

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

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

1. Go to the **Access Sessions** page (System > Monitor > Access Logs).

2. In the **Access Sessions** page, click the **[Lockouts]** button.
3. The **Account Lockouts** modal page allows administrators to view a list of locked-out accounts and to restore login privileges to locked out users.



4. The **Account Lockouts** modal page displays the following about each lockout:
   - ***Attempt Account***. Username that caused the lockout.
   - ***From Address***. IP address from which the failed login attempts originated.
   - ***Attempt Time***. Date and time at which lockout occurred.
   - ***Tries***. Number of times user tried to log in to the user interface.
5. ***To remove the lock for the user account*** and allow logins from the username and/or IP address, click the bomb icon ( ).

Global Settings for Lockouts

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

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

Audit Logs

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

Managing Scheduled Tasks

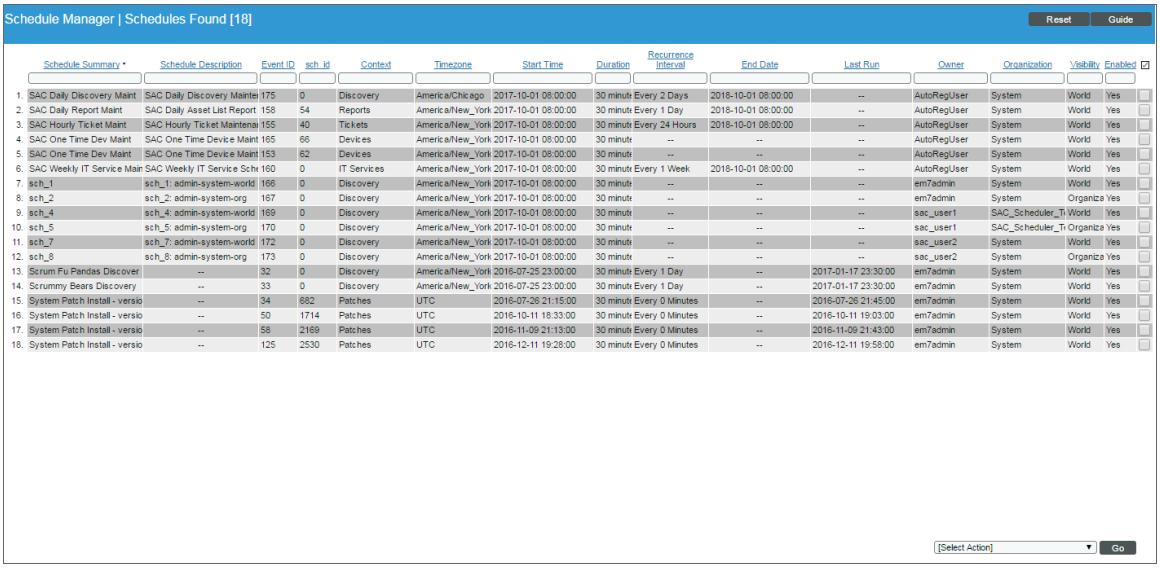
The **Schedule Manager** page (Registry > Schedules > Schedule Manager) allows you to view and manage all the scheduled processes you have defined in your system.

You can define scheduled processes in the following pages:

- Report Scheduler. (For more information, see the ***Reports*** manual.)
- My Work Schedule. (For more information, see the ***Organizations and Users*** manual.)
- Recurring Ticketing Scheduler. (For more information, see the ***Ticketing*** manual.)
- Discovery Control Panel. (For more information, see the ***Discovery and Credentials*** manual.)
- Dashboards. (For more information, see the ***Dashboards*** manual.)
- IT Service Editor. (For more information, see the ***IT Services*** manual.)
- Device Manager. (For more information, see the ***Device Management*** manual.)
- Backup Management. (For more information, see the section on *Configuration Backups*.)

Viewing the List of Schedules

The **Schedule Manager** page (Registry > Schedules > Schedule Manager) displays the following about each schedule:

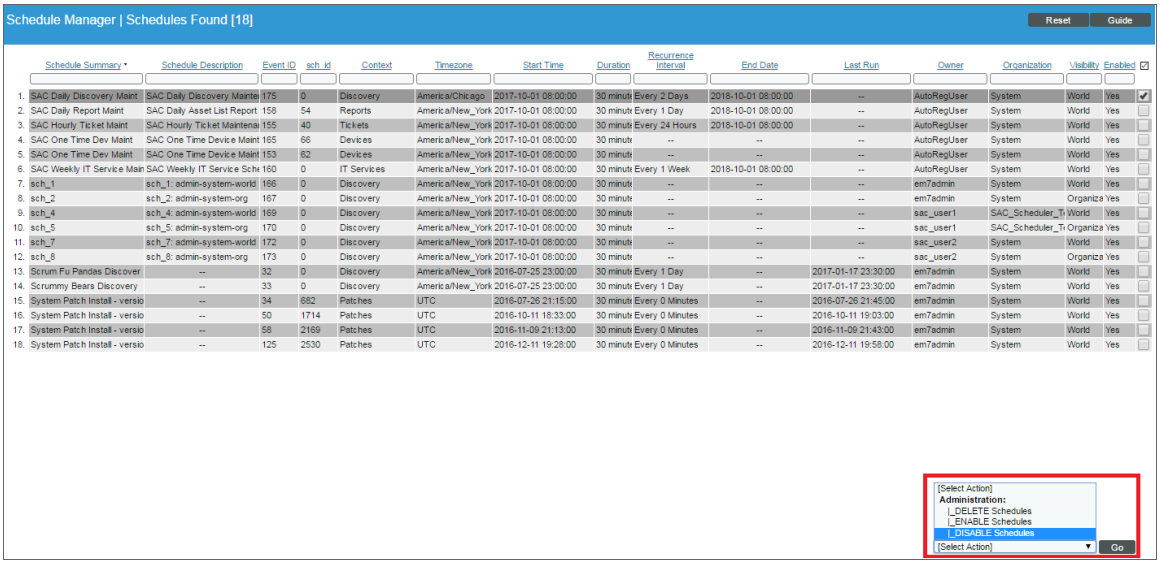


- ***Schedule Summary***. Displays the name assigned to the scheduled process.
- ***Schedule Description***. Displays a description of the scheduled process.
- ***Event ID***. Displays a unique, numeric ID for the scheduled process. SL1 automatically created this ID for each scheduled process.
- ***sch id***. Displays a unique, numeric ID for the schedule. SL1 automatically created this ID for each schedule.
- ***Context***. Displays the area of SL1 upon which the schedule works.
- ***Timezone***. Displays the time zone associated with the scheduled process.
- ***Start Time***. Displays the date and time at which the scheduled process will begin.
- ***Duration***. Displays the duration, in minutes, which the scheduled process occurs.
- ***Recurrence Interval***. If applicable, displays the interval at which the scheduled process recurs.
- ***End Date***. If applicable, displays the date and time on which the scheduled process will recur.
- ***Last Run***. If applicable, displays the date and time the scheduled process most recently ran.
- ***Owner***. Displays the username of the owner of the scheduled process.
- ***Organization***. Displays the organization to which the scheduled process is assigned.
- ***Visibility***. Displays the visibility level for the scheduled process. Possible values are "Private", "Organization", or "World".
- ***Enabled***. Specifies if the scheduled process is enabled. Possible values are "Yes" or "No".

Enabling or Disabling One or More Schedules

You can enable or disable one or more scheduled process from the **Schedule Manager** page (Registry > Schedules > Schedule Manager). To do this:

1. Go to the **Schedule Manager** page (Registry > Schedules > Schedule Manager).

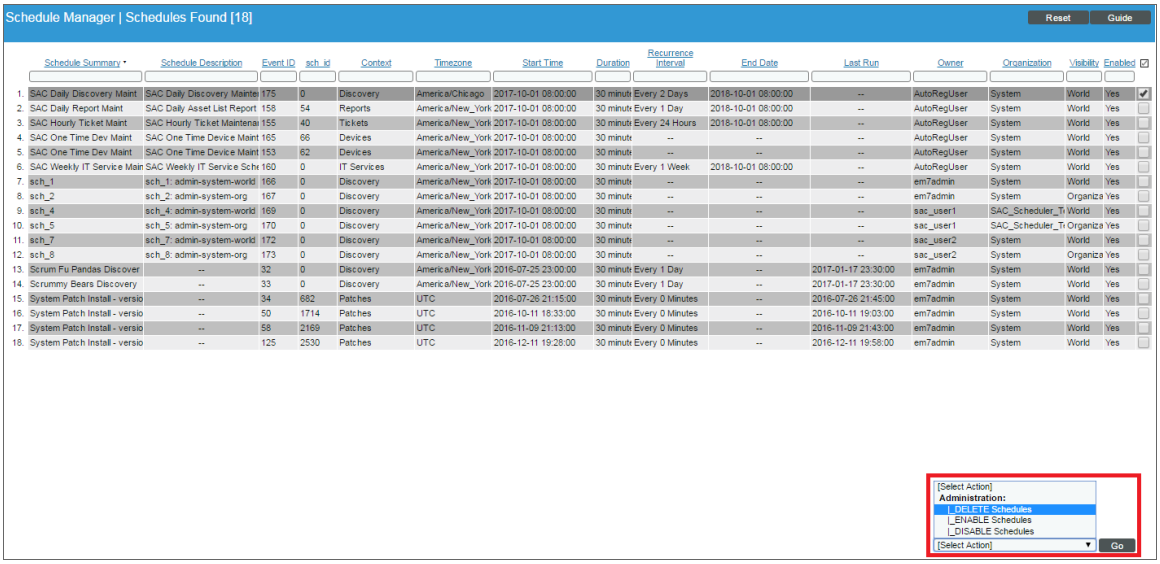


2. Select the checkbox icon for each scheduled process you want to enable or disable.
3. Click the ***Select Action*** menu and choose *Enable Schedules* or *Disable Schedules*.
4. Click the **[Go]** button.

Deleting One or More Schedules

You can delete one or more scheduled process from the **Schedule Manager** page (Registry > Schedules > Schedule Manager). To do this:

1. Go to the **Schedule Manager** page (Registry > Schedules > Schedule Manager).



2. Select the checkbox icon for each scheduled process you want to delete.
3. Click the ***Select Action*** menu and choose *Delete Schedules*.
4. Click the **[Go]** button.

Monitoring Overall System Usage and Statistics

The **System Usage** page displays:

- Tables that show the type and number of each type of task performed by SL1
- A pie graph showing the percent of the total data-collection load handled by each Data Collector or *Collector Group*
- An optional line graph that displays system usage. To enable the display of this graph, go to the **Behavior Settings** page (System > Settings > Behavior) and uncheck the ***Hide Perpetual License Count*** checkbox. The graph displays the following metrics over time:
    - ***Capacity***. The total monitoring capacity of the system. This value is determined by the license(s) for the Database Server(s) or All-In-One Appliance(s) in the system.
    - ***Number of Devices***. The number of devices currently discovered in the system.

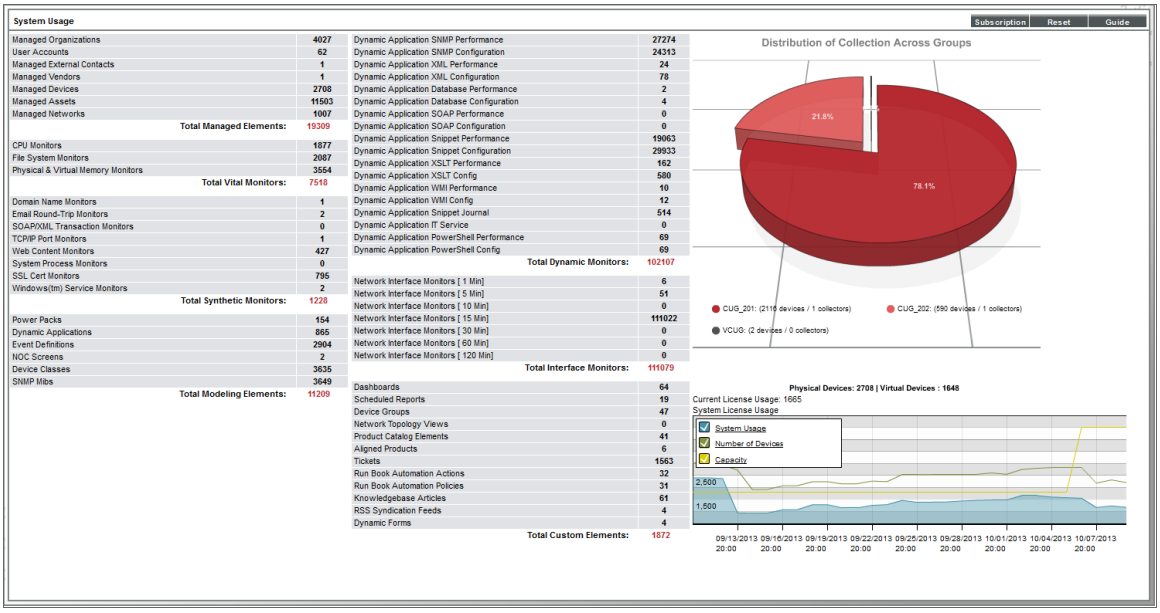
- ***System Usage***. The amount of ***Capacity*** that the devices in the system are currently using. This value is the sum of the ***Device Ratings*** for all devices in the system. The ***Device Rating*** for each device is calculated daily and is based on the number of collections performed for that device.

- If you have a subscription license, you can also generate reports about subscription licensing.

NOTE: The pie graph does not appear for All-In-One Appliances.

To view the **System Usage** page:

1. Go to the **System Usage** page (System > Monitor > System Usage).
2. The **System Usage** page appears:

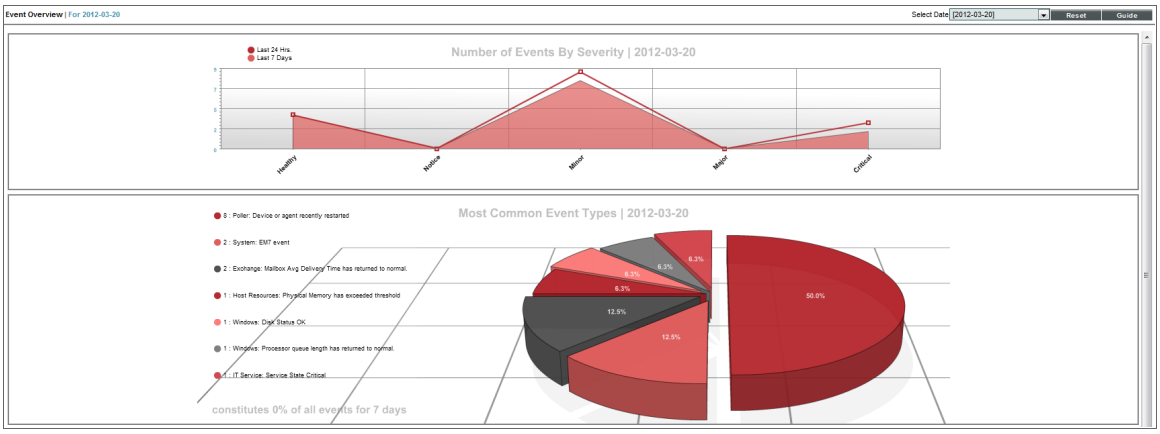


Viewing an Overview of All Events

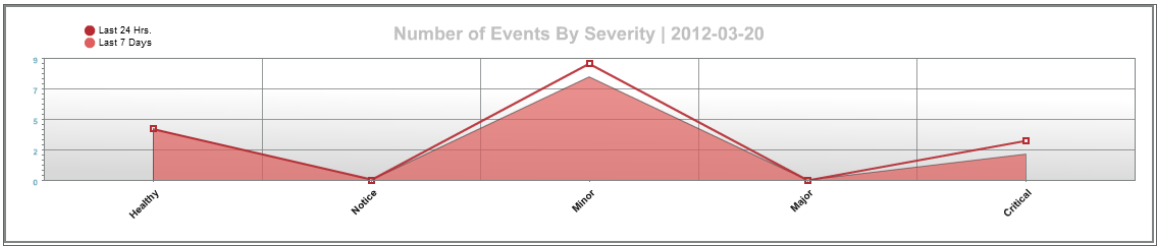
The **Event Overview** page provides a graphical overview of all events in SL1.

To view the **Event Overview** page:

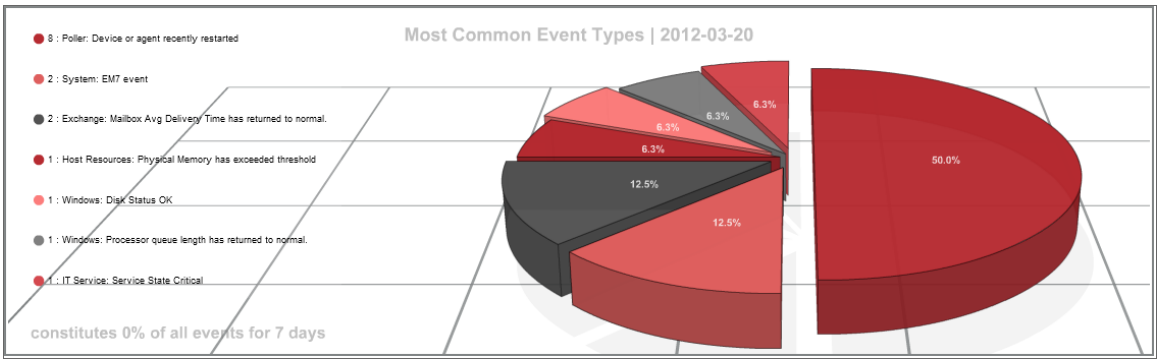
1. Go to the **Event Overview** page (System > Monitor > Event Overview).



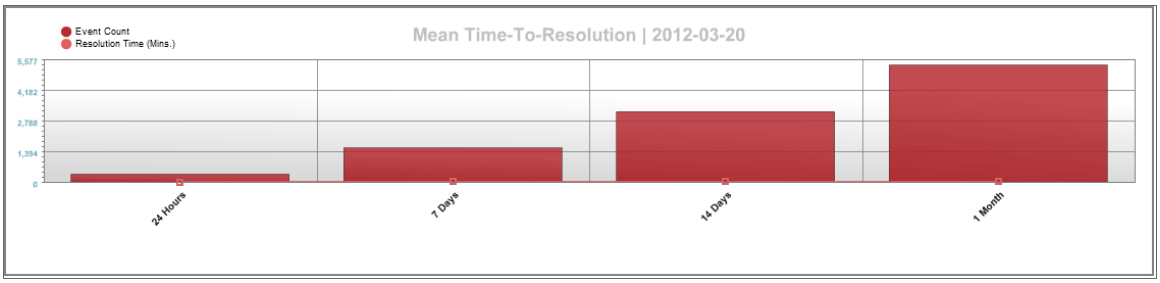
2. The **Event Overview** page displays the following reports:



- ***Number of Events by Severity***. This graph displays event distribution by severity for the last 24 hours and for the last 7 days.
    - The y-axis displays the number of events.
    - The x-axis displays severity.
    - The red line represents events in the last 24 hours.
    - The blue line represents events in the last 7 days.
    - Mousing over a data point in the red line displays the number of events of the specified severity in the last 24 hours.
    - Mousing over a data point on the blue line displays the number of events of the specified severity in the last 7 days.



- ***Most Common Event Types***. This pie graph displays the ten most frequently occurring events for the last 7 days.
    - Each slice of the pie represents an event type. The legend on the left maps each slice color to an event and lists the actual number of events of that type.
    - The graph displays percent. Compared to the total number of occurrences for the top ten events, each slice displays the percent that belong to a specific event.



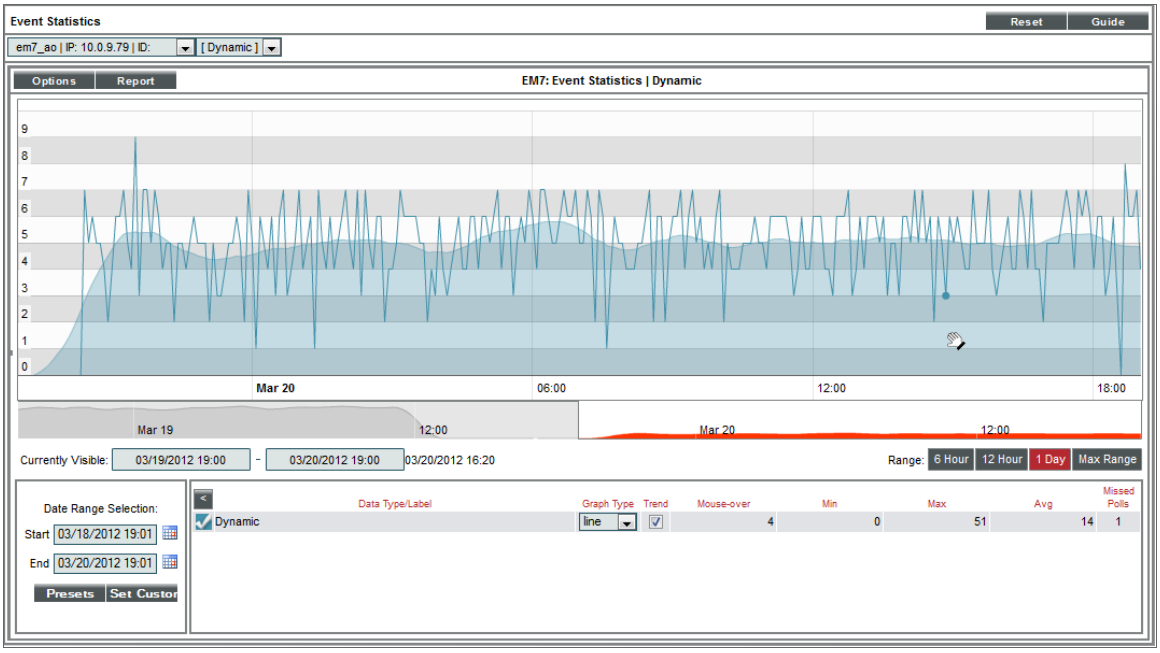
- ***Mean Time-to-Resolution***. This bar graph displays the number of events generated in the last 24 hours, 7 days, 14 days, and 30 days, and their average resolution time.
    - The y-axis displays the number of events.
    - The x-axis displays the time span. There is a bar for 24 hours, 7 days, 14 days, and 30 days.
    - The red bars represent the actual number of events associated with the time-to-resolution.
    - The blue bars represent the average number of events associated with the time-to-resolution.
    - Mousing over a bar displays the number of events associated with the time-to-resolution.

Viewing Events by Appliance and Event Source

The **Event Statistics** page displays a graph of the number of events processed by a selected Database Server, Data Collector, or Message Collector.

To generate the report:

1. Go to the **Event Statistics** page (System > Monitor > Event Statistics).



2. In the **Event Statistics** page, supply values in the following fields:

   - ***Appliance***. In the field in the upper left, select from the list of all Database Servers, Data Collectors, and Message Collectors.
   - ***Event Type***. In the field in the upper right, select from the list of event types. The choices are:
     - *Syslog*. Event was generated from standard system log generated by device.
     - *Internal*. Event was generated by SL1.
     - *Trap*. Event was generated by an SNMP trap.
     - *Dynamic*. Event was generated by a monitoring application running on the device.
     - *API*. The event was generated by an external API.
     - *Email*. The event was generated by an incoming email.

3. The graph displays the average number of events processed by the selected appliance, for the selected duration.

   - The y-axis displays the average number of events.
   - The x-axis displays time. The increments vary depending upon the selected data type (from the **[Options]** menu) and the date range (from the ***Date Range Selection*** pane).
   - Mousing over any point in any line displays the value at that time-point in the***Mouse-over*** column in the **Data Table** pane.

- You can use your mouse to scroll the report to the left and right.

Chapter 6

Diagnostic Tools

Overview

This chapter describes some diagnostic tools for troubleshooting and diagnosing problems in SL1.

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

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

This chapter includes the following topics:

Viewing Information About ScienceLogic Processes

The **Process Manager** page allows you to view a list of ScienceLogic processes and optionally define parameters for those processes. These processes gather, manipulate, and publish the data used in SL1.

CAUTION: ScienceLogic recommends that you do not edit the values in this page without first consulting ScienceLogic. Incorrect values can severely disrupt ScienceLogic platform operations.

ScienceLogic processes fall into three scheduling categories or *Frequencies*:

- ***Asynchronous***. The process is launched in response to a system event or user request.
- ***Scheduled***. The process is launched on a regular schedule.
- ***Always***. The process always runs while SL1 is running.

SL1 performs many tasks in parallel:

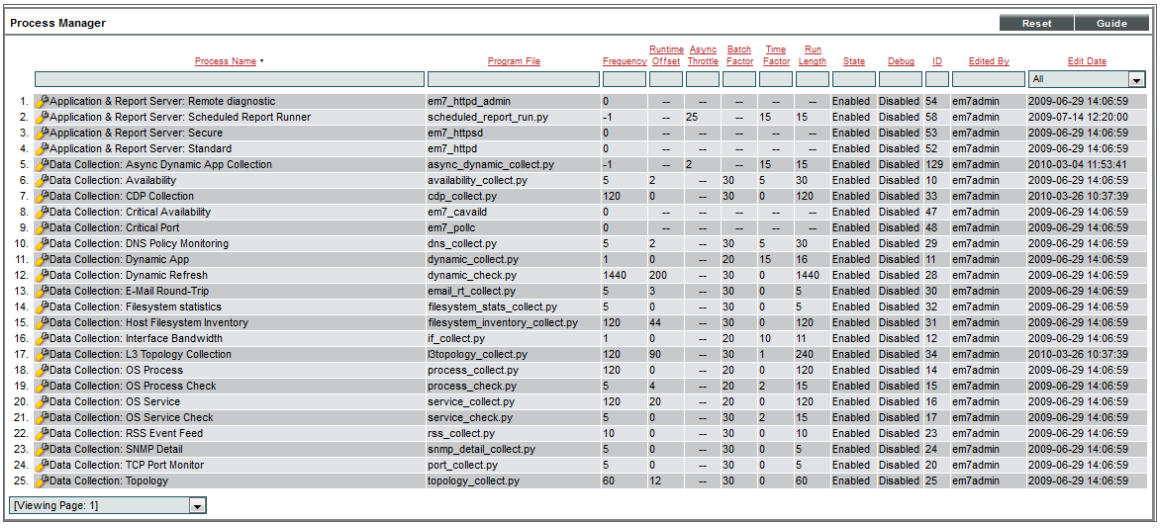
- Through a modular design, allowing functions to be distributed to multiple processing platforms.
- Through multi-processing, where multiple instances of a process run simultaneously.

The **Process Manager** page allows you to view and edit the parameters of system processes.

Viewing the List of ScienceLogic Processes

To view the list of process in the **Process Manager** page:

1. Go to the **Process Manager** page (System > Settings > Admin Processes).



Process Manager

Reset | Guide

	Process Name	Program File	Frequency	Runtime Offset	Async Throttle	Batch Factor	Time Factor	Run Length	State	Debug	ID	Edited By	Edit Date
													All
1.	Application & Report Server: Remote diagnostic	em7_httpd_admin	0	--	--	--	--	--	Enabled	Disabled	54	em7admin	2009-06-29 14:06:59
2.	Application & Report Server: Scheduled Report Runner	scheduled_report_run.py	-1	--	25	--	15	15	Enabled	Disabled	58	em7admin	2009-07-14 12:20:00
3.	Application & Report Server: Secure	em7_httpsd	0	--	--	--	--	--	Enabled	Disabled	53	em7admin	2009-06-29 14:06:59
4.	Application & Report Server: Standard	em7_httpd	0	--	--	--	--	--	Enabled	Disabled	52	em7admin	2009-06-29 14:06:59
5.	Data Collection: Async Dynamic App Collection	async_dynamic_collect.py	-1	--	2	--	15	15	Enabled	Disabled	129	em7admin	2010-03-04 11:53:41
6.	Data Collection: Availability	availability_collect.py	5	2	--	30	5	30	Enabled	Disabled	10	em7admin	2009-06-29 14:06:59
7.	Data Collection: CDP Collection	cdp_collect.py	120	0	--	30	0	120	Enabled	Disabled	33	em7admin	2010-03-26 10:37:39
8.	Data Collection: Critical Availability	em7_cavaild	0	--	--	--	--	--	Enabled	Disabled	47	em7admin	2009-06-29 14:06:59
9.	Data Collection: Critical Port	em7_pollc	0	--	--	--	--	--	Enabled	Disabled	48	em7admin	2009-06-29 14:06:59
10.	Data Collection: DNS Policy Monitoring	dns_collect.py	5	2	--	30	5	30	Enabled	Disabled	29	em7admin	2009-06-29 14:06:59
11.	Data Collection: Dynamic App	dynamic_collect.py	1	0	--	20	15	16	Enabled	Disabled	11	em7admin	2009-06-29 14:06:59
12.	Data Collection: Dynamic Refresh	dynamic_check.py	1440	200	--	30	0	1440	Enabled	Disabled	28	em7admin	2009-06-29 14:06:59
13.	Data Collection: E-Mail Round-Trip	email_rt_collect.py	5	3	--	30	0	5	Enabled	Disabled	30	em7admin	2009-06-29 14:06:59
14.	Data Collection: Filesystem statistics	filesystem_stats_collect.py	5	0	--	30	0	5	Enabled	Disabled	32	em7admin	2009-06-29 14:06:59
15.	Data Collection: Host Filesystem Inventory	filesystem_inventory_collect.py	120	44	--	30	0	120	Enabled	Disabled	31	em7admin	2009-06-29 14:06:59
16.	Data Collection: Interface Bandwidth	if_collect.py	1	0	--	20	10	11	Enabled	Disabled	12	em7admin	2009-06-29 14:06:59
17.	Data Collection: L3 Topology Collection	l3topology_collect.py	120	90	--	30	1	240	Enabled	Disabled	34	em7admin	2010-03-26 10:37:39
18.	Data Collection: OS Process	process_collect.py	120	0	--	20	0	120	Enabled	Disabled	14	em7admin	2009-06-29 14:06:59
19.	Data Collection: OS Process Check	process_check.py	5	4	--	20	2	15	Enabled	Disabled	15	em7admin	2009-06-29 14:06:59
20.	Data Collection: OS Service	service_collect.py	120	20	--	20	0	120	Enabled	Disabled	16	em7admin	2009-06-29 14:06:59
21.	Data Collection: OS Service Check	service_check.py	5	0	--	30	2	15	Enabled	Disabled	17	em7admin	2009-06-29 14:06:59
22.	Data Collection: RSS Event Feed	rss_collect.py	10	0	--	30	0	10	Enabled	Disabled	23	em7admin	2009-06-29 14:06:59
23.	Data Collection: SNMP Detail	snmp_detail_collect.py	5	0	--	30	0	5	Enabled	Disabled	24	em7admin	2009-06-29 14:06:59
24.	Data Collection: TCP Port Monitor	port_collect.py	5	0	--	30	0	5	Enabled	Disabled	20	em7admin	2009-06-29 14:06:59
25.	Data Collection: Topology	topology_collect.py	60	12	--	30	0	60	Enabled	Disabled	25	em7admin	2009-06-29 14:06:59

[Viewing Page: 1]

2. The **Process Manager** page displays information about each ScienceLogic process. The **Process Manager** page displays the following for each process:

   - ***Process Name***. Name of the process.
   - ***Program File***. Name of the executable file associated with the process.
   - ***Frequency***. Frequency with which the platform launches the process. Possible values are:
     - *Asynchronous*. The process is launched in response to a system event or user request.
     - *Always*. The process always runs while SL1 is running.
     - *Scheduled*. The process runs at intervals ranging from 1 Minute to Daily.
   - ***Runtime Offset***. This field applies only to scheduled processes and allows the platform to stagger the launch of a process. The field specifies the number of minutes after the default scheduled time to execute a process. The default scheduled time at which processes are initially executed is midnight UTC. So if a process has a ***Frequency*** of *5 Minutes* and the ***Runtime Offset*** is set to "2", the process will execute at two minutes past UTC midnight, seven minutes past UTC midnight, 12 minutes past UTC midnight, 17 minutes past UTC midnight, etc. Choices range from 0–1439.
   - ***Async Throttle***. This field applies only to asynchronous processes. This field indicates the number of jobs per process that can run simultaneously.
   - ***Batch Factor***. This field applies only to scheduled processes and determines how many multithreaded child processes are spawned on each execution of the process.

     *number of tasks a process is responsible for completing/**Batch Factor** = number of child processes that will be spawned*

     - The number of tasks is typically determined by the number of devices the process is collecting data from.
     - The maximum number of child processes is limited by the number of CPUs installed in the SL1 appliance that runs the process.
   - ***Time Factor***. Determines how long the process can run before being stopped by the process manager. This setting only applies to asynchronous processes and scheduled processes. For asynchronous processes, this is the length of time an instance of the process can run. For scheduled processes, the value of ***Time Factor*** is used to calculate ***Run Length***.

     (***Frequency*** * ***Time Factor***) + ***Frequency*** = ***Run Length***

     For example, suppose a process runs every 15 minutes (as specified in the ***Frequency*** field). A ***Time Factor*** of 2 means the process is allowed to run for 45 minutes. A ***Time Factor*** of 0 means the process is allowed to run for 15 minutes.
   - ***Run Length***. Specifies how long the process can run before being stopped by the process manager. This number is based on the ***Time Factor*** for the process.
   - ***State***. Current operational state of the process. Possible values are:
     - *Enabled*. Process can run.
     - *Disabled*. Process cannot run.

- ***Debug***. Specifies whether debugging information is enabled for the process. For more details on debugging a process, see the section ***Debugging a Process***.
- ***ID***. Unique numeric ID assigned to each process by SL1.
- ***Edited By***. Date and time the process settings were last edited.
- ***Edit Date***. Date and time the process settings were last edited.

Searching and Filtering the List of ScienceLogic Processes

The **Process Manager** page includes 13 filters, in the top row in the list of processes. You can specify one or more parameters to filter the display of processes. Only processes that meet all the filter criteria will be displayed in the **Process Manager** page.

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

- For each filter except ***Edit Date***, you must enter text to match against. SL1 will search for processes that match the text, including partial matches. Text matches are not case-sensitive. You can use the following special characters in each filter:
  - , (comma). Specifies an "or" operation. For example:

    "dell, micro" would match all values that contain the string "dell" OR the string "micro".
  - & (ampersand). Specifies an "and" operation. For example:

    "dell & micro" would match all values that contain the string "dell" AND the string "micro".
  - ! (exclamation mark). Specifies a "not" operation. For example:

    "!dell" would match all values that do not contain the string "dell".
- ***Process Name*** You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Process Manager** page will display only processes that have a matching name.
- ***Program File***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Process Manager** page will display only processes that have a matching program file.
- ***Frequency*** . You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Process Manager** page will display only processes that have a matching frequency number.
- ***Runtime Offset***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Process Manager** page will display only processes that have a matching runtime offset.
- ***Async Throttle***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Process Manager** page will display only processes that have a matching throttle number.
- ***Batch Factor***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Process Manager** page will display only processes that have a matching batch factor.

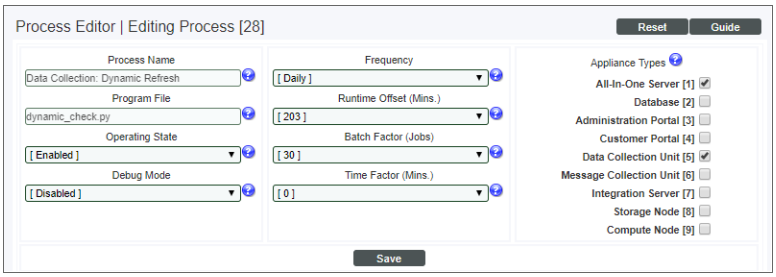
- ***Time Factor***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Process Manager** page will display only processes that have a matching time factor.
- ***Run Length***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Process Manager** page will display only processes that have a matching run length.
- ***State***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Process Manager** page will display only processes that have a matching state ("Enabled" or "Disabled").
- ***Debug***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Process Manager** page will display only processes that have a matching debug state ("Enabled" or "Disabled").
- ***ID***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Process Manager** page will display only processes that have a matching ScienceLogic process ID.
- ***Edited By***. You can enter text to match, including special characters (comma, ampersand, and exclamation mark), and the **Process Manager** page will display only processes that have a matching"created by" or "edited by" value.
- ***Edit Date***. You can select from a list of time periods. The **Process Manager** page will display only processes that have been created or edited within that time period:
    - *All*. Display all processes that match the other filters.
    - *Last Minute*. Display only processes that have been edited within the last minute.
    - *Last Hour*. Display only processes that have been edited within the last hour.
    - *Last Day*. Display only processes that have been edited within the last day.
    - *Last Week*. Display only processes that have been edited within the last week.
    - *Last Month*. Display only processes that have been edited within the last month.
    - *Last Year*. Display only processes that have been edited within the last year.

Editing the Parameters of a ScienceLogic Process

To view details about a specific process or edit the settings for a specific process:

> CAUTION: ScienceLogic recommends that you do not edit the values in this page without first consulting ScienceLogic. Incorrect values can severely disrupt ScienceLogic platform operations.

1. Go to the **Process Manager** page (System > Settings > Admin Processes).
2. In the **Process Manager** page, find the process you want to edit. Click its wrench icon ().



3. The **Process Editor** page appears and is populated with values from the selected process.

   - ***Process Name***. Name of the process. This field is read-only and cannot be changed.
   - ***Program File***. Name of the executable file associated with the process. This field is read-only and cannot be changed.
   - ***Operating State***. Current operational state of the process. Specifies whether the process is enabled and able to run. Select from the drop-down list. The choices are:
     - *Enabled*. Process can run.
     - *Disabled*. Process cannot run.
   - ***Debug Mode***. Enables or disables debugging information for a process. For more details on debugging a process, see the section ***Debugging a Process***.

NOTE: You cannot enable debug mode for the process *Message Collection: SNMP Trap*.

   - ***Frequency***. This field appears only for scheduled processes and asynchronous processes. Specifies the frequency with which SL1 launches the process. Select from the drop-down list. The choices are:
     - *Asynchronous*. For asynchronous processes, this is the only available option. You cannot edit the frequency.
     - *Scheduled*. For scheduled processes, you can edit the frequency. You can select from intervals ranging from 1 Minute to Daily.

NOTE: If a process is set to a frequency of *Asynchronous* or *Always*, this field cannot be changed. If a process is set to a time interval, this field cannot be changed to *Asynchronous* or *Always*.

   - ***Async Throttle***. This field appears only for asynchronous processes. This field indicates the number of jobs per process that can run simultaneously. This setting only applies to asynchronous processes.
   - ***Runtime Offset***. This field only appears for scheduled processes. This field allows SL1 to stagger the launch of a process. The value specified in this field specifies minutes after the default scheduled time for a process. For example, if a process has a ***Frequency*** of *5 Minutes* and the ***Minute Offset*** is set to "2", the process will execute at two minutes past the hour, seven minutes past the hour, 12 minutes past the hour, 17 minutes past the hour, etc. Choices range from 0–1439.

- ***Batch Factor***. This field applies only to scheduled processes and determines how many multithreaded child processes are spawned on each execution of the process.

  *number of tasks a process is responsible for completing/**Batch Factor** = number of child processes that will be spawned*

  - The number of tasks is typically determined by the number of devices the process is collecting data from.
  - The maximum number of child processes is limited by the number of CPUs installed in the SL1 appliance that runs the process.

- ***Time Factor***. This field appears only for scheduled processes and asynchronous processes. This field determines how long a process can run before being killed.

  - For scheduled processes, SL1 uses the formula (***Frequency*** * ***Time Factor***) + ***Frequency***.

    For example, suppose a process runs every 15 minutes. A factor of 2 means the process is allowed to run for 45 minutes. Factor of 0 means process is allowed to run for 15 minutes.

  - For asynchronous processes, SL1 simply uses the value in this field as the number of minutes a process can run. This field does not appear for processes that are always running.

- ***Appliance Types***. Specifies the appliance types where the process is allowed to run.

NOTE: All changes to the settings in the **Process Manager** page are logged in the **Audit Logs** page (System > Monitor > Audit Logs). The associated log entry will specify the user who altered a process, the process that was altered, and which settings for the process were changed.

4. If you make changes to one or more fields, click the **[Save]** button to save your changes.

Debugging a Process and Viewing Debug Logs

When you debug a process, you tell SL1 to use verbose logging for that process. You can then view SL1 log file to view the logs.

There might be circumstances where you have narrowed down a problem to a specific ScienceLogic process (for example, based on an error message or event). When this happens, you might find it helpful to turn on debugging for that process and view the debug logs.

WARNING: ScienceLogic recommends that you enable the debug option only while troubleshooting a problem and that you then immediately turn off debugging when you have completed troubleshooting. Don't leave the debug option enabled during normal operation of SL1. When you turn on debugging, SL1 will run significantly more slowly.

NOTE: You cannot enable debug mode for the process *Message Collection: SNMP Trap*.

To enable the debug option for a process:

1. In the **Process Manager** page, find the process you want to edit. Select its wrench icon ( ).
2. The **Process Editor** page appears and is populated with values for the selected process.
3. Edit the following field:
   - ***Debug***. Enables or disables debugging information for a process. Select *Enabled*.
4. Click the **[Save]** button in the **Process Editor** page.
5. Log in to the console of the appliance where the process is running. Alternately, you can use SSH to open a shell session on the appliance. Log in as ***em7admin*** with the appropriate password. The default password is ***em7admin***.

TIP: To view a list of IP addresses for all appliances in your system, go to the **Appliance Manager** page (System > Settings > Appliances).

6. If the process you are debugging is a process that has a ***Frequency*** of *Always*, you must restart the process to make it pick up the new debug status (enabled). To restart the process, enter the following at the shell prompt:

```
sudo service process_name restart
```

   For example, if you were debugging the process for the event engine, you would enter:

```
sudo service em7_event restart
```

7. Navigate to the directory **/var/log/em7**. View the file **silo.log**. The most recent entries will be posted at the end of the file.
8. After you have finished troubleshooting the process, remember to disable debugging. If the process has a ***Frequency*** of *Always*, you must restart the process to make it pick up the new debug status (disabled).

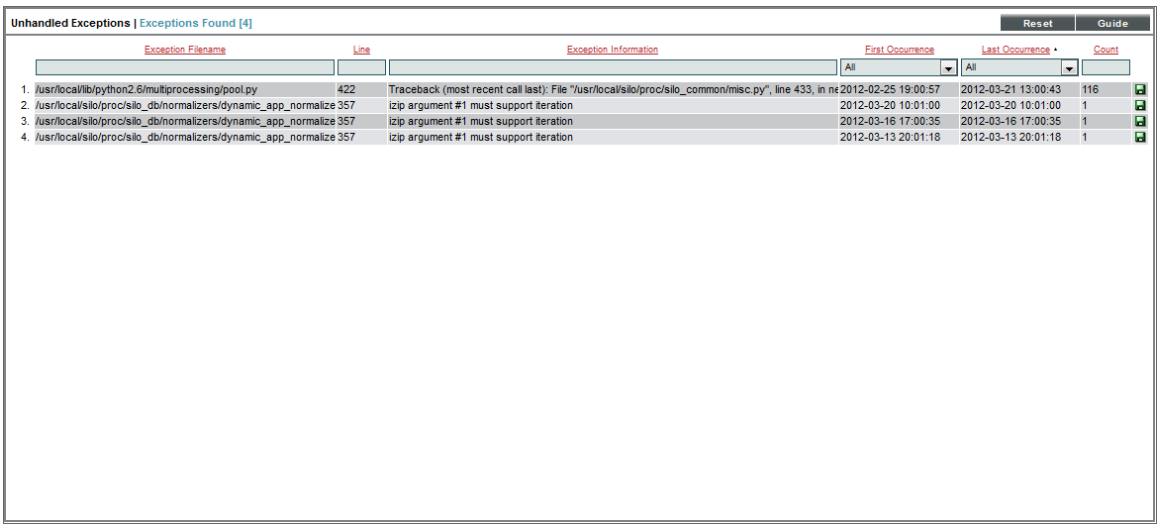
Viewing Information About Unhandled Exceptions

An ***exception*** specifies that something happened "out of the norm" that is preventing the software from executing the next step. Exceptions are a specific type of error, usually the result of invalid input, missing input, or a network error that prevents communication between software modules. For most exceptions, SL1 will handle the exception by logging a specific error in the System Logs and will continue to run the process. However, ***if the platform does not handle the exception***, the process will stop running, and SL1 will generate an error message describing ***the unhandled exception***.

Viewing the List of Unhandled Exceptions

To view the list of unhandled exceptions for all appliances:

1. Go to the **Unhandled Exceptions** page (System > Monitor > Unhandled Exceptions).
2. The **Unhandled Exceptions** page displays the following for each unhandled exception:



- ***Exception Filename***. Full path of the file where the exception occurred.
- ***Line***. Line number of the line in the file where the exception occurred.
- ***Exception Information***. Error message associated with the exception.
- ***First Occurrence***. Date and time of the first occurrence of the exception.
- ***Last Occurrence***. Date and time of the last occurrence of the exception.
- ***Count***. Number of times the exception has occurred.

Searching and Filtering the list of Unhandled Exceptions

The **Unhandled Exceptions** page includes six filters. You can filter the list of exceptions by one or multiple of the following parameters: exception filename, line number, exception descriptions, first occurrence, last occurrence, and count. Only exceptions that meet all the filter criteria will be displayed in the **Unhandled Exceptions** page.

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

- For the first three filters, you must enter text to match against. SL1 will search for exceptions that match the text, including partial matches. Text matches are not case sensitive. You can use the following special characters in each filter:
    - , Specifies an "or" operation. For example:

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

- **!** Specifies a "not" operation. For example:

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

- ***Exception Filename***. You can enter text to match, including special characters, and the **Unhandled Exceptions** page will display only exceptions that have a matching filename.
- ***Line***. You can enter text to match, including special characters, and the **Unhandled Exceptions** page will display only exceptions that have a matching line number.
- ***Exception Information***. You can enter text to match, including special characters, and the **Unhandled Exceptions** page will display only exceptions that have a matching description.
- ***First Occurrence***. Only those exceptions that match all the previously selected fields and have the specified first occurrence date will be displayed. The choices are:
  - *All*. Display exceptions with all first occurrence dates.
  - *Last Minute*. Display only exceptions that first occurred within the last minute.
  - *Last Hour*. Display only exceptions that first occurred within the last hour.
  - *Last Day*. Display only exceptions that first occurred within the last day.
  - *Last Week*. Display only exceptions that first occurred within the last week.
  - *Last Month*. Display only exceptions that first occurred within the last month.
  - *Last Year*. Display only exceptions that first occurred within the last year.
- ***Last Occurrence***. Only those exceptions that match all the previously selected fields and have the specified last occurrence date will be displayed. The choices are:
  - *All*. Display exceptions with all last occurrence dates.
  - *Last Minute*. Display only exceptions that last occurred within the last minute.
  - *Last Hour*. Display only exceptions that last occurred within the last hour.
  - *Last Day*. Display only exceptions that last occurred within the last day.
  - *Last Week*. Display only exceptions that last occurred within the last week.
  - *Last Month*. Display only exceptions that last occurred within the last month.
  - *Last Year*. Display only exceptions that last occurred within the last year.
- ***Count***. You can enter text to match, including special characters, and the **Unhandled Exceptions** page will display only exceptions that have a matching count number.

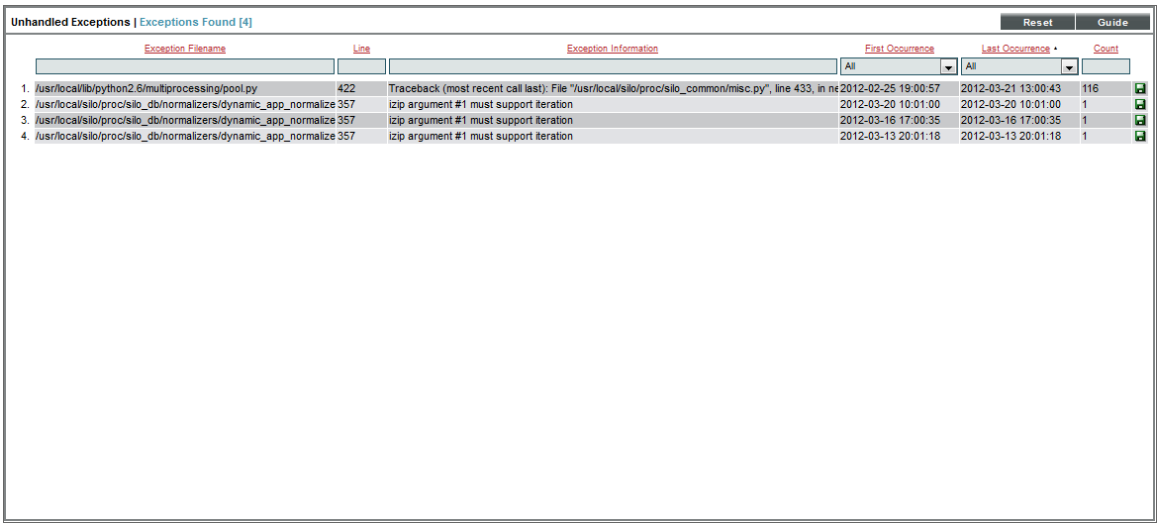
Saving the Unhandled Exception to the Local Computer

You can save the full text of the unhandled exception to a file on your local computer. You can then view the text in a text editor.

To save the full text of the unhandled exception to a file:

1. Go to the **Unhandled Exceptions** page (System > Monitor > Unhandled Exceptions).

2. In the **Unhandled Exceptions** page, find the exception you want to save to a file. Click its green diskette icon ( ).



3. When prompted, you can either immediately view the text file with a text editor or save the file to your local computer for viewing later.

Viewing the Database Tables on the Database Server

In some circumstances, you might need to view the contents of the database tables (the permanent tables are stored on the Database Server). There are two ways to do this:

- Using the built-in Database Tools in the **Database Tool** page (System > Tools > DB Tool).
- Using the link to the phpMyAdmin interface in the **Appliance Manager** page (System > Settings > Appliances).

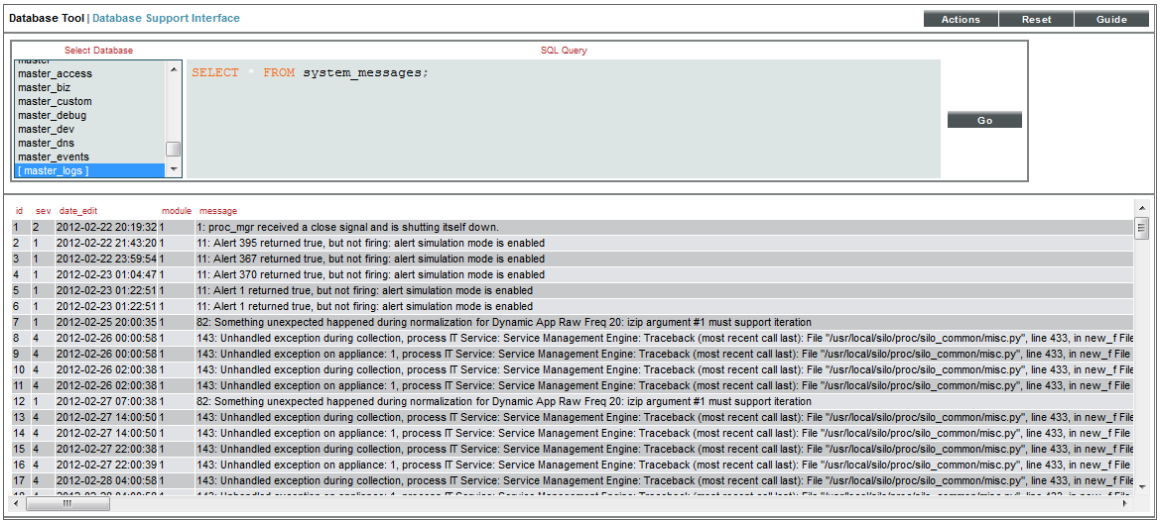
Accessing the Database Tool

The **Database Tool** page allows administrators to view information about the internal ScienceLogic databases and run SQL queries against those internal databases.

CAUTION: Contact ScienceLogic for details on using the **Database Tool** page and troubleshooting databases. Do not make changes to the database or run the Optimizer Tool without guidance from ScienceLogic.

To access the database tool:

1. Go to the **Database Tool** page (System > Tools > DB Tool).



2. ***To run an SQL query*** from the **Database Tool** page, enter values in the following fields:

   - ***Select Database***. Select a database to query.
   - ***SQL Query***. Enter an SQL query to execute against the selected database. For more information on each database and each table, use the options in the **[Actions]** menu.

NOTE: You must be familiar with SQL and know how to build a proper query before using the **Database Tool** page.

3. Click the **[Go]** button to execute the query.
4. The results from the query are displayed in the pane at the bottom of the page.
5. ***To view the reports*** about the a database(s), click the **[Actions]** menu. The following options are available:

   - ***Engines***. Displays status information about the server's storage engines. For each engine, the modal page displays a description of the engine, whether the engine is supported by SL1, and whether or not the engine supports transactions, XA, and save points.
   - ***Global Status***. Displays a list of global variables used in the database tables and the current value for each global variable.
   - ***InnoDB Variables***. Displays a list of InnoDB variables used in SL1 and the value for each variable.
   - ***Open Tables***. Displays a list of currently open tables. For each table, the modal page displays the database name, table name, whether the table is currently in use, and whether the table is currently locked.

- ***Optimizer Tool***. Leads to the **Database Optimizer Tool** page, where you can choose to optimize, repair, check, flush, or analyze all the tables in a database.

CAUTION: Contact ScienceLogic for details on using the **Database Optimizer Tool** page. Do not run the Optimizer Tool without guidance from ScienceLogic.

- ***Processes***. Displays a list of running threads on the databases and tables. For each process, the modal page displays the connection ID, the database user who issued the statement, the host name of the client that issued the statement, the affected database, the command, the time in seconds that the thread has been in its current state, the state of the thread, and any available description of the process.
- ***Table Status***. Displays the status of each database table in the platform. For each table, the modal page displays the table name, the database engine, database version, row format, number of rows, average row-length, length of the data file, maximum length of the data file, length of the index file, number of allocated but unused bytes, the next auto-increment value, the create time for the table, the update time for the table, the table's character set and collation, the live checksum value, options used with CREATE TABLE, and any comments.
- ***Variables***. Displays a list of all database system variables used in SL1 and the value of each variable.

Disabling Normalization, Re-Enabling Normalization, and Backfilling Raw Data

ScienceLogic does not recommend stopping normalization on Data Collectors. However, there are rare occasions where ScienceLogic Customer Support might ask you to disable normalization as part of troubleshooting.

To disable normalization:

1. Either go to the console of the Database Server or use SSH to access the Database Server.
2. Log in as user em7admin with the appropriate password.
3. Type the following at the command line:

```
sudo vi /etc/siteconfig/siloconf.siteconfig
```

4. This is the file where users can customize the silo.conf file. In step #7, you will execute a command that sends these changes to the system silo.conf file.
5. In the LOCAL section, add the following line:

```
rollups_disabled=ON
```

6. Save your changes and exit the file (:wq).
7. At the command line, type the following command to rebuild the configuration file:

```
sudo /opt/em7/share/scripts/generate-silo-conf.py > silo.conf
```

8. You must restart the data collection process to ensure they receive the change. Type the following at the command line:

```
sudo service em7_hfpulld restart
sudo service em7_lfpulld restart
sudo service em7_mfpulld restart
```

To re-enable normalization and normalize data that was collected while normalization was disabled:

1. Either go to the console of the Database Server or use SSH to access the Database Server.
2. Log in as user em7admin with the appropriate password.
3. Type the following at the command line:

```
sudo vi /etc/siteconfig/siloconf.siteconfig
```

4. This is the file where users can customize the silo.conf file. In step #7, you will execute a command that sends these changes to the system silo.conf file.
5. In the LOCAL section, add the following line:

```
rollups_disabled=OFF
```

6. Save your changes and exit the file (:wq).
7. At the command line, type the following command to rebuild the configuration file:

```
sudo /opt/em7/share/scripts/generate-silo-conf.py > silo.conf
```

8. You must restart the data collection process to ensure they receive the change. Type the following at the command line:

```
sudo service em7_hfpulld restart
sudo service em7_lfpulld restart
sudo service em7_mfpulld restart
```

9. At the command line, type the following to normalize the data that was collected while normalization was disabled:

```
[/opt/em7/backend/data_normalizer_backfill.py --database, <database> --dids <
[device IDs]> --start <start date> --end <end date> --workers <number of workers>
```

NOTE: To get help, at the shell prompt, type "/opt/em7/backend/data_normalizer_backfill.py -h".

where:

- --database *database*. Specifies the database that you want to backfill with normalized data. The choices are:
    - data_avail. Table that stores normalized data for availability.
    - data_cv. Table that stores normalized data for Web Content policies.
    - data_dns. Table that stores normalized data for DNS policies.

    - data_email. Table that stores normalized data for Email Round-Trip policies.
    - data_ports. Table that stores normalized data for TCP-IP Ports policies.
    - data_procs. Table that stores normalized data for System Processes policies.
    - data_services. Table that stores normalized data for Windows Services policies.
    - data_storage. Table that stores normalized data for file systems.
    - data_tv. Table that stores normalized data for SOAP/XML Transaction policies.
    - dynamic_app_data_*appID*. Table that stores normalized data for a Dynamic Application. Specify the application ID for the Dynamic Application.

- --dids *device IDs*. Specifies the device ID of the device or devices for which you want to normalize data.
    - You can specify a single device ID.
    - You can specify multiple device IDs, separated by commas and surrounded by square brackets.
    - If you do not specify any device IDs, SL1 will normalize the specified data for all devices in your system.

- --start *start date*. The timestamp that specifies the data to normalize. Raw data with a time stamp at this time or later will be normalized. SL1 will normalize data starting with this timestamp and ending with the end-date timestamp.
    - Specify the timestamp in the format yyyy-mm-dd hh:mm:ss, using a 24-hour clock. Surround the timestamp with single quotes.

- --end *end date*. The timestamp that specifies the data to normalize. Raw data with a time stamp at this time or earlier will be normalized. SL1 will normalize data starting with the start-date timestamp and ending with this timestamp.
    - Specify the timestamp in the format yyyy-mm-dd hh:mm:ss, using a 24-hour clock. Surround the timestamp with single quotes.

- --workers *workers*. Number of worker processes to assign to this task. This field is optional. Please consult ScienceLogic Customer Support for suggestions on worker processes.

  For example:

```
python /opt/em7/backend/data_normalizer_backfill.py --database dynamic_app_data_16 -
-start '2017-10-01 00:00:00' --end '2017-10-10 00:00:00' --workers 10
```

  This command normalizes raw data collected by the Dynamic Application with an application ID of 16, associated with all subscriber devices (no device IDs specified, so defaults to "all devices"), and that was collected between midnight on October 1, 2017 and midnight on October 10, 2017. The data_normalizer_backfill.py code uses ten worker processes to perform the normalization.

Chapter 7

Changing Passwords and IP Addresses

Overview

This chapter describes how to:

- Change every administrator password used in SL1.
- Disable root access.
- Change the IP address of an appliance.

> **NOTE:** Appliances installed as an AWS EC2 instance have the "root" operating system account disabled by default. During the setup process, the user "ec2-user" is automatically added to the operating system configuration. The ec2-user account can be used to perform administrative tasks that require SSH command-line access. The ec2-user account is permitted to perform all operating system commands using the "sudo" command without a password.

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

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

This chapter includes the following topics:

Disabling phpMyAdmin

The phpMyAdmin interface provides a web interface for viewing and managing MySQL databases. By default, you can log in to the Database Server server using the phpMyAdmin interface to view and manage the MySQL databases on all Database Servers, Data Collectors, and Message Collectors in the system.

To disable phpMyAdmin, you must disable the service and then disable the ports on which the service runs. To do this:

1. If you are using a distributed system, either go to the console of the Database Server or use SSH to access the Database Server. Open a shell session on the server. Log in as "root".
2. If you are using an All-In-One Appliance, either go to the console of the All-In-One Appliance or use SSH to access the All-In-One Appliance. Open a shell session on the server. Log in as "root".

NOTE: For details on enabling and using SSH, see the manual ***System Administration***. For details and warnings about root access and instructions on how to make root access secure, see the manual ***System Administration***.

3. Open a vi session to edit the file /etc/siteconfig/firewalld-rich-rules.siteconfig
4. Add the following lines:

```
rule service name="phpmyadmin" reject
rule port port="8008" protocol="tcp" reject
```

5. Save your changes and exit the file.
6. Tell SL1 to pick up the changes to firewalld. To do this, type the following at the command line:

```
sudo /opt/em7/share/scripts/update-firewalld-conf.py
```

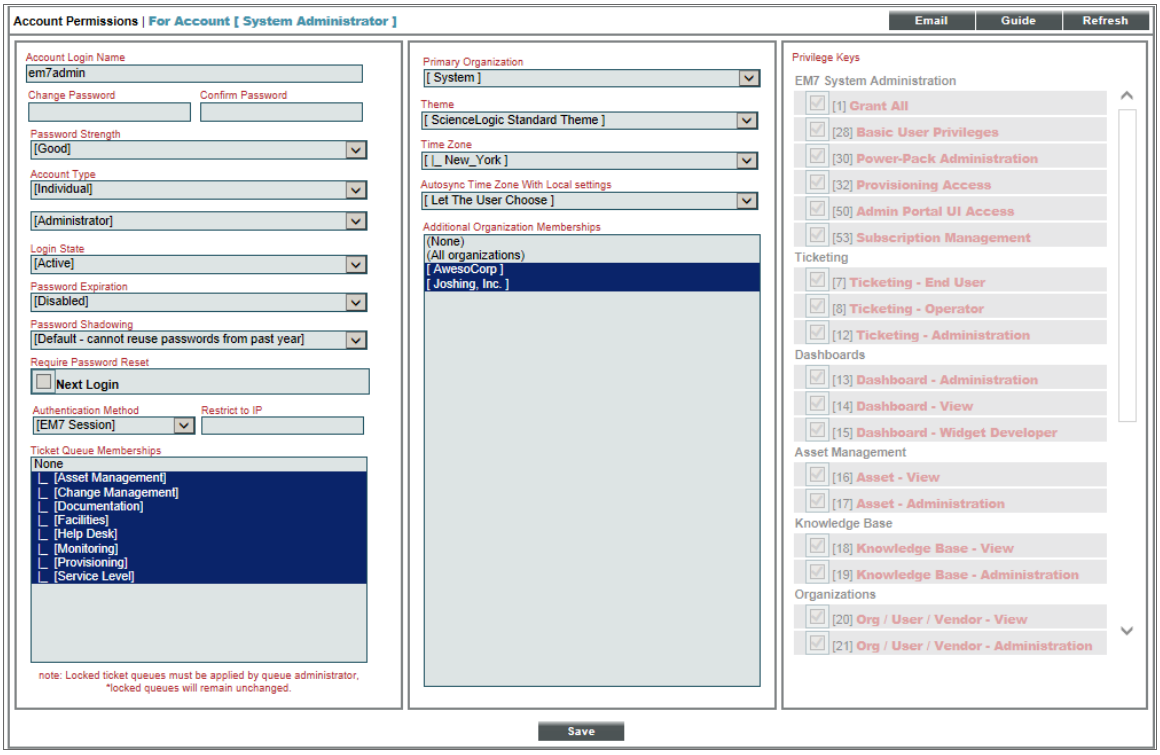
7. Restart the firewall services so that the phpMyAdmin service and port 8008 will no longer be allowed. To do this, type the following at the command line:

```
sudo systemctl restart firewalld
sudo systemctl restart nginx
```

Changing the Password for the Default Account for the User Interface

To change the password for the default em7admin user account, which can be used to access the user interface, perform the following steps:

1. Go to the **User Accounts** page (Registry > Accounts > User Accounts).
2. Click the wrench icon ( ) for the em7admin user. The **Account Permissions** page appers.



3. Enter the new password in the ***Change Password*** field.
4. Re-type the new password in the ***Confirm Password*** field.
5. Click the **[Save]** button. A pop-up window appears, asking you to confirm the change.
6. Click "OK" in the pop-up window. The message "Password Saved" is displayed.

Changing the Password for the Default Console User

To change the password for the default administrative user ***em7admin*** for console logins and SSH access:

1. Either go to the console of the SL1 appliance or use SSH to access the server.
2. Log in as user ***em7admin*** with the appropriate password. The default password is ***em7admin***.
3. At the shell prompt, type the following:

   ```
   passwd
   ```

4. When prompted, type and re-type the new password.

Changing the Password for the Web Configuration Utility

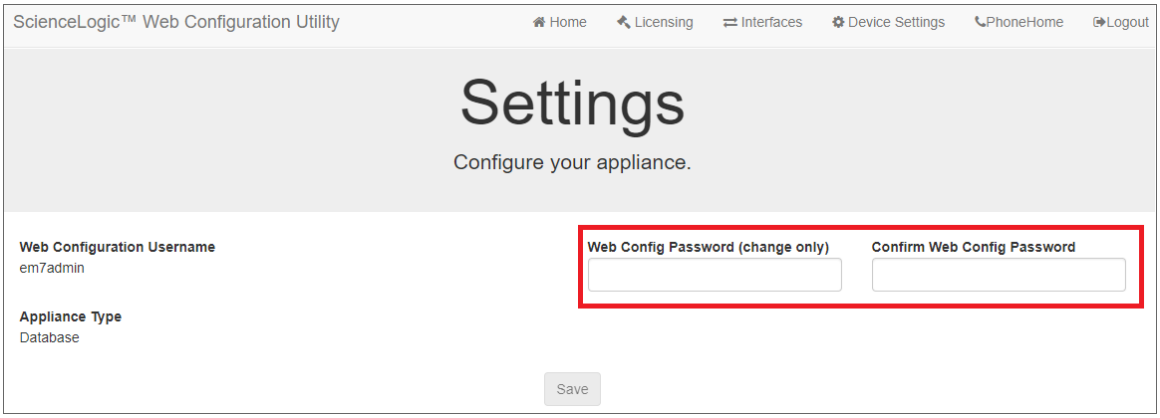
You can change the password for the Web Configuration Utility.

NOTE: If you want to change the password for the Web Configuration Utility on all SL1 appliances, you must log in to the Web Configuration Utility on each appliance and perform the steps in this section.

NOTE: You cannot change the username for the Web Configuration Utility. The username remains ***em7admin***.

To change the password for the Web Configuration Utility:

1. Log in to the Web Configuration Utility. The **Configuration Utilities** page appears.
2. Click the **[Device Settings]** button. The **Settings** page appears.



3. In the **Settings** page, type the following:

- ***Web Config Password (change only)***. Type the new password.
- ***Confirm Web Config Password***. Type the new password again.

4. Click **[Save]**
5. Perform steps 1-4 for each appliance for which you want to change the password for the Web Configuration Utility.

Changing Database Passwords

The following SL1 appliances include a database instance:

- All-In-One Appliances
- Database Servers
- Data Collectors
- Message Collectors

By default, SL1 appliances use the following user accounts to access appliance databases:

- ***ap_user***. This user is used by the user interface to access the database on a Database Server or All-In-One Appliance. This user account exists only on the Administration Portal and does not exist by default on Data Collectors and Message Collectors. By default, this user has the user name ***apuser*** and the password ***apuser***.
- ***dbuser***. This user is used by ScienceLogic platform processes to access the database instance on all appliances. By default, this user has the user name ***root***.

To change the password for the ***ap_user*** account, you must:

1. Configure a new password for the Administration Portal using the Web Configuration Utility for the Administration Portal.

To change the password for these ***dbuser*** account, you must:

1. Configure a new password in the database instance.
2. Configure SL1 to use the new password.

Configuring a New Password in the Database Instance

Perform the following steps to change the password for a user in the database instance:

1. Either go to the console of the Database Server, All-In-One Appliance, Data Collector, or Message Collector or use SSH to access the server.
2. Log in as ***em7admin*** with the appropriate password.
3. Execute the following commands, entering the username ***root*** and the new password where indicated:

```
silo_mysql
set password for '<username>'=PASSWORD('<new password>');
```

```
set password for '<username>'@'localhost'=PASSWORD('<new password>');
```

4. In a distributed system, perform steps 1-3 on each Database Server, Data Collector, or Message Collector

Configuring the Platform to Use the New Password

If you changed the ***root*** password for a Database Server or All-In-One Appliance, you must update the password in the following locations:

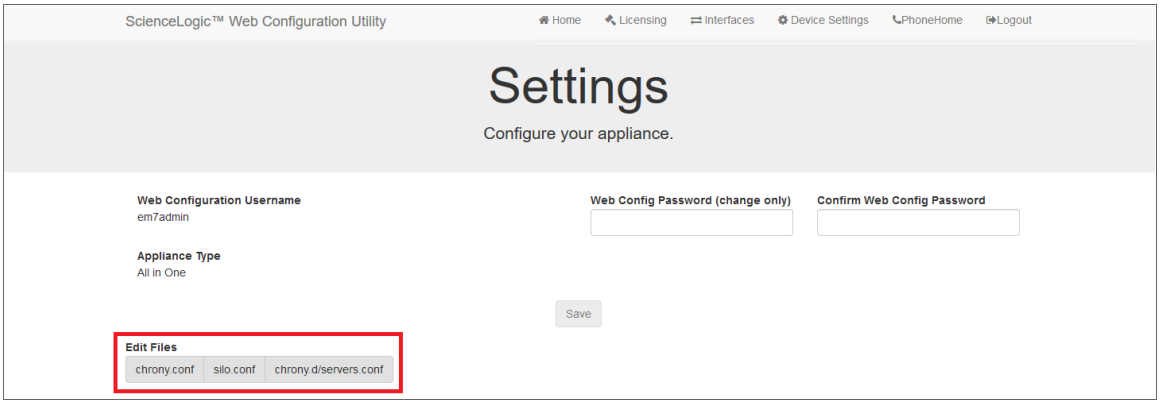
- In the silo.conf file on the Database Server or All-In-One Appliance itself. You must change the value for the ***dbpasswd*** option in the [CENTRAL] and [LOCAL] sections of silo.conf.
- In the silo.conf file on the Database Server or All-In-One Appliance itself. You must change the value for the ***ap_pass*** option in the [CENTRAL] section of the silo.conf file.
- In the silo.conf file on all Administration Portals in your system. You must change the value for the ***dbpasswd*** option in the [CENTRAL] section of silo.conf.
- In the silo.conf file on all Administration Portals in your system. You must change the value for the ***ap_pass*** option in the [CENTRAL] section of the silo.conf file.
- By default, SL1 uses the root password for a Database Server to connect to all Data Collectors and Message Collectors. If you changed the root password for a Database Server but did not change the root password for the Data Collectors and Message Collectors, you must *update the master.system_settings_licenses table* on the Database Server with the root password for all Data Collectors and Message Collectors.

If you changed the ***root*** password for a Data Collector and/or Message Collector, you must update the password in the following locations:

- In the silo.conf file on the Data Collector and/or the Message Collector itself. You must change the value for the ***dbpasswd*** option in the [LOCAL] section of silo.conf.
- In the master.system_settings_licenses table on the Database Server.

Editing Silo.Conf

1. Log in to the Web Configuration Utility. The **Configuration Utilities** page appears.
2. Click the **[Device Settings]** button. The **Settings** page appears.



3. In the Edit Files section, click **silo.conf**. The Silo.conf Editor modal page appears:

4. Edit the value assigned to ***dbuser*** and to ***ap_user***. Assign the value you defined in the section *Configuring a New Password in the Database Instance.*
5. To save your changes, click **Save** and then close the modal window.

Updating the master.system_settings_licenses Table

To update the master.system_settings_licenses table after you have changed the root password on a Data Collector or Message Collector:

1. Go to the **Appliance Manager** page (System > Settings > Appliances).
2. Locate the Data Collector or Message Collector in the list of appliances. Note the value in the ***ID*** column for the Data Collector or Message Collector.
3. Go to the **Database Tool** page (System > Tools > DB Tool).
4. Enter the following in the ***SQL Query*** field, replacing <new password> with the new password and <ID value of Collector> with the value you noted in step 2:

```
UPDATE master.system_settings_licenses SET db_user='root', db_pass=<new password>
WHERE id=<ID value of Collector>;
```

If you want to update all Data Collectors and Message Collectors with the same password, enter the following in the SQL Query field, replacing <new password> with the new password:

```
UPDATE master.system_settings_licenses SET db_user='root', db_pass='<new
```

```
password>' WHERE function in (5,6);
```

5. Click the **[Go]** button.

Changing IP Addresses

This section describes how to change the primary IP address of an appliance.

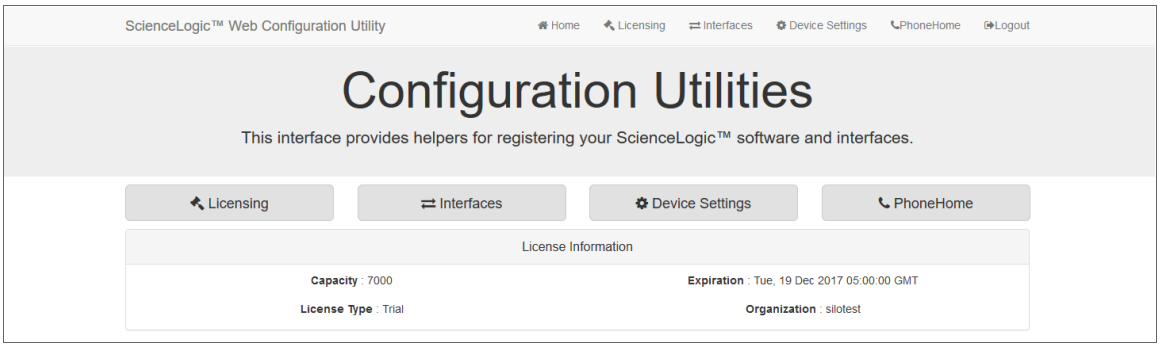
Preparing to Change the IP Address of a Database Server

Before you change the IP address on a Database Server, you must perform the following steps on every Data Collector and Message Collector appliance in your system:

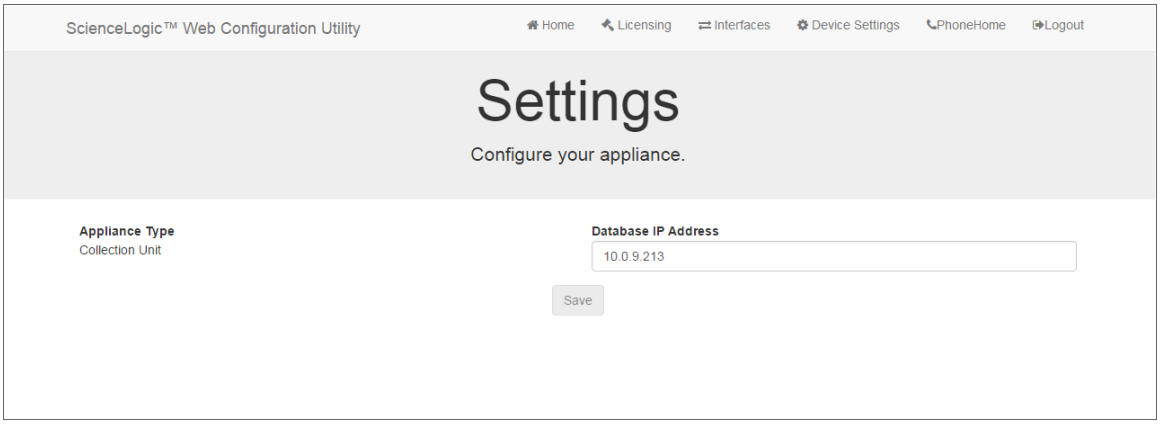
1. Log in to the Web Configuration Utility using any web browser supported by SL1. The address of the Web Configuration Utility is in the following format:

   https://*ip-address-of-appliance*:7700

2. You will be prompted to enter your username and password. Log in as ***em7admin*** with the appropriate password. The main page appears:



3. In the main page, select **[Device Settings]**. The **Settings** page appears.



4. Edit the following field:

    - ***Database IP Address***. Enter the new IP address for the Database Server.

5. Click **[Save]**.

Changing the IP Address of an Appliance

To change the primary IP address of an appliance, you must make changes in three places:

- In the user interface of the SL1
- In the ifconfig file
- In the silo.conf file

To change the primary IP address of a SL1 Appliance in the ScienceLogic user interface.

1. Go to the **Appliance Manager** page (System > Settings > Appliances).
2. Click the wrench icon () for the appliance.
3. Enter the new IP address in the ***IP Address*** field.
4. Click **[Save]**.

To change the IP address, Netmask, Gateway addresss, and DNS Server for an appliance in the ifconfig file:

1. Either go to the console of the SL1 appliance or use SSH to access the server.
2. Login as user ***em7admin*** with the appropriate password.
3. Enter the following at the command line:

```
sudo ifconfig
```

4. Your output will look ike this:

```
ens32: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.64.68.20 netmask 255.255.255.0 broadcast 10.64.68.255
inet6 fe80::250:56ff:fe84:455f prefixlen 64 scopeid 0x20<link>
ether 00:50:56:84:45:5f txqueuelen 1000 (Ethernet)
RX packets 1774927 bytes 161985469 (154.4 MiB)
RX errors 0 dropped 861 overruns 0 frame 0
TX packets 1586042 bytes 158898786 (151.5 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 0 (Local Loopback)
RX packets 13406577 bytes 4201274223 (3.9 GiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 13406577 bytes 4201274223 (3.9 GiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

5. Examine the output, find the first interface in the output, and note its name.

6. Use the vi editor to edit the settings for the interface. To do this, enter the following at the command line:

```
sudo vi /etc/sysconfig/network-scripts/ifcfg-interface name you noted in step #4
```

For example, from our output, we could enter:

```
sudo vi /etc/sysconfig/network-scripts/ifcfg-ens32
```

7. Your output will look like this:

```
TYPE=Ethernet
BOOTPROTO=none
DNS1=10.64.20.33
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
NAME=ens32
UUID=d471435d-9adf-47c9-b3f3-32f61dccbad8
DEVICE=ens32
ONBOOT=yes
IPADDR=10.64.68.20
PREFIX=24
GATEWAY=10.64.68.1
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
```

8. You can edit one or more of the following settings:

   - ***DNS1***=IP address of the DNS server that will be used by the SL1 appliance.
   - ***IPADDR***=IP address of the SL1 appliance.
   - ***PREFIX***=netmask for the SL1 appliance.
   - ***GATEWAY***=IP address of the network gateway that will be used by the SL1 appliance.

9. Save your changes and exit the file (:wq)
10. At the command line, enter the following:

```
sudo service network restart
```

To change the primary IP address of a SL1 Appliance in the silo.conf file:

1. Either go to the console of the SL1 appliance or use SSH to access the server.
2. Login as user ***em7admin*** with the appropriate password.
3. Enter the following at the command line:

```
sudo vi /etc/siteconfig/siloconf.siteconfig
```

4. Change the following line in the [LOCAL] section of the file to specify the new IP address:

```
ipaddress = XXX.XXX.XXX.XXX
```

5. Save and quit the file (:wq).
6. At the command line, enter the following command to rebuild the configuration file:

```
sudo /opt/em7/share/scripts/generate-silo-conf.py
```

7. Execute the following command to restart the network service:

```
systemctl restart sshd
```

Reconfiguring Administration Portals After Changing the IP Address of a Database Server

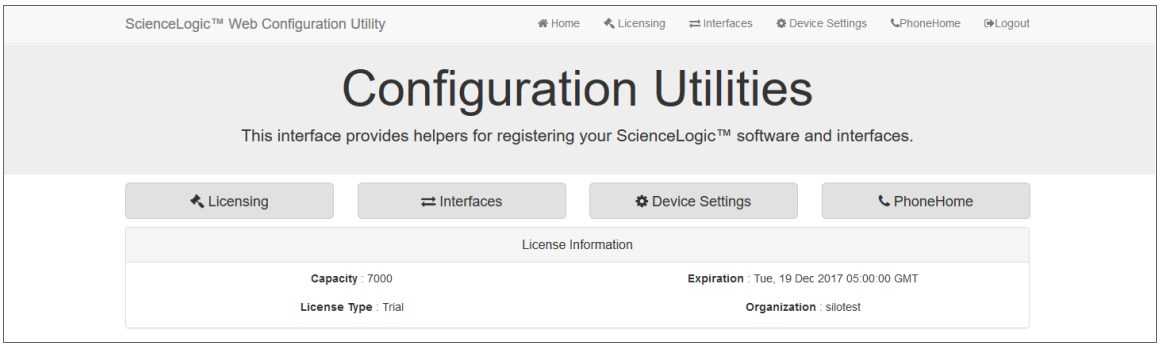
If you changed the IP address on the primary Database Server in your system, you must perform the following steps on every Administration Portal appliance in your system:

1. Log in to the Web Configuration Utility using any web browser supported by SL1. The address of the Web Configuration Utility is in the following format:

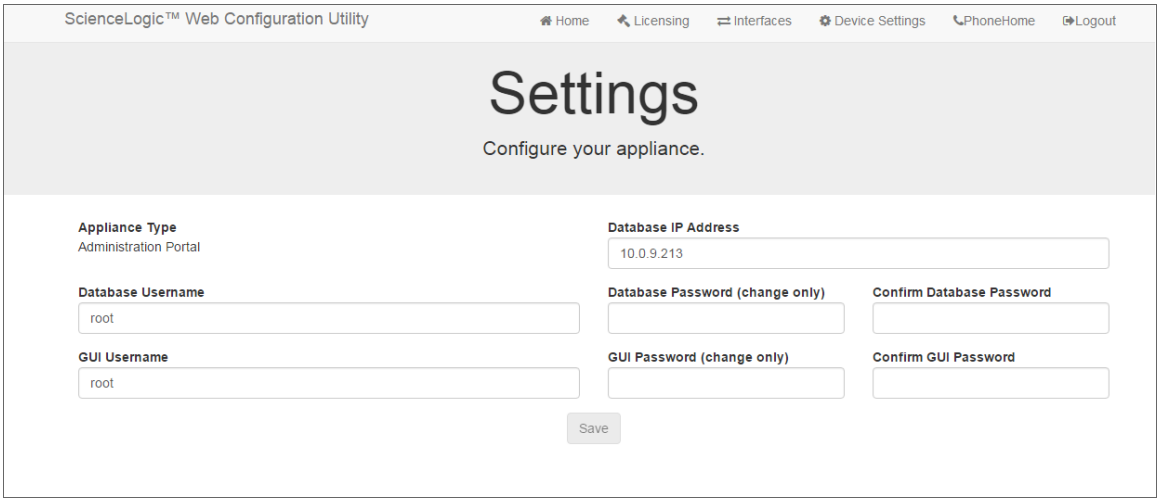
   https://ip-address-of-appliance:7700

   Enter the address of the Web Configuration Utility in to the address bar of your browser, replacing "ip-address-of-appliance" with the IP address of the SL1 appliance.

2. You will be prompted to enter your username and password. Log in as ***em7admin*** with the appropriate password. The main page appears:



3. In the main page, select **[Device Settings]**. The **Settings** page appears.



4. Edit the following field:

   - ***Database IP Address***. Enter the new IP address for the Database Server.

5. Click **[Save]**.

Chapter 8

Backup Management

Overview

SL1 allows you to define three types of backups for your system: Configuration Backup, Full Backup, and Disaster Recovery Backup. A configuration backup stores a copy of the core database tables, while a full backup and a disaster recovery backup backs up everything in your ScienceLogic database. This chapter will describe how to define and restore from each backup type.

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

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

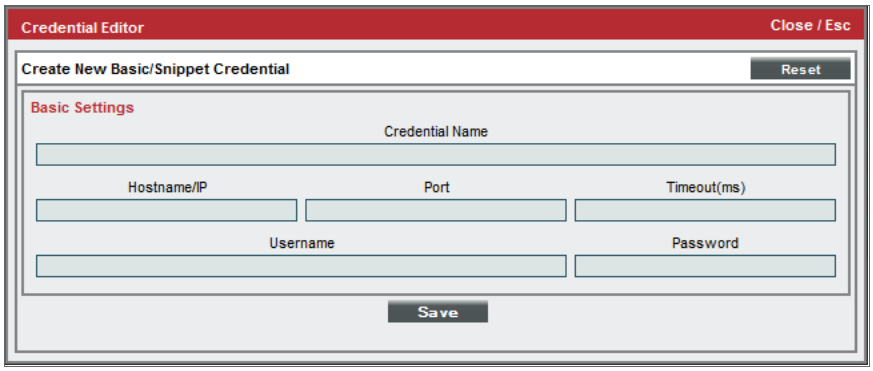
This chapter includes the following topics:

Creating a Backup Credential

To configure a backup, you must create a **Basic/Snippet** Credential that allows SL1 to write to the external systems where you will store the backups. To create a backup credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. In the **Credential Management** page, click the **[Actions]** button in the upper right of the page. Select **Create Basic/Snippet Credential**.

3. The **Credential Editor** page appears, where you can define values in the following fields:



   - ***Credential Name***. Name of the credential. Can be any combination of alphanumeric characters.
   - ***Hostname/IP***. The hostname or IP address.
   - ***Port***. This field is deprecated. Backups will not use this field.
   - ***Timeout (ms)***. This field is deprecated. Backups will not use this field.
   - ***Username***. Username to use when connecting to the external system. If you are backing up to NFS-remote, this field is not required.
   - ***Password***. Password to use when connecting to the external system. If you are backing up to NFS-remote, this field is not required.
4. Click the **[Save]** button.

Configuration Backups

A configuration backup stores a local copy of the core database tables that are required to restore a SL1 system, and optionally transfers the copy to an external system. A configuration backup entails:

- Configuration backup includes scope and policy information, but ***not performance data, data collected using configuration Dynamic Applications, events, or logs***. The following databases are backed up during a configuration backup:
   - ***master***. Includes system-level settings for SL1, Dynamic Application definitions and alignments, run book automation and action policies, monitoring policy definitions, and credentials.
   - ***master_access***. Includes user account information, access keys, and access hooks.
   - ***master_biz***. Includes asset information, dashboards, distribution lists, document templates, IT Service policy information, knowledge base information, organization information, product SKU information, RSS feeds, ticketing information, and user preferences.

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.

- ***master_custom***. Includes GUI customizations, dashboard widget definitions, PowerPack files, and custom attributes for the Integration Server.
- ***master_dns***. Includes DNS information.
- ***master_dev***. Includes information associated with device records, excluding performance data, data collected using configuration Dynamic Applications, events, or logs.
- ***master_events***. The configuration backup includes only the event_suppressions database table from this database. This table stores event suppression settings.
- ***master_filestore***. Includes information about files, PowerPacks, notes, installed packages, and installed patches.
- ***master_platform***. Includes information about ScienceLogic appliances, deployed package, and RPMs.
- ***master_reports***. Includes custom report definitions.
- ***scheduler***. Includes all instances of scheduled items: reports, discovery sessions, etc.

NOTE: You can configure the staging and remote directories used for backups in the master.system_settings_backup database, to ensure that the backup can be placed on a directory that has enough disk space. For remote directories, the current unix time will be appended to the directory name to ensure the directory name is unique each time the backup runs.

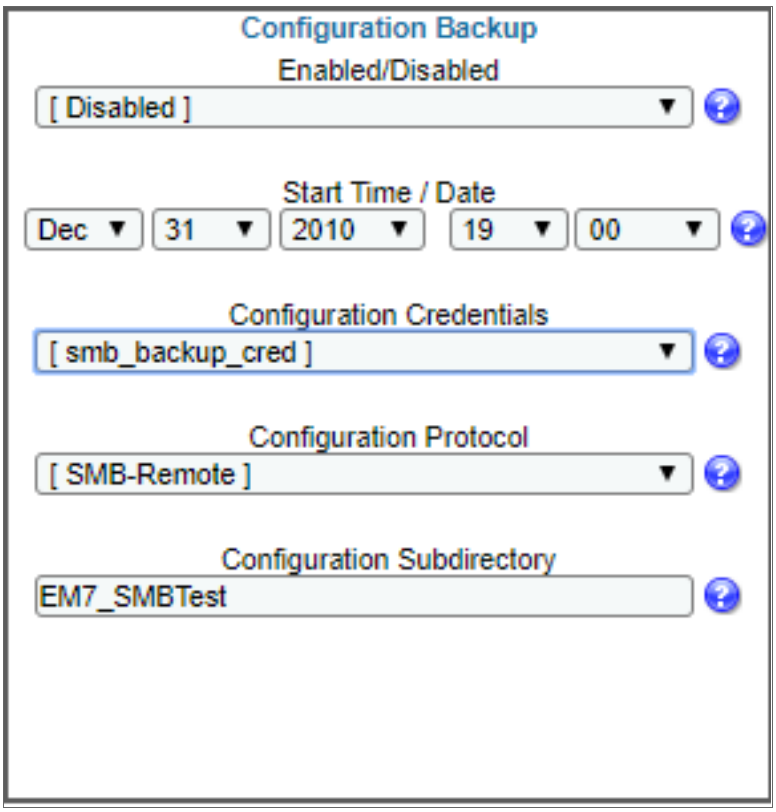
- SL1 automatically launches this backup every day, at the time you specify.
- SL1 saves local copies of the last seven days of backups and stores the first backup of the month for the current month and the three previous months.
- A configuration backup also contains all the files and folders specified in /etc/backup.conf.
- During configuration backup, the ScienceLogic database remains online.

Defining a Configuration Backup

A configuration backup stores a local copy of the core database tables that are required to restore a SL1 system. A Configuration backup includes scope and policy information, but ***not performance data or logs***. Configutration backups backup the files and folders specified in /etc/backup.conf.

To define and schedule a configuration backup:

1. Go to the **Backup Management** page (System > Settings > Backup).
2. In the **Configuration Backup** pane, provide values in the following fields:



- ***Enabled/Disabled***. Enables or disables configuration backups. When enabled, SL1 automatically executes configuration backups every day, at the time specified in the ***Start Time / Date*** field.
- ***Start Time / Date***. If you enabled configuration backups, you must specify the daily start time. This is the time at which SL1 will automatically execute configuration backups every day. You must also specify the date on which the daily backups will begin. Use the drop-down lists to select the date and time.
- ***Configuration Credentials***. Optional. If you want to store the configuration backup on a remote NFS mount or a remote SMB mount, you must select a credential in this field. The credential must be of type ***Basic/Snippet*** and specify the hostname or IP, user name, and password.
- ***Configuration Protocol***. Optional. If you specified a configuration credential in the ***Configuration Credentials*** field, you must select the type of external system where the backup will be stored.
    - *NFS-Remote*. When you select this option, SL1 stores the full backup on an NFS mount. You specify the NFS mount with the ***Configuration Credentials*** field and the ***Configuration Subdirectory*** field. ***The system creates the backup file directly on the external NFS mount***, instead of creating the backup file on the appliance, transferring the backup file to the NFS mount, and then removing the backup file from the appliance.

NOTE: If you select the *NFS-remote* option, and your NFS mount is hosted on a Solaris system, you must perform the steps listed in the *Additional Configuration for Solaris NFS Mounts* section.

- *SMB-Remote*. When you select this option, SL1 stores the full backup on an SMB mount. You specify the SMB mount with the ***Configuration Credentials*** field and the ***Configuration Subdirectory*** field. ***The system creates the backup file directly on the external SMB mount***,.

- ***Configuration Subdirectory***. Optional. If you specified NFS mount or SMB mount by selecting a credential, in the ***Configuration Credentials*** field, you can specify a directory on the NFS mount or SMB mount in which you would like to store the configuration backup. When entering the subdirectory path, omit the leading slash ("/").

NOTE: SL1 always maintains local copies of configuration backups from the last seven days and the first day of the month for the current month and the previous three months. Even if you choose to store configuration backups on a remote NFS mount or a remote SMB mount, SL1 still maintains local copies of configuration backups.

3. Click the **[Save]** button to save your settings. SL1 will execute the configuration backup every day, starting on the date you specified in the ***Start Time / Date*** field, at the time you specified in the ***Start Time / Date*** field.
4. To run the backup immediately, click the **[Backup Now]** button under ***Configuration Backup***. SL1 will immediately run the backup, and will still run the backup every day at the time you specified in the ***Start Time*** field.

Restoring a Configuration Backup

If your database has been backed up using a configuration backup, in the event of data corruption or other failure, you will need to restore your system using the configuration backup. The backup file contains one .sql file for each database that was included in the backup. To restore a database using the backup file:

1. Either go to the console of the Database Server or use SSH to access the server.
2. Login as user ***em7admin*** and sudo to the root account.

```
sudo -s
```

3. Perform the following commands to uncompress the backup file:

```
mkdir /data.local/db/restore_tmp
cd /data.local/db/restore_tmp
pigz -dc <full path and file name for backup.tgz> | tar xvf
```

4. Navigate to the directory that contains the .sql files from the backup:

```
cd /data/backup/remote<unix timestamp>
```

where:

- *unix timestamp* is appended to each remote directory to ensure that naming is unique.

5. The directory will contain one .sql file for each database included in the backup. To restore a database, execute the following command using the username of a user that has administrative privileges in MySQL (by default, the user is ***root*** and the password is ***em7admin***):

```
silo_mysql <name_of_database> -u <username> -p<password> < <name_of_
database>.sql
```

NOTE: Do not include a space between "-p" and the password.

For example, to restore the database "master" as the user "root" with the default password of "em7admin", perform the following command:

```
silo_mysql master -u root -pem7admin < master.sql
```

6. Re-license the Database Server using the standard licensing procedure.
7. To restore all the databases that are included in the backup file, repeat step 6 for each .sql file.

Full Backup

A full backup makes a full backup of the ScienceLogic database. This type of backup is recommended for SL1 systems in small-to-medium enterprises. A full backup entails:

- Full backup includes all configuration data, performance data, and log data.
- Full backup is disabled by default. You can configure SL1 to automatically launch this backup at a frequency and time you specify.
- During full backup, the ScienceLogic database remains online.
- The backup is stored on a remote NFS mount or a remote SMB mount.

NOTE: ***ScienceLogic does not recommend Full Backups for large SL1 systems***. For large SL1 systems, ScienceLogic recommends you use the ***DR Backup*** option or a SAN with snapshot technology to backup and restore data.

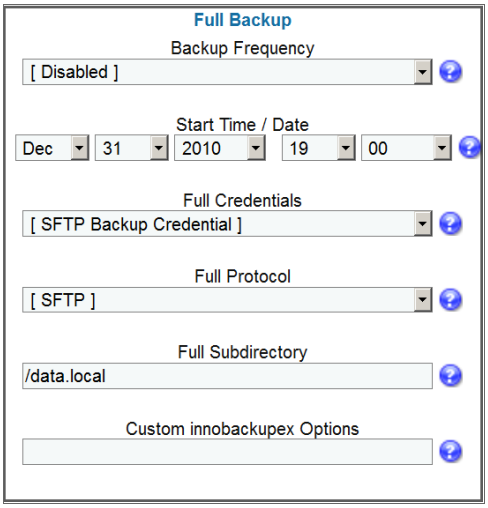
NOTE: You can configure the staging and remote directories used for backups in the master.system_settings_backup database, to ensure that the backup can be placed on a directory that has enough disk space. For remote directories, the current unix time will be appended to the directory name to ensure the directory name is unique each time the backup runs.

Defining a Full Backup

Full backup includes all configuration data, performance data, and log data. SL1 automatically launches this backup and frequency and time you specify.

To define and schedule a full backup:

1. Go to the **Backup Management** page (System > Settings > Backup).
2. In the **Full Backup** pane, provide values in the following fields:



- ***Backup Frequency***. You must specify how frequently SL1 should automatically execute a full backup. Your choices are:
  - *Disabled*. Full backups are disabled.
  - *Daily*. SL1 will execute full backups every day.
  - *Weekly*. SL1 will execute full backups once a week.
  - *Monthly*. SL1 will execute full backups once a month.
- ***Start Time / Date***. Specify the time of day at which SL1 should automatically execute full backups. You must also specify the date on which the backups will begin. If you selected *Weekly* or *Monthly* in the ***Backup Frequency*** field, the date you select will determine which day of the week or month the backups will be scheduled. Use the drop-down lists to select the date and time.
- ***Full Backup Credentials***. You must store full backups on an external system (not the Database Server or All-In-One Appliance). You can specify that full backups be stored on a remote NFS mount or a remote SMB mount. To specify where to store full backups, you must select a credential in this field. The credential must be of type ***Basic/Snippet*** and specify the hostname or IP, username, and password.
- ***Full Protocol***. Specify the type of external system where the full backup will be stored. Choices are:

- *NFS-Remote*. When you select this option, SL1 stores the full backup on an NFS mount. You specify the NFS mount with the ***Configuration Credentials*** field and the ***Configuration Subdirectory*** field. ***The system creates the backup file directly on the external NFS mount***, instead of creating the backup file on the appliance, transferring the backup file to the NFS mount, and then removing the backup file from the appliance.

NOTE: If you select the *NFS-remote* option, and your NFS mount is hosted on a Solaris system, you must perform the steps listed in the *Additional Configuration for Solaris NFS Mounts* section.

- *SMB-Remote*. When you select this option, SL1 stores the full backup on an SMB mount. You specify the SMB mount with the ***Configuration Credentials*** field and the ***Configuration Subdirectory*** field. ***The system creates the backup file directly on the external SMB mount***.

- ***Full Subdirectory***. Specify a directory on the remote NFS mount or the remote SMB mount in which you would like to store the full backup. When entering the subdirectory path, omit the leading slash ("/").
- ***Custom innobackupex Options***. Specify one or more custom backup options. For details on these options, see http://www.percona.com/doc/percona-xtrabackup/2.1/innobackupex/innobackupex_option_reference.htm.

3. Select the **[Save]** button to save your settings. SL1 will execute the full backup at the frequency and time you specified in the ***Backup Frequency*** and ***Start Time*** fields.
4. To run the backup immediately, click the **[Backup Now]** button under ***Full Backup***. SL1 will immediately run the backup and will still run the backup at the frequency and time you specified in the ***Backup Frequency*** and ***Start Time*** fields.

Restoring a Full Backup

To restore a SL1 system using a full backup file, perform the following steps:

NOTE: These steps assume that the Database Server has not been previously configured.

NOTE: To complete these steps, you must be familiar with how to edit a file using the vi text editor. If you need assistance with these steps, please contact ScienceLogic Support.

1. The Database Server you are restoring the backup to must be at the same revision number as the Database Server that created the backup file.
2. Either go to the console of the Database Server where you want to restore the backup or use SSH to log in to that the Database Server.
3. Log in as user ***em7admin*** and then sudo to the root account:

```
sudo -s
```

4. Execute the following commands:

> **WARNING:** Executing this command will stop the database. SL1 will not be operational until you complete the restore procedure.

```
systemctl stop em7
systemctl stop mariadb
rm -rf /data/db/*
```

5. Execute the following two commands, substituting in the full path name of your backup file:

```
cd /data/db

pigz -dc <full_path_and_name_of_backup_file.gz> | xbstream -x -C .
```

6. Execute the following commands:

> **NOTE:** Depending on the size of the backup, the innobackupex command might take a long time to complete.

```
cd /data/db
innobackupex --apply-log /data/db 2>&1 | tee /data/tmp/restore.log
chown -R mysql:mysql /data/db/*
systemctl start mariadb
systemctl start em7
```

7. Re-license the Database Server using the standard licensing procedure.

Additional Configuration for Solaris NFS Mounts

To use the *NFS-remote* backup protocol with an NFS mount hosted on a Solaris system, you must configure the Solaris system to allow the backup process to change file ownership permissions. To do this:

- In /etc/dfs/dfstab on the Solaris system, you must specify that the fully-qualified domain name of the Database Server or All-In-One Appliance can access the NFS file system as root. For example:

```
share -F nfs -o sec=sys,root=database.sciencelogic.local -d "ScienceLogic Backup
Share" /export/home/backup
```

- In /etc/defaults/nfs on the Solaris system, include the line "NFSMAPID_DOMAIN=<domain of Database Server or All-In-One Appliance>. For example:

```
NFSMAPID_DOMAIN=ScienceLogic.local
```

You can test this configuration by mounting the NFS file system from the console of your SL1 appliance, creating a new file on the file system using the "touch" command, and then executing the command "ls -la". If the Solaris system is configured correctly, the output of the ls command will indicate that the new file was created and owned by the "root" user.

Defining a DR Backup

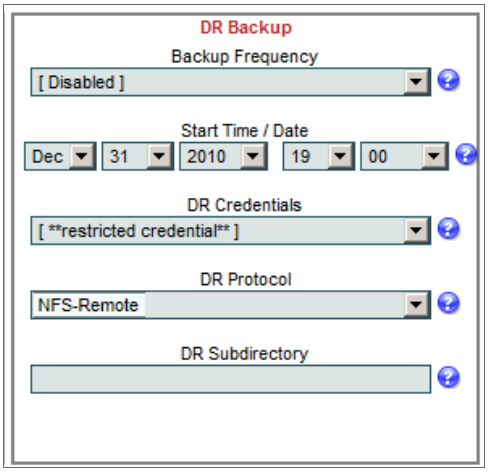
For SL1 systems configured for disaster recovery, DR Backup temporarily stops replication, performs a full backup of the disaster-recovery database, and then re-enables replication and performs a partial resync from the primary.

DR backup includes all configuration data, performance data, and log data. During DR backup, the primary ScienceLogic database remains online.

NOTE: The ***DR Backup*** fields appear only for systems configured for Disaster Recovery. DR Backup is not available for the two-node DRBD-HA cluster.

To define and schedule a DR backup:

1. Go to the **Backup Management** page (System > Settings > Backup).



2. In the **DR Backup** pane, provide values in the following fields:

   - ***Backup Frequency***. You must specify how frequently SL1 should automatically execute a full backup. Your choices are:
     - *Disabled*. DR backups are disabled.
     - *Daily*. SL1 will execute DR backups every day.
     - *Weekly*. SL1 will execute DR backups once a week.
     - *Monthly*. SL1 will execute DR backups once a month.

- ***Start Time/Date***. Specify the time of day at which SL1 should automatically execute DR backups. You must also specify the date on which the backups will begin. If you selected *Weekly* or *Monthly* in the ***Backup Frequency*** field, the date you select will determine which day of the week or month the backups will be scheduled. Use the drop-down lists to select the date and time.
- ***DR Credentials***. You must store DR backups on an external system (not the Database Server or All-In-One Appliance). You can specify that DR backups be stored on an NFS mount or SMB mount. To specify where to store full backups, you must select a credential in this field. The credential must be of type ***Basic/Snippet*** and specify the hostname or IP, username, and password to access the external system. For more information on credentials, see the **Credential Management** page.

NOTE: Your organization membership(s) might affect the list of credentials you can see in the ***Full Backup Credentials*** field. For details, see the ***Discovery and Credentials*** manual.

- ***DR Protocol***. Specifies where SL1 should store the full backups. Choices are:
    - *NFS-Remote*. When you select this option, SL1 stores the full backup on an NFS mount. You specify the NFS mount with the ***Full Backup Credentials*** field and the ***Full Subdirectory*** field. ***The system creates the backup file directly on the external NFS mount***.

NOTE: If you select the *NFS-remote* option, and your NFS mount is hosted on a Solaris system, you must perform the steps listed in the *Additional Configuration for Solaris NFS Mounts* section of this chapter.

    - *SMB-Remote*. When you select this option, SL1 stores the full backup on an SMB mount. You specify the SMB mount with the ***Full Backup Credentials*** field and the ***Full Subdirectory*** field. ***The system creates the backup file directly on the external SMB mount***.

NOTE: ScienceLogic strongly recommends that you use the ***DR Protocol*** option *NFS-Remote* or *SMB-Remote* when performing a DR backup; the other ***DR Protocol*** options cause the resync step to take much longer.

- ***DR Subdirectory***. Specify a directory on theNFS mount or SMB mount in which you would like to store the DR backup.

3. Click the **[Save]** button to save your settings. SL1 will execute the DR backup at the frequency and time you specified in the ***Backup Frequency*** and ***Start Time*** fields.
4. To run the backup immediately, click the **[Backup Now]** button under ***DR Backup***. SL1 will immediately run the backup and will still run the backup at the frequency and time you specified in the ***Backup Frequency*** and ***Start Time*** fields.

Restoring a DR Backup

To restore a Database Server using a DR backup file, perform the following steps:

NOTE: These steps assume that the Database Server has not been previously configured.

1. The Database Server you are restoring the backup to must be at the same revision number as the Database Server that created the backup file.
2. Either go to the console of the Database Server where you want to restore the backup or use SSH to access the Database Server.
3. Log in as user ***em7admin*** and duso to the root account:

```
sudo -s
```

4. Execute the following commands:

WARNING: Executing this command will stop the database. SL1 will not be operational until you complete the restore procedure.

```
systemctl stop em7
systemctl stop mariadb
rm -rf /data/db/*
```

5. Execute the following commands, substituting the full pathname of your backup file:

```
cd /data/db
pigz -dc <full path and name to backup file.tgz> | tar xvf -
mv /data/db/data/db/* .
rm -rf /data/db/data
cp /data/db/etc/my.cnf.d/silo_mysql.cnf /root/silo_mysql.bak
rm -rf /data/db/etc
chown -R mysql:mysql /data/db/*
```

6. Execute the following commands to restart SL1 and the database:

```
systemctl start em7
systemctl start mariadb
```

Chapter 9

Subscription Licenses

Overview

If you have a subscription license, you can use the **[Subscription]** button in the **System Usage** page (System > Monitor > System Usage) to:

- View a report on license usage.
- Download system usage data for manual upload to the ScienceLogic billing server.
- Upload a receipt from the ScienceLogic billing server.

If your SL1 system is configured to communicate with the ScienceLogic billing server, usage data will be sent automatically from your SL1 system to the ScienceLogic billing server once a day. After the ScienceLogic billing server receives the usage data, SL1 will automatically mark the license usage file as delivered.

If your SL1 system is not configured to communicate with the ScienceLogic billing server or if the connection to the ScienceLogic billing server fails, you can manually upload usage data to the ScienceLogic billing server.

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

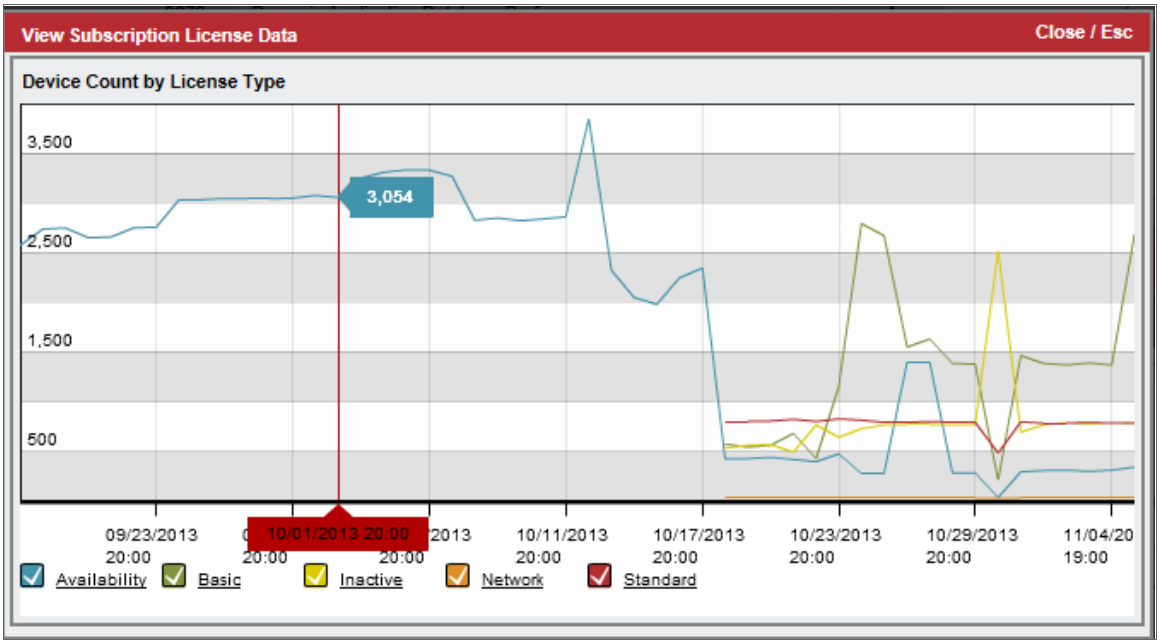
- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon ( ).

This chapter includes the following topics:

Viewing a Report on License Usage

If you have a subscription license, you can view a report on license usage for your SL1 system. To view a report on license usage for your SL1 system:

1. Go to the **System Usage** page (System > Monitor > System Usage).
2. Click the **[Subscription]** button.
3. Select *View Subscription License Data*.
4. The **View Subscription License Data** modal page appears and displays a report on license usage.



5. The **View Subscription License Data** modal page displays a graph. The graph displays:
   - Number of monitored devices on the y-axis.
   - Date and time on the x-axis.
   - Each colored line on the graph represents a device category.

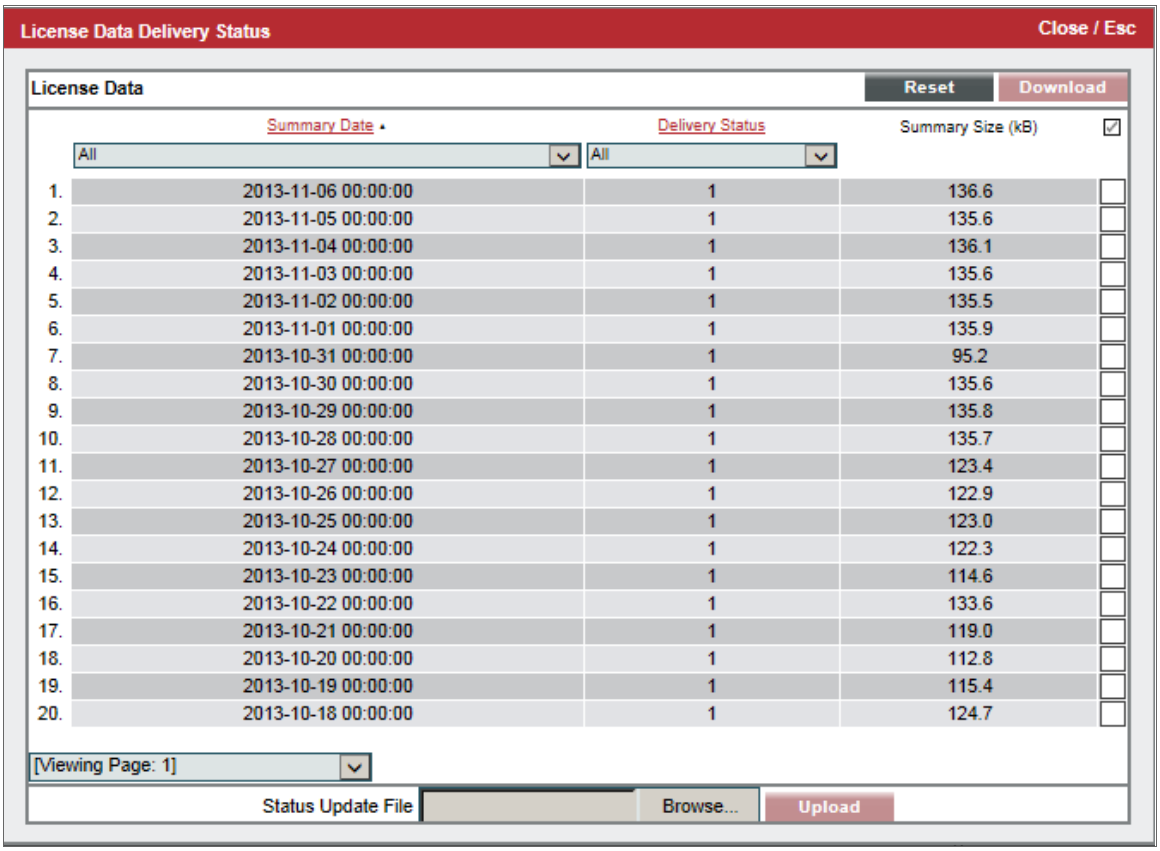
Device categories depend upon your specific license agreement with ScienceLogic. The types of device categories that can appear in the **View Subscription License Data** modal page will reflect your license agreement with ScienceLogic.

Viewing Delivery Status

The **License Data Delivery Status** page displays the status of one or more daily license-usage files. To view the **License Data Delivery Status** page:

1. Go to the **System Usage** page (System > Monitor > System Usage).
2. Click the **[Subscription]** button.
3. Select *License Data Delivery Status*.
4. The **License Data Delivery Status** modal page appears and displays a list of daily license-usage files. For each daily license-usage file, the **License Data Delivery Status** page displays the following:

   - ***Summary Date***. Date associated with the daily license-usage file.
   - ***Delivery Status***. Possible values are:
     - "*0*" *(zero)*. File has not been uploaded to the ScienceLogic billing server.
     - "*1*" *(one)*. File has been uploaded to the ScienceLogic billing server and may be deleted from the SL1 system by the automated maintenance process.
   - ***Summary Size***. Size of the daily license-usage file.



Manually Uploading License Usage to ScienceLogic

If your SL1 system is configured to communicate with ScienceLogic, usage data will automatically be sent to the ScienceLogic billing server once a day. After the ScienceLogic billing server receives the usage data, SL1 will automatically mark the license usage file as delivered.

If your SL1 system is not configured to communicate with ScienceLogic or if the connection to the ScienceLogic billing server fails:

- You can use the **License Data Delivery Status** page to manually download the daily license-usage file.
- You can then log in to the ScienceLogic billing server and manually upload the daily license-usage file.
- You can then use the **License Data Delivery Status** page to upload the ScienceLogic "receipt" to your SL1 system, allowing SL1 to mark the license usage file as delivered.
- License usage files will not be deleted from your system until they are delivered.

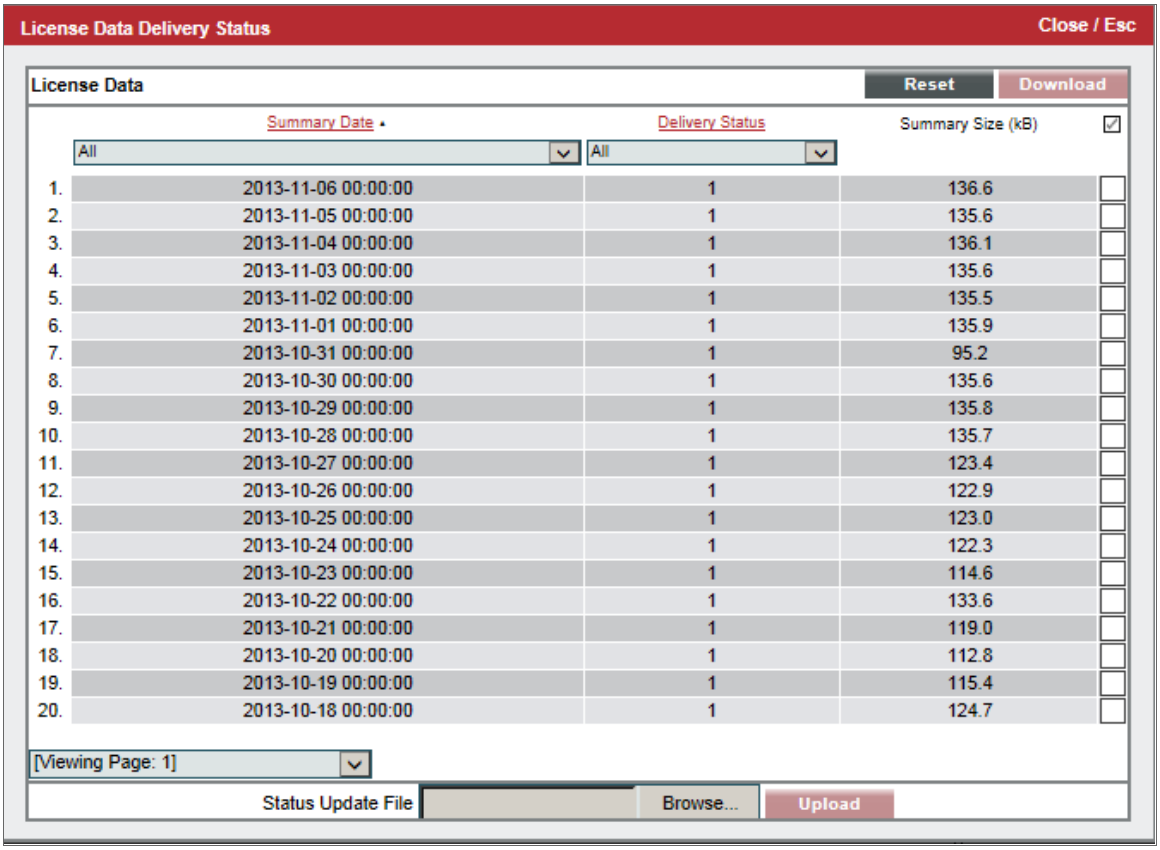
Downloading the Daily License-Usage File

If your SL1 system is not configured to communicate with ScienceLogic or if the connection to the ScienceLogic billing server fails, you can use the **License Data Delivery Status** page to manually download the daily license-usage file. You can then log in to the ScienceLogic Licensing and Billing server and manually upload the daily license-usage file.

To download the daily license-usage file using the **License Data Delivery Status** page:

1. Go to the **System Usage** page (System > Monitor > System Usage).
2. Click the **[Subscription]** button and select *License Data Delivery Status*.

3. Select one or more daily license-usage files to download to your local computer, then click the **[Download]** button.



NOTE: If the download size exceeds 50MB, the **[Download]** button becomes disabled.

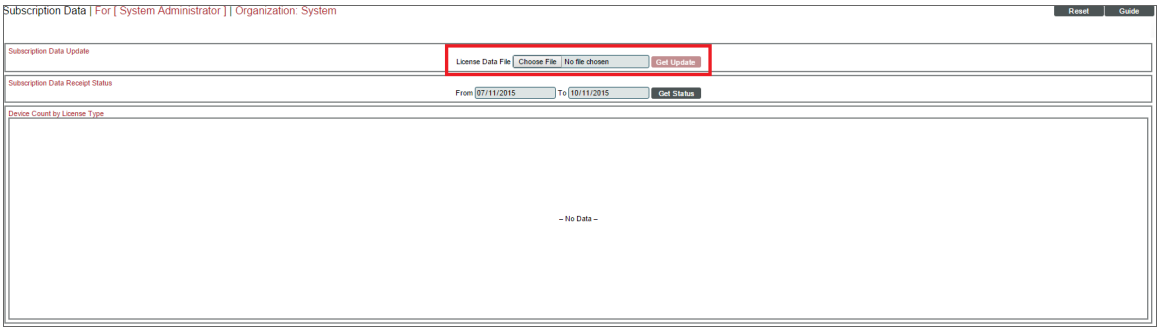
4. The daily license-usage file will be saved to your local computer. The downloaded file is usually named "license_data.json.gz".

Manually Uploading the Daily License-Usage File to ScienceLogic

After downloading the daily license-usage file to your local computer, you can manually upload the file to the ScienceLogic billing server. To do this:

1. Log in to the ScienceLogic billing system.
2. Go to the **Subscription Data** page (Preferences > Account > Subscription).
3. In the **Subscription Data** page, go to the **Subscription Data Update** pane. Use the **[Browse]** button to find the daily license-usage file that you downloaded to your local computer.

4. Click the **[Get Update]** button to upload the daily license-usage file to the ScienceLogic server.



5. The ScienceLogic server will provide a "receipt" file for you to download. This file is usually called "status_updated.json.gz". You must upload this receipt to your SL1 system.

Uploading the ScienceLogic Receipt

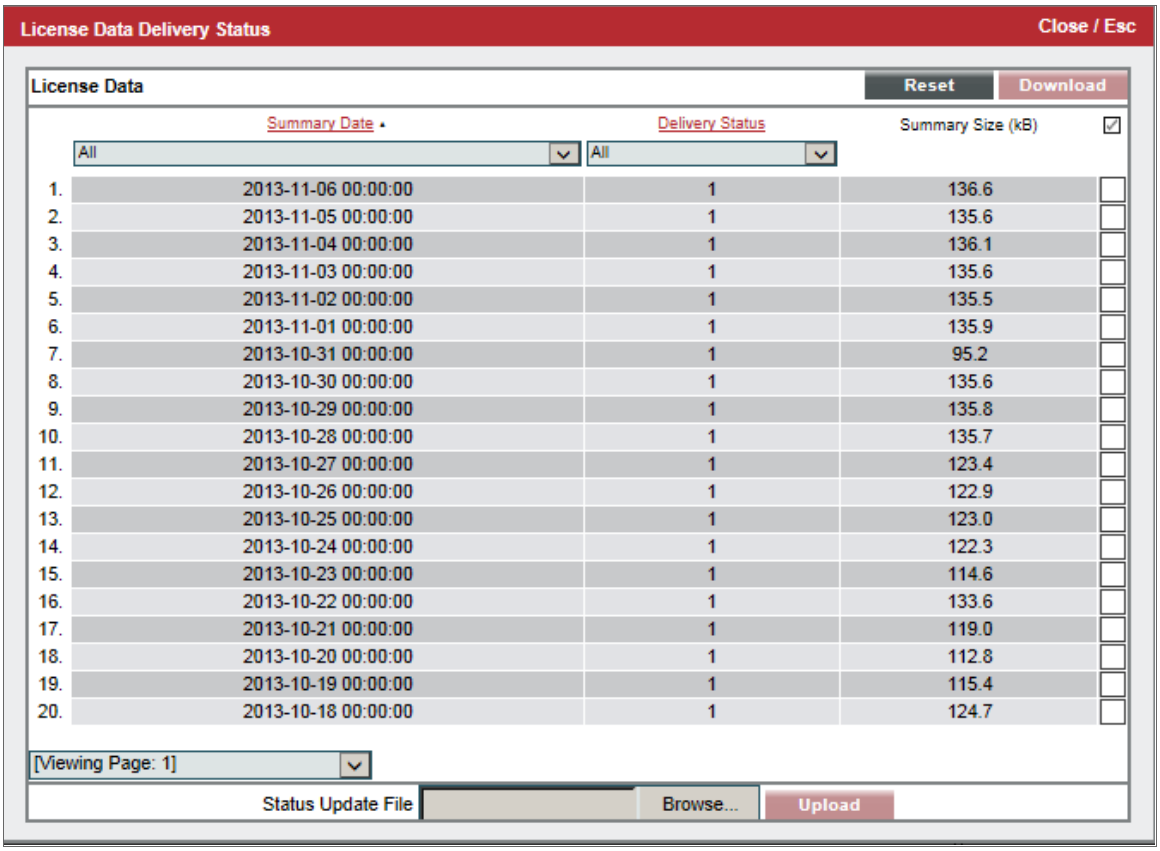
After uploading the daily license-usage file to the ScienceLogic Billing server, the ScienceLogic server will provide a "receipt" file for you to download. This file is usually called "status_updated.json.gz".

You must upload this "receipt" file to your SL1 system to inform your SL1 system that the upload was successful and that the SL1 system may delete the daily license-usage file.

To upload the "receipt" file:

1. Go to the **System Usage** page (System > Monitor > System Usage).
2. Click the **[Subscription]** button and select *License Data Delivery Status*.
3. In the ***Status Update File*** field, use the **[Browse]** button to locate the "receipt" file.

4. Click the **[Upload]** button to upload the "receipt" file to your SL1 system:



Data Retention Settings for Licensing

The **Data Retention Settings** page contains settings for subscribers.

To adjust these settings:

1. Go to the **Data Retention Settings** page (System > Settings > Data Retention).
2. The following sliders appear under the **Subscription Data Retention** heading:

   - ***Subscriber Device Configuration Data***. For users with a subscriber license. Number of months to retain the files and database tables that contain configuration information for a device. Default value is twelve months.
   - ***Subscriber Device Usage Data***. For users with a subscriber license. Number of months to retain information on total number of events and total number of tickets. Default value is six months.
   - ***Subscriber System Configuration Data***. For users with a subscriber license. Number of months to retain the files and database tables that contain configuration information for the SL1 system. Default value is twelve months.

- ***Subscriber System Usage Data***. For users with a subscriber license. Number of months to retain information on total number of events and total number of tickets. Default value is six months.
- ***Subscriber Device Type Data***. For users with a subscriber license. Number of months to retain the files and database tables that map each device to a device category, as per your subscriber license. Default value is six months.
- ***Subscriber Daily Delivery Data***. For users with a subscriber license. Number of months to retain the "crunched" license usage data that is calculated each day using the Subscriber Device Configuration Data, Subscriber System Configuration Data, Subscriber System Usage Data, and Subscriber Device Type Data. SL1 will not prune data that has not yet been delivered to the ScienceLogic Licensing and Billing server.

Chapter 10

CAC Authentication

Overview

SL1 supports CAC authentication. The **Client Certificate & CAC Authentication** page allows you to define a check for SSL certificate that controls whether the login page is displayed to the end user. This feature is primarily used to authenticate Common Access Card (CAC) users against a Department of Defense (DoD) issued server-side certificate; however, based on your business needs, this feature can also be used with your own client/server certificates.

The CAC is a United States DoD smartcard issued as standard identification for active duty military personnel, reserve personnel, civilian employees, and eligible contractor personnel.

Each CAC contains a client-side security certificate from the DoD certificate authority (DoD Root CA). This client-side certificate allows the CAC to authenticate with web servers that include the server-side security certificate from the DoD certificate authority. Web servers with the server-side security certificate are deemed secure for DoD use.

SL1 allows you to configure appliances that provide the user interface (Administration Portal, All-In-One Appliance, or the Database Server) for use with DoD certificates or your own certificates. You can install server-side certificates on the user interface appliances and then authenticate access to those web servers with a CAC or a client-side certificate associated with a user's web browser.

When authentication of the client-side certificate against the server-side certificate is successful, SL1 displays the ScienceLogic login page to the end user. The client-side certificate does not authenticate the username and password. The client-side certificate authenticates only that the user is permitted access to the user interface, and in the case of a DoD issued server-side certificate, that the user interface appliance (Administration Portal, All-In-One Appliance, or the Database Server) is deemed secure for DoD use. If CAC authentication is enabled, SL1 verifies the client-side certificate every time a page is accessed in the user interface; if a client-side certificate is unavailable or invalid, the user is immediately logged out of the user interface.

NOTE: Currently, SL1 does not support client-side certificate authentication for login to the console, either through SSH or through a keyboard connected to the appliance.

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

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

This chapter includes the following topics:

Prerequisites

To use client certificate authentication with SL1, you must first perform the following tasks:

1. Users must have either:
   - Valid CACs with valid client-side certificates already loaded onto the cards.
   - Valid client-side certificates installed in their web browser.
2. If CACs are used, the browser through which the user logs on to the user interface must be able to read security certificates from the cards. For Mozilla Firefox, users can install http://www.forge.mil/Resources-Firefox.html . For Internet Explorer, users must purchase and install commercial software for reading security certificates.
3. In the **Behavior Settings** page (System > Settings > Behavior), you must enable the following field
   - ***Force Secure HTTPS***. Only when the Administration Portal, All-In-One Appliance, or the Database Server uses HTTPS will the appliance request a security certificate from the CAC or client web browser.
4. In the **SSL Certificates** page (System > Settings > Authentication > Admin SSL Certificates), you must install the server-side certificate on the Administration Portal, All-In-One Appliance, or the Database Server. For CAC authentication, the server-side certificate is issued by the DoD. To learn more about importing a certificate, see the section *Importing an SSL Certificate*.
5. You can customize the user name that is displayed in SL1 after CAC authentication. You can edit the ScienceLogic configuration file to customize the displayed user name.

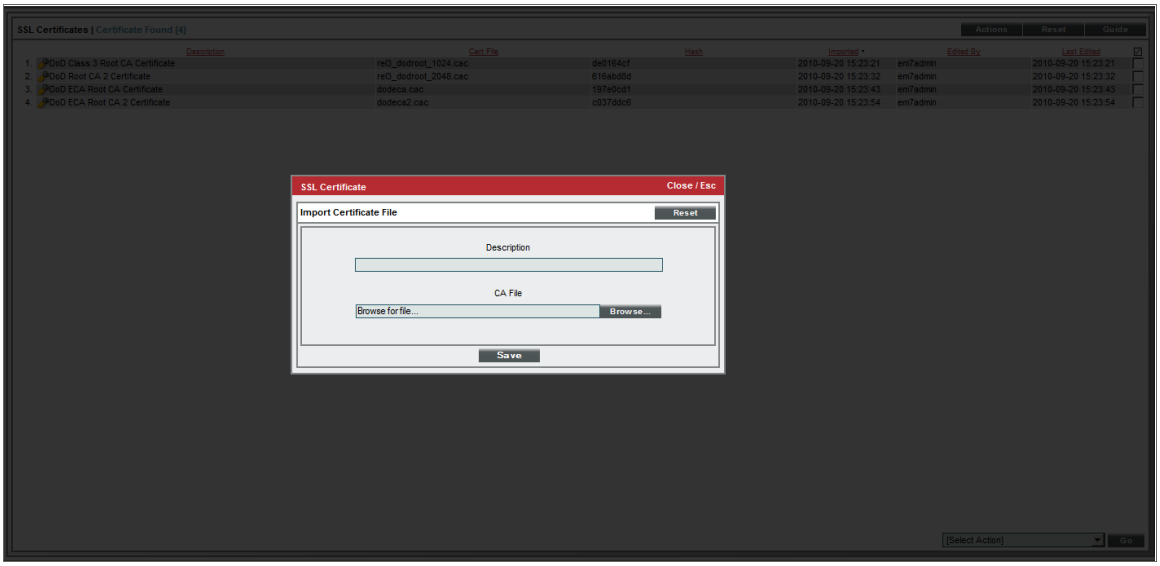
6. In the **Client Certificate & CAC Authentication** page (System > Settings > Authentication > CAC Client Cert Auth), you must configure the server-side certificate and test it against your client-side certificate.

Importing an SSL Certificate

Secure Sockets Layer, or SSL, is a protocol for securely transmitting data via the Internet. SSL uses a private key to encrypt data to be transferred over an Internet connection. In SL1, you can import server-side SSL certificate files, including DoD certificate files used in CAC authentication, to the Administration Portal, All-In-One Appliance, or the Database Server.

To import an SSL certificate for CAC authentication:

1. Go to the **SSL Certificates** page (System > Settings > Authentication > SSL Certificates).
2. In the **SSL Certificates** page, click the **[Actions]** menu. Select ***Import DoD Root CA Certificate***. The **Import Certificate** modal page appears.



3. In the **Import Certificate** modal page, enter the following:
   - ***Description***. Description of the certificate.
   - ***CA File***. Browse for the server-side certificate file on your local computer.
4. Click the **[Save]** button to load the certificate to the Administration Portal, All-In-One Appliance, or the Database Server.

Updating the ScienceLogic Configuration File

By default, the certificate configuration file (em7_certificate.conf) is configured to display a CAC user's common name (CN) as a user name in SL1 after CAC authentication. If this is your preference, then you do not need to update the configuration file and can skip this section.

However, if you prefer that SL1 display only the user name portion of the CAC user's CN, then you can edit the certificate configuration file to parse out the user name from the certificate CN.

To do so:

1. Log in to the console of the ScienceLogic appliance as the root user.
2. Navigate to the directory /etc/ngnix/conf.d/ :

```
cd /etc/ngnix/conf.d/
```

3. Open the file em7_certificate.conf with a text editor like vi:

```
vi em7_certificate.conf
```

4. Edit the file to look like this:

```
map $ssl_client_s_dn $ssl_client_username {
~/CN=[A-Z\.]+(?<num>[0-9]+) $num;
}
```

5. Save and quit (:wq) the file.

Defining the Client Certificate

When you define a CAC or client-side certificate on a web browser, you are actually selecting a server-side certificate on the SL1 appliance and testing the client-side certificate (on your browser or your CAC) against the certificate on the appliance.

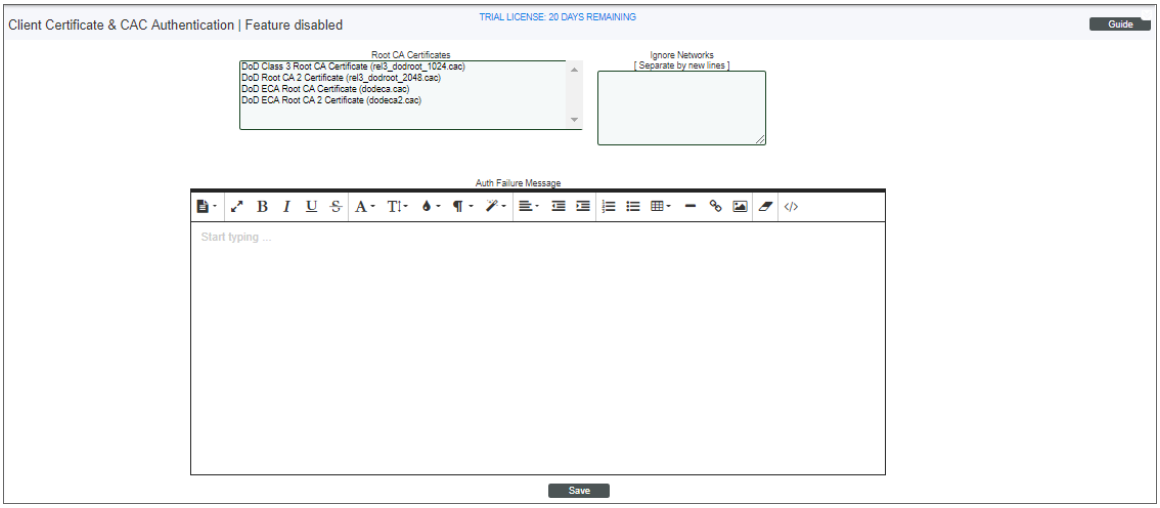
You can also define some custom settings for client-side certificate authentication. You can define error messages that are displayed to the end user when authentication fails. You can also define IP addresses for which the user interface will not perform authentication.

When authentication is successful, the user interface displays the **ScienceLogic Login** page to the user.

To define the authentication settings:

1. Access the user interface with your CAC or a browser with your client-side certificate installed.

2. Go to the **Client Certificate & CAC Authentication** page (System > Settings > Authentication > CAC Client Cert Auth).



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

   - ***Root CA Certificates***. Select from a list of certificates installed on the **SSL Certificates** page (System > Settings > Authentication > Admin SSL Certificates). Your client-side certificate will be authenticated against the selected server-side certificate.
   - ***Certificate User Field***. Specifies which field in the certificate the platform will use to find the username. The choices are:
     - *Common Name*
     - *MS UPN*
   - ***Auth Failure Message***. Enter text for the error message that appears to users if authentication fails.
   - ***Ignore Networks***. In this field, you can enter a list of networks and hosts from which certificate authentication ***is not required***. During each login, the platform will compare the client's IP address to the list entered in this field. If the client's IP address is included in this field, SL1 will not require certificate authentication from that client.

     - You can enter one or more IP addresses, each separated by a new-line character (press the **[<Enter>]** key).
     - In the list of IPs to ignore, you can enter only the first octet, only the first and second octet, only the first, second, and third octet, or all four octets. SL1 will interpret the entry as if the rightmost octet is followed by * (asterisk).

       For example:

       - 192.168.10.142 will allow a single host to log in to the user interface without certificate authentication
       - 192 behaves the same as entering 192*. This will allow all hosts included in 192.0.0.1 through 192.254.254.254 to log in to the user interface without certificate authentication

- 192.168.10.24 behaves the same as entering 192.168.10.24*. This will allow all hosts 192.168.10.24, 192.168.10.240, 192.168.10.241, 192.168.10.242, 192.168.10.243, 192.168.10.244, 192.168.10.245, 192.168.10.246, 192.168.10.247, 192.168.10.248, and 192.168.10.249

4. Click the **[Save]** button to save your settings. The user interface displays the message:

```
Settings Saved Successfully. Configuration must be tested in order to take
effect.
```

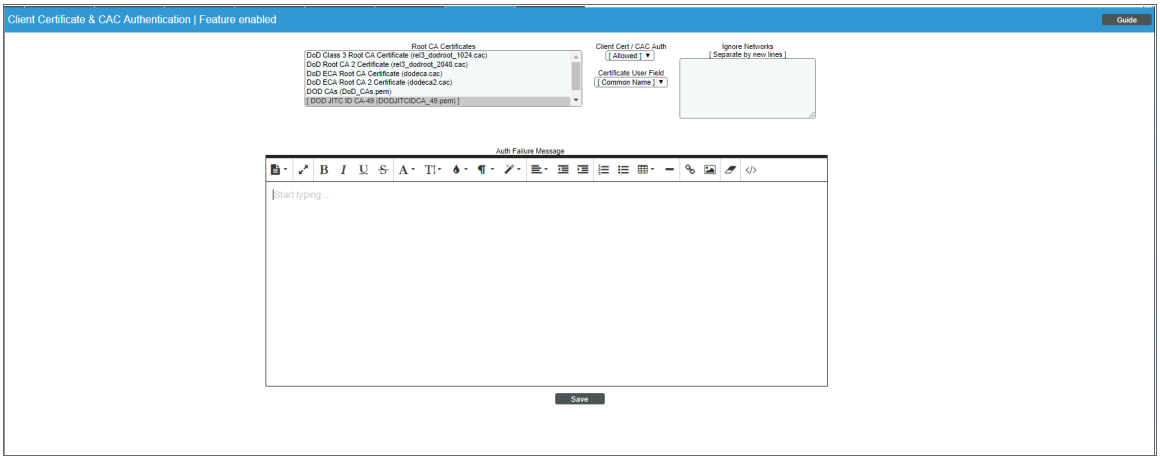
5. Click the **Test** link to test the configuration against your current client-side certificate.

Testing the Configuration

After you define the certificate authentication settings, you must test your client-side certificate against the server-side certificate you selected in the ***Root CA Certificates*** field. Testing your configuration is required to prevent an incorrect configuration from preventing administrator access to the user interface. If the test is successful, the certificate authentication settings will be applied. If the test is unsuccessful, the certificate authentication settings will not be applied.

To test certificate authentication settings:

1. Access the user interface with your CAC or a browser with the your client-side certificate installed.
2. Go to the **Client Certificate & CAC Authentication** page (System > Settings > Authentication > CAC Client Cert Auth).



3. Define the authentication settings.
4. After defining the certificate, you will see the following message at the top of the pane:

```
Configuration must be tested in order to take effect: TEST.
```

5. Click the **TEST** link. SL1 will attempt to authenticate your client-side certificate against the selected server-side certificate.

6. If the test authentication is successful, SL1 will display the following message at the top of the pane and end users with the appropriate client certificate or CAC can now access the user interface using client certificate authentication:

```
Configuration verified and enabled.
```

7. A new field, ***Client Cert / CAC Auth***, appears with a default value of *Allowed*. You can select one of the following values for this field:

    - *Allowed*. This is the default value. Users with CAC and a corresponding account in the platform are automatically logged in to the platform when the user enters the URL of the Administration Portal or the All-In-One. If a CAC user does not have an account defined in the platform, the login screen is displayed. When a non-CAC user enters the URL of the Administration Portal or the All-In-One, he/she will see the message defined in the ***Auth Failure Message*** field (defined in the previous section).
    - *Locked*. Users with CAC and an aligned account in the platform are automatically logged in to the platform when the user enters the URL of the Administration Portal or the All-In-One. If a CAC user does not have an account defined in the platform, or a user does not have a CAC, when that user enters the URL of the Administration Portal or the All-In-One, he/she will see the message defined in the ***Auth Failure Message*** field (defined in the *certificate authentication settings*).

NOTE: ScienceLogic recommends that you set this field to *Locked* unless your implementation specifically requires one of the other options.

    - *Disabled*. When a user enters the URL of the Administration Portal or the All-In-One Appliance, the platform displays the login screen.

8. Select the **[Save]** button to save the setting in the ***Client Cert / CAC Auth field***.
9. If the test authentication is unsuccessful, the user interface will display the following message at the top of the pane. The settings will not be applied, and client certificate authentication will not be used until the problem is corrected:

```
ERROR: configuration was not successfully tested with CAC or Client
Certificate.
```

Chapter 11

Installing an SSL Certificate

Overview

SSL is an acronym for Secure Sockets Layer. SSL is a protocol for securely transmitting data via the internet. SSL uses a private key to encrypt data to be transferred over the Internet connection. Usually, URLs that include "HTTPS" are using SSL for security.

To implement SSL, an SSL certificate resides on the web server and is used to encrypt the data and to identify the website. The SSL certificate contains information about the certificate holder, the domain for which the certificate was issued, the name of the Certificate Authority who issued the certificate, and the root and the country in which the certificate was issued.

There are two ways to acquire an SSL certificate:

- You can purchase a certificate from a vendor (called a "certificate authority"), such as VeriSign or GeoTrust.
- You can "self-sign" your own certificate. Using available tools (both open source and proprietary), you can create and sign your own SSL certificate instead of purchasing from a certificate authority.

SL1 includes a self-signed certificate from ScienceLogic. Self-signed certificates can trigger a warning message in some browsers. For this reasons, some customers might prefer to purchase an SSL certificate from a certificate authority and install the certificate on one or more servers.

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

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

This chapter includes the following topics:

Certificates for ScienceLogic Servers

Each SL1 appliance includes a self-signed certificate from ScienceLogic.

Each SL1 appliance uses the Nginx web server and OpenSSL.

If you want to use commercial SSL certificates with SL1, you must purchase certificates for the following SL1 appliances:

- For each Administration Portal, Database Server, or All-In-One Appliance you must purchase ***two*** certificates, one for the standard user interface and one for the Configuration Utility.
- For each Data Collector, you must purchase one certificate, for use with the Configuration Utility.
- For each Message Collector, you must purchase one certificate, for use with the Configuration Utility.

Requesting a Commercial SSL Certificate

To purchase a commercial SSL certificate, you must first create a private key and then use the private key to create a Certificate Signing Request (CSR). You must then send the CSR to a Certificate Authority (CA). Some well-known CAs are VeriSign, GeoTrust, Thawte, GoDaddy, and Comodo. The CA will charge you a fee and send you a certificate for use with your private key.

To create a CSR, perform the following on each SL1 appliance.

1. Either go to the console of the SL1 appliance or use SSH to access the server. Open a shell session on the SL1 appliance. Log in as "em7admin".
2. First, you must generate a private key for the server. To do this, enter the following at the shell prompt:

   ```
   sudo openssl genrsa -aes256 -out [keyname].key 4096
   ```

   where:

   - *[keyname]* is a name for the private key. For example, you might want to name the private key for an administration portal *adminport.key*.

NOTE: Make sure the file is **not** named ***silossl.key***. This is the name of the pre-existing ScienceLogic, self-signed certificate file.

3. You will be prompted to enter a pass phrase for the key.
4. Best practice is to make a backup copy of the key file and the pass phrase and store both in a secure location.

5. You must remove the pass phrase from the key before generating a Certificate Signing Request (CSR). To do this, enter the following at the shell prompt, inserting the keyname you used where indicated:

```
sudo openssl rsa -in [keyname].key -out [keyname].key.insecure
```

6. Next, you must create a Certificate Signing Request (CSR) for the private key you created in the previous steps. To do this, enter the following at the shell prompt:

```
sudo openssl req -new -key [keyname].key.insecure -out [keyname].csr
```

where:

- *[keyname]* is a name for the CSR for the specific server. For example, you might want to name the private key for an administration portal *adminport.key* and name the CSR for that key *adminport.csr*.

NOTE: Make sure the keyname is **not** ***silossl.key***. This is the name of the pre-existing ScienceLogic, self-signed certificate file.

7. You will be prompted to enter the Common Name. Enter the fully qualified domain name of the server where the certificate will be used and SSL and https will be run.

   For example, if the SL1 appliance is accessed at https://company.adminportal.com, you would enter "company.adminportal.com" as the Common Name.

8. You can now send the .csr file to a Certificate Authority. The Certificate Authority will provide details on how to send the .csr file. The Certificate Authority will send you a .crt file. The .crt file is the public key that matches your private key for the SL1 appliance. Some Certificate Authorities, e.g. GoDaddy, might use an intermediate certificate to sign the provided certificate. If an intermediate certificate is used, the Certificate Authority will provide a bundle of chained certificates in a second .crt file.

Creating Your Own Certificate

There are two ways to create your own SSL certificate:

- If your organization is a root Certificate Authority (for example, some departments of the US government), you can create your own private key and public key for each ScienceLogic server.
- If your security requirements allow a self-signed certificate, you can create your own private key and public key for each SL1 appliance.

Remember to create key pairs for all for each SL1 appliance in your SL1 system and also remember to create two key pairs for each Administration Portal in your SL1 system. For a list of required certificates, see the *Certificates for ScienceLogic Servers* section.

If your organization is a Certificate Authority, see your organization's internal documentation on creating a certificate for Nginx.

If you want to create a self-signed certificate, perform the following:

1. Either go to the console of the SL1 appliance or use SSH to access the server. Open a shell session on the SL1 appliance. Log in as "em7admin".
2. First, you must generate a private key for the server. To do this, enter the following at the shell prompt:

   ```
   sudo openssl genrsa -aes256 -out [keyname].key 4096
   ```

   where *[keyname]* is a name for the private key. For example, you might want to name the private key for an administration portal *adminport.key*.

NOTE: Make sure the file is **not** named ***silossl.key.***. This is the name of the pre-existing ScienceLogic, self-signed certificate file.

3. You will be prompted to enter a pass phrase for the key.
4. Best practice is to make a backup copy of the key file and the pass phrase and store both in a secure location.
5. Next, you must create a self-signed certificate based on the private key you generated in the previous steps.

   To do this, enter the following at the shell prompt:

   ```
   sudo openssl req -new -x509 -nodes -sha1 -days 365 -key [keyname].key -out
   [keyname].crt
   ```

   where:

   - *[keyname]*.key is the private key for the SL1 appliance .
   - *[keyname]*.crt is the public key (certificate) for the SL1 appliance.

   For example, you might want to name the private key for an administration portal *adminport.key* and name the certificate file for that key *adminport.crt*.

NOTE: Make sure the files are **not** named ***silossl.crt*** and ***silossl.key***. These are the names of the pre-existing ScienceLogic, self-signed certificate files.

6. The resulting .crt file is the public key that matches your private key for the SL1 appliance.

Installing the Certificate on an SL1 Appliance

ScienceLogic does not provide support for third party certificates. Be advised that installing a new SSL certificate can affect the operation of SSL services.

Most certificate authorities provide support and resources on installing and enabling their certificates in Nginx web servers. If you have questions, please refer to your Certificate Authority.

WARNING: The following steps will stop and restart the SL1 appliance and temporarily make the Administration Portal site unavailable. Confirm with your System Administrator that you are permitted to restart the ScienceLogic Web Service.

NOTE: These instructions assume that you are familiar with the Linux shell and the "vi" editor.

To install a commercial SSL certificate on a SL1 appliance, perform the following:

1. Purchase a certificate from a certificate authority.
2. Copy the certificate files (*.key and all *.crt files) to a server that can access the SL1 appliance via SFTP.

NOTE: Make sure the files are **not** named ***silossl.crt*** and ***silossl.key***. These are the names of the pre-existing ScienceLogic, self-signed certificate files.

3. Use SFTP or SCP to copy the .crt file(s) and the .key file to the SL1 appliance in the /etc/nginx directory.
4. Either go to the console of the SL1 appliance or use SSH to access the server. Open a shell session on the SL1 appliance. Log in as "em7admin".
5. If an intermediate certificate has been used to sign the certificate file, execute the following commands to combine the server certificate and the bundle of chained certificates provided by the Certificate Authority, entering the server certificate name, bundle name, and combined certificate name where indicated:

```
cd /etc/nginx
cat [server certificate name].crt [bundle name].crt > [combined certificate name].crt
```

   Use the combined .crt file name when updating the nginx configuration.

6. For each appliance, edit the following files to configure the certificate for the Configuration Utility:
   - /etc/nginx/conf.d/em7webconfig.conf
   - /etc/nginx/conf.d/em7_sladmin.conf
   - Edit the following lines, removing references to silossl.crt and silossl.key and replacing with the names of the new .key and .crtfiles:

```
ssl_certificate /etc/nginx/[name of .crt file];

ssl_certificate_key /etc/nginx/[name of .key file];
```

7. In addition, for each Administration Portal, Database Server, and All-In-One Appliance, you must also edit the following files to configure the certificate for the user interface:

    - /etc/nginx/conf.d/em7ngx_web_ui.conf
    - /etc/nginx/conf.d/em7ngx_em7proxy_web_ui.conf
    - Edit the following lines, removing references to silossl.pem and silossl.key and replacing with the names of the new key files:

    ```
    ssl_certificate /etc/nginx/[name of .crt file];

    ssl_certificate_key /etc/nginx/[name of .key file];
    ```

8. Next, you will need to restart the webconfig and webserver. To do this, execute the following command:

    - For all appliances, enter:

    ```
    sudo systemctl restart nginx
    ```

9. To test the SSL certificate, open a browser session and connect to the Administration Portal, Database Server, or All-In-One Appliance using https.

    - From the Administration Portal, go to System > Settings > Appliances.
    - In the **Appliance Manager** page, select the toolbox icon () for each server. Notice that the URL for the Configuration Utility includes https.

Chapter 12

Authentication Profiles and Resources

Overview

This chapter describes the following topics:

- ***Authentication Profiles***. Policies that align user accounts with one or more types of authentication.
- ***Authentication Resources***. Configuration policies that describe how SL1 should communicate with a user store.

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

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

This chapter includes the following topics:

Authentication Profiles

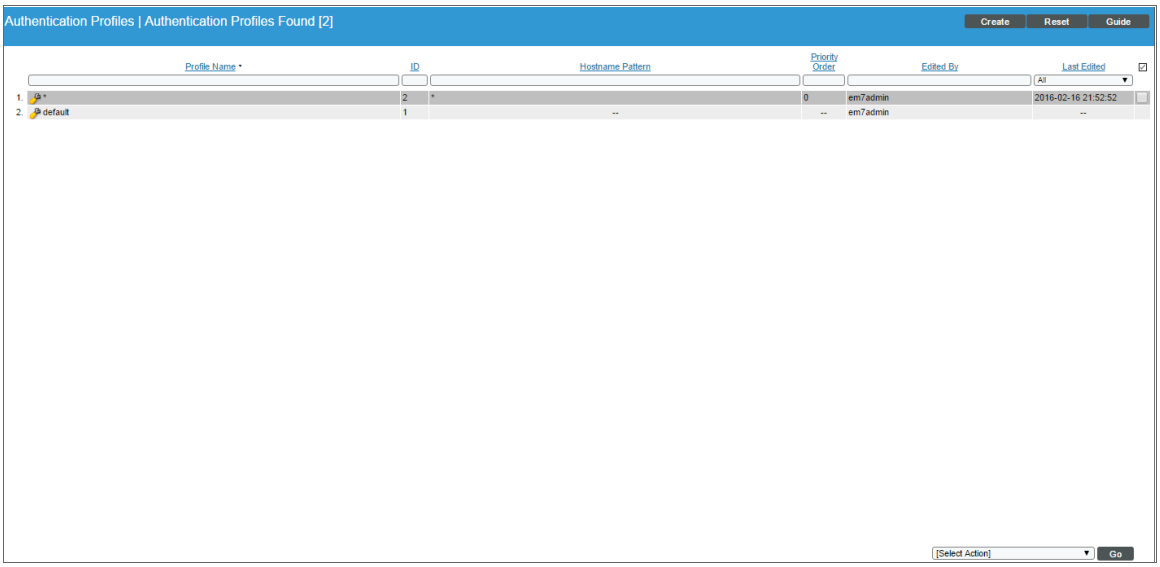
Authentication profiles are policies that align user accounts with one or more types of authentication:

- ***Alignment by pattern matching***. SL1 examines the URL or IP address that a user enters in a browser to connect to an Administration Portal, Database Server, or All-In-One Appliance. If the URL or IP address matches the criteria specified in an authentication profile, SL1 will automatically use the matching profile to perform user authentication.
- ***Credential Source***. Specifies from where SL1 should extract the user name and password or certificate to be authenticated. These credentials are passed to SL1 via HTTP. SL1 then passes the credentials to each authentication resource specified in the authentication profile. The authentication resources communicate with user stores that can authenticate the credentials.
- ***Authentication Resource***. Specifies the connector to use to communicate with the user store, the credential to use to connect to the user store (if applicable), and the URLs to examine during authentication. Also maps attributes from the user's account in the user store to fields in the ScienceLogic user account. For details on creating an authentication resource, see the section on *Authentication Resources*.

Viewing the List of Authentication Profiles

To view a list of all authentication profiles in SL1:

1. Go to the **Authentication Profiles** page (System > Settings > Authentication > Profiles).



2. The following information is displayed about each authentication profile:

- ***Profile Name***. Name of the authentication profile.
- ***ID***. Unique numeric ID, automatically assigned by SL1 to each authentication profile.
- ***Hostname Pattern***. This field is used to match the URL or IP address that a user enters in a browser to connect to an Administration Portal, Database Server, or All-In-One Appliance. If the URL or IP address matches the value in this field, SL1 applies the authentication profile to the user for the current session.
- ***Priority Order***. If your SL1 System includes multiple authentication profiles, SL1 evaluates the authentication profiles in priority order, ascending. This column displays the priority order value for the authentication profiles.
- ***Edited By***. The user who created or last edited the authentication profile.
- ***Last Edited***. Date and time the authentication profile was created or last edited.

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

Filtering the List of Authentication Profiles

You can filter the list of authentication profiles on the **Authentication Profiles** page by one or more of the following parameters: **Profile Name**, **ID**, **Hostname Pattern**, **Priority Order**, **Edited By**, and **Last Edited**. The list of authentication profiles is dynamically updated as you select each filter. For each filter except **Last Edited**, you must enter text to match against. SL1 will search for authentication profiles that match the text, including partial matches. Text matches are not case-sensitive. You can use the following special characters in each filter except **Last Edited**:

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

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

- & (ampersand). Specifies an "and" operation. For example:

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

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

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

- ^ (caret mark). Specifies "starts with". For example:

  "^micro" would match all strings that start with "micro", like "microsoft".

  "^" will include all rows that have a value in the column.

  "!^" will include all rows that have no value in the column.

- $ (dollar sign). Specifies "ends with". For example:

  "$ware" would match all strings that end with "ware", like "VMware".

  "$" will include all rows that have a value in the column.

  "!$" will include all rows that have no value in the column.

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.

Only authentication profiles that meet all the following filter criteria will be displayed in the **Authentication Profiles** page:

- ***Profile Name***. Name of the authentication profile. You can enter text to match, including special characters, and the **Authentication Profiles** page will display only authentication profiles that have a matching name.
- ***ID***. Unique numeric ID, automatically assigned by SL1 to each authentication profile. You can enter text to match, including special characters, and the **Authentication Profiles** page will display only authentication profiles that have a matching ID.
- ***Hostname Pattern***. This field is used to match the URL or IP address that a user enters in a browser to connect to an Administration Portal, Database Server, or All-In-One Appliance. If the URL or IP address matches the value in this field, SL1 applies the authentication profile to the user for the current session. You can enter text to match, including special characters, and the **Authentication Profiles** page will display only authentication profiles that have a matching hostname pattern.
- ***Priority Order***. You can enter text to match, including special characters, and the **Authentication Profiles** page will display only authentication profiles that have a matching priority number.
- ***Edited By***. The user who created or last edited the authentication profile. You can enter text to match, including special characters, and the **Authentication Profiles** page will display only authentication profiles that have been created or edited by a matching username.
- ***Last Edited***. Date and time the authentication profiles was created or last edited. You can select from a list of time periods. The **Authentication Profiles** page will display only authentication profiles that have been created or edited within that time period.

The "default" Authentication Profile

SL1 includes a *default* authentication profile, for which the following rules apply:

- You cannot delete the *default* profile.
- If an ***AP Hostname Pattern*** fails to match all the other authentication profiles, SL1 applies the *default* authentication profile.
- For users running version 7.7 or earlier of SL1 who apply one or more patches to upgrade to version 7.8, the ***default*** profile allows ScienceLogic authentication to perform as it did prior to version 7.8.
  - On patched systems, the *default* profile is included in the patch.
  - On patched systems, the *default* profile is pre-configured to allow ScienceLogic administrators to log in via the ScienceLogic login page and the authentication resource *EM7 Internal*.

- On patched systems, the *default* profile is pre-configured to allow credentials via *CAC/Client Certificate*, *HTTP Auth*, or the *EM7 Login Page*.
- On patched systems, the *default* profile is pre-configured to use all legacy authentication resources: *SSO (legacy)*, *LDAP/AD (legacy)*, and *EM7 Internal*.

NOTE: Administrators can edit the default profile and use the new, non-legacy authentication resources but are not required to do so.

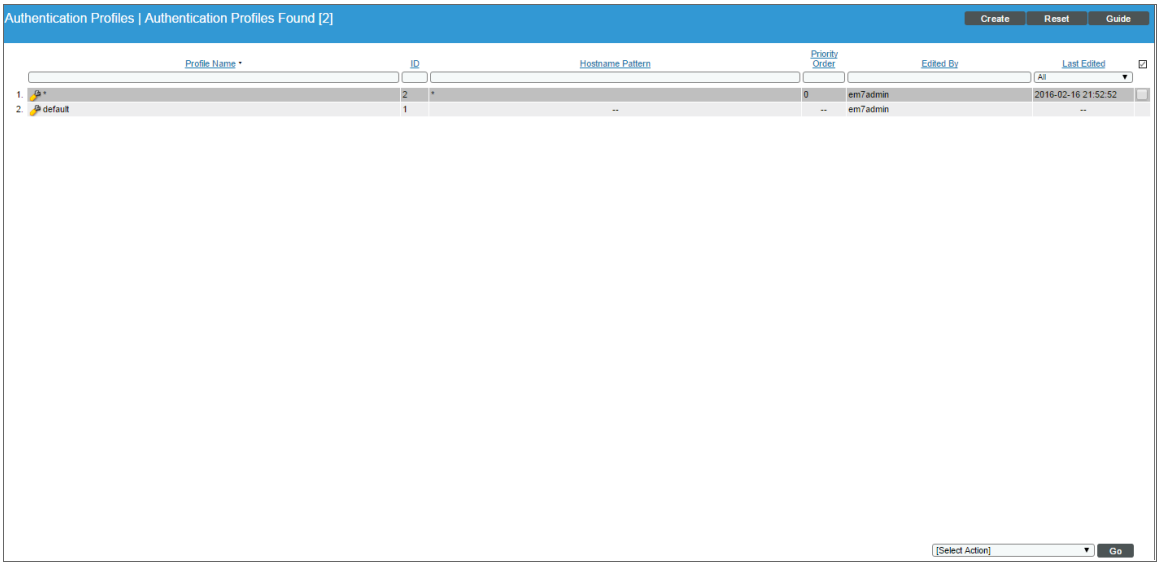
- For users who installed version 7.8 or later of SL1 using an ISO, initially the *default* profile is pre-configured to allow ScienceLogic administrators to log in via *CAC/Client Certificate*, *HTTP Auth*, or the *EM7 Login Page* and the authentication resource *EM7 Internal*. This allows administrators to log in and perform initial configuration on the SL1 system.
  - On ISO systems, the *default* profile is included in the patch.
  - On ISO systems, the *default* profile is pre-configured to allow credentials via *CAC/Client Certificate*, *HTTP Auth*, or the *EM7 Login Page*.
  - On ISO systems, the *default* profile is pre-configured to use only the authentication resource *EM7 Internal*.

NOTE: After initial configuration, administrators can edit the ***default*** profile as best fits their organization.

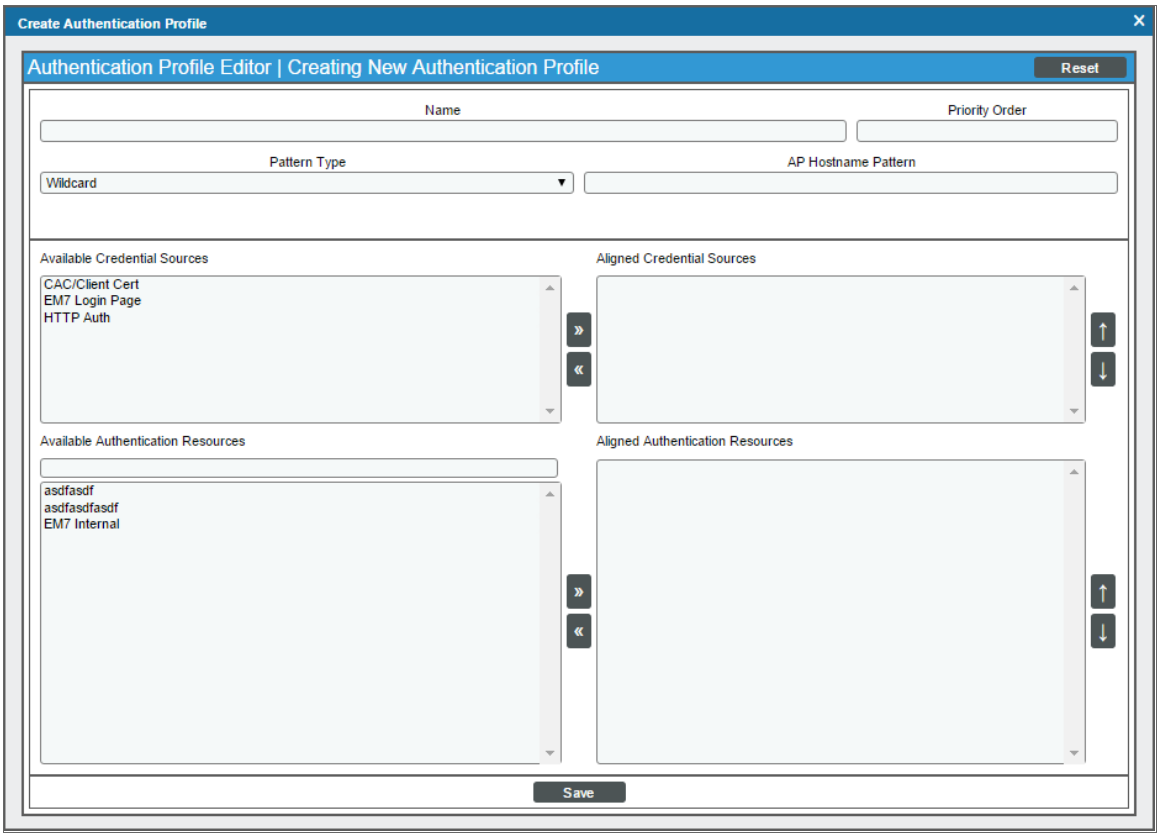
Creating an Authentication Profile

To create a new authentication profile:

1. Go to the **Authentication Profiles** page (System > Settings > Authentication > Profiles).



2. Click the **[Create]** button. The **Authentication Profile Editor** modal page appears.



3. Enter values in the following fields:

   - ***Name***. Name of the authentication profile.
   - ***Priority Order***. If your SL1 System includes multiple authentication profiles, SL1 evaluates the authentication profiles in ascending priority order. SL1 will apply the authentication profile that matches the hostname or IP in the current URL AND has the lowest value in the ***Priority Order*** field.
   - ***Pattern Type***. Specifies how SL1 will evaluate the value in the ***AP Hostname Pattern*** field. Choices are:
     - *Wildcard*. SL1 will perform a text match, with wildcard characters (asterisks).
     - *Regex*. SL1 will use regular expressions to compare the ***AP Hostname Pattern*** to the current session information.

- ***AP Hostname Pattern***. This field is used to match the URL or IP address that a user enters in a browser to connect to an Administration Portal, Database Server, or All-In-One Appliance. If the URL or IP address matches the value in this field, SL1 applies the authentication profile to the user for the current session.
    - For example, if you specify "*" (asterisk), any IP address or URL will match. SL1 will then apply this authentication profile to every session on an Administration Portal, Database Server, or All-In-One Appliance.
    - If you enter "192.168.38.235", SL1 will apply the authentication profile to each session on an Administration Portal, Database Server, or All-In-One Appliance where the user enters "192.168.38.235" into the browser.
    - If you enter "*.sciencelogic.local", SL1 will apply the authentication profile to each session on an Administration Portal, Database Server, or All-In-One Appliance where the user enters a URL ending with ".sciencelogic.local" into the browser.
- ***Available Credential Sources***. This field tells SL1 how to retrieve the user's credentials from the HTTP request to SL1. To align a credential source with the authentication profile, highlight the credential source and click the right-arrow button. You can select zero, one, or multiple credential sources for the authentication profile. Initially, this pane displays a list of all the credential sources:
    - *CAC/Client Cert*. SL1 will retrieve a certificate from the HTTP request.
    - *EM7 Login Page*. SL1 will retrieve a user name and password from the ScienceLogic login page fields.
    - *HTTP Auth*. SL1 will retrieve a user name and password from the HTTP request.

NOTE: If you are using Single Sign-On (SSO) authentication, the ***Available Credential Sources*** field is ignored. You do not have to align a credential source because credentials are submitted directly to an Identity Provider (IdP) instead of SL1.

- ***Aligned Credentials Sources***. This field displays the list of credential sources that have been aligned with the authentication profile. The authentication profile will examine each credential source in the order in which it appears in this list. When the authentication profile find the user's credential, the authentication profile stops examining any remaining credential sources in the list.
- ***Available Authentication Resources***.This field tells SL1 which authentication resources to use to authenticate the retrieved credentials. To align an authentication resource with the authentication profile, highlight the authentication resource and click the right-arrow button. You must select at least one authentication resource (but can select more than one). For details on creating an authentication resource, see the section on *Authentication Resources*.
- ***Aligned Authentication Resources***. This field displays the list of authentication resources that have been aligned with the authentication profile. The authentication profile will examine each authentication resource in the order in which it appears in this list. When an authentication resource successfully authenticates the user, the authentication profile stops executing any remaining authentication resources in the list.

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

Editing an Authentication Profile

The **Authentication Profiles** page allows you to edit an existing authentication profile. To do so:

1. Go to the **Authentication Profiles** page (System > Settings > Authentication > Profiles).
2. Find the authentication profile that you want to edit. Click its wrench icon ().
3. The **Authentication Profile Editor** modal page appears. In this page, you can edit the value of one or more fields.
4. Click the **[Save]** button to save your changes to the authentication profile.

Deleting One or More Authentication Profiles

The **Authentication Profiles** page allows you to delete one or more authentication profiles from SL1. To do so:

1. Go to the **Authentication Profiles** page (System > Settings > Authentication > Profiles).
2. Select the checkbox of each authentication profile that you want to delete.
3. Click the ***Select Actions*** menu (in the lower right), select *DELETE Authentication Profile*, and then click the **[Go]** button. The selected authentication profiles will be deleted.

NOTE: You cannot delete the ***default*** authentication profile.

Authentication Resources

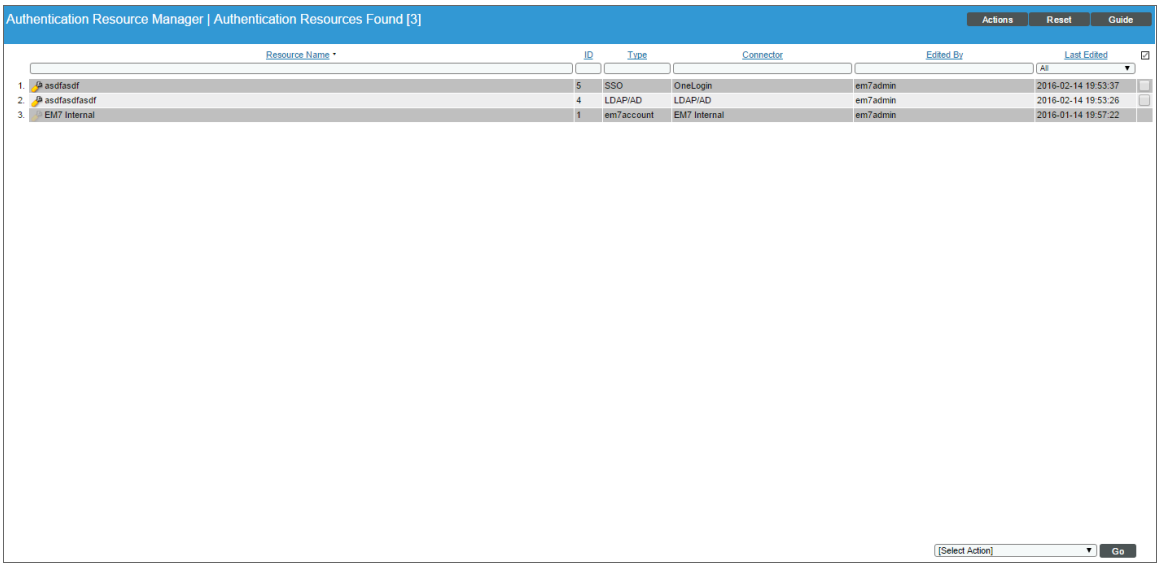
An authentication resource is a configuration policy that describes how SL1 should communicate with a user store. An authentication resource specifies the connector to use to communicate with the user store, the credential to use to connect to the user store (if applicable), and the URLs to examine during authentication. An authentication resource also maps attributes from the user's account in the user store to fields in the ScienceLogic user account.

Viewing the List of Authentication Resources

The **Authentication Resource Manager** page displays a list of all authentication resources in the SL1 System.

To view the list of authentication resources :

1. Go to the **Authentication Resource Manager** page (System > Settings > Authentication > Resources).



2. The following information is displayed about each authentication resource:

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

- ***Resource Name***. Name of the authentication resource.
- ***ID***. Unique numeric ID, automatically assigned by SL1 to each authentication resource.
- ***Type***. Specifies the user store that is associated with the resource. Possible types are:
  - *EM7 Internal*. The authentication resource communicates and passes information to and from the ScienceLogic Database.
  - *LDAP/AD*. The authentication resource communicates and passes information to and from an LDAP server or Active Directory server.
  - *SSO*. The authentication resource communicates and passes information to and from a SAML Identity Provider (IdP) or Service Provider (SP).

- ***Connector***. The software that allows communication between the authentication resource and the user store. Possible connectors are:
  - *EM7 Internal*. Software that communicates with the ScienceLogic Database.
  - *LDAP/AD*. Software that communicates with an LDAP server or Active Directory server.
  - *LDAP/AD - Legacy*. Software that communicates with an LDAP server or Active Directory server for ScienceLogic servers that were configured prior to version 7.8 of SL1. SL1 Systems that were upgraded to version 7.8 using patches can continue to use the same authentication methods without making changes to user accounts or the LDAP server or Active Directory server.
  - *OneLogin*. Software that communicates with a SAML Identity Provider (IdP).
  - *SimpleSAML - Legacy*. Software that communicates with a SAML Identity Provider (IdP) and Service Provider (SP) for ScienceLogic servers that were configured prior to version 7.8 of SL1. SL1 Systems that were upgraded to version 7.8 using patches can continue to use the same authentication methods without making changes to user accounts, the SAML configuration, or the SSO provider.
- ***Edited By***. The user who created or last edited the authentication resource.
- ***Last Edited***. Date the time the authentication resource was created or last edited.

Filtering the List of Authentication Resources

You can filter the list of authentication resources on the **Authentication Resource Manager** page by one or more of the following parameters: **Resource Name**, **ID**, **Type**, **Connector**, **Edited By**, and **Last Edited**.The list of authentication resources is dynamically updated as you select each filter. For each filter except **Last Edited**, you must enter text to match against. SL1 will search for authentication resources that match the text, including partial matches. Text matches are not case-sensitive. You can use the following special characters in each filter except **Last Edited**:

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

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

- & (ampersand). Specifies an "and" operation. For example:

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

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

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

- ^ (caret mark). Specifies "starts with". For example:

  "^micro" would match all strings that start with "micro", like "microsoft".

  "^" will include all rows that have a value in the column.

  "!^" will include all rows that have no value in the column.

- $ (dollar sign). Specifies "ends with". For example:

  "$ware" would match all strings that end with "ware", like "VMware".

  "$" will include all rows that have a value in the column.

  "!$" will include all rows that have no value in the column.

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.

Only authentication resources that meet all the following filter criteria will be displayed in the **Authentication Resource Manager** page:

- ***Resource Name***. Name of the authentication resource. You can enter text to match, including special characters, and the **Authentication Resource Manager** page will display only authentication resources that have a matching name.
- ***ID***. Unique numeric ID, automatically assigned by SL1 to each authentication resource. You can enter text to match, including special characters, and the **Authentication Resource Manager** page will display only authentication resources that have a matching ID.
- ***Type***.Specifies the user store that is associated with the resource. You can enter text to match, including special characters, and the **Authentication Resource Manager** page will display only authentication resources that have a matching type.
- ***Connector***. The specific software that allows communication between the authentication resource and the user store. You can enter text to match, including special characters, and the **Authentication Resource Manager** page will display only authentication resources that have a matching connector.
- ***Last Edited***. Date and time the authentication resources was created or last edited. You can select from a list of time periods. The **Authentication Resource Manager** page will display only authentication resources that have been created or edited within that time period.
- ***Edited By***. ScienceLogic user who created or last edited the authentication resource. You can enter text to match, including special characters, and the **Authentication Resource Manager** page will display only authentication resources that have been created or edited by a matching username.

The "EM7 Internal" Resource

The *EM7 Internal* resource allows you to access the user store in the ScienceLogic database.

- By default, each SL1 System, whether upgraded to version 7.8 or built from a 7.8 ISO, includes the *EM7 Internal* authentication resource.
- You cannot create an *EM7 Internal* authentication resource.
- You cannot edit or delete the *EM7 Internal* authentication resource included with your SL1 System.
- Each SL1 System can include only one the *EM7 Internal* authentication resource.

The Legacy Authentication Resources

SL1 includes two "legacy" authentication resources:

- *LDAP/AD* with connector *LDAP/AD - Legacy*
- *SSO (legacy)* with connector *SimpleSAML - Legacy*

These legacy authentication resources allow patched systems (systems that upgraded to version 7.8 of SL1) to continue using the same authentication as used prior to upgrading to version 7.8.

- Legacy authentication resources are available only on systems that have upgraded from a previous version of SL1.
- You cannot create a new authentication resource using the legacy connectors.
- If you edit and save changes to the *LDAP/AD* authentication resource, SL1 updates the connector from *LDAP/AD - Legacy* to the non-legacy connector *LDAP/AD*.

Creating an LDAP/AD Authentication Resource

The **LDAP/AD Auth Resource Editor** modal page allows you to define an authentication resource for use with an LDAP/AD user store. An LDAP/AD authentication resource specifies the connector (communication software) to use to communicate with the LDAP/AD user store and the credential to use to connect to the user store. An LDAP/AD authentication resource can also map attributes from the user's LDAP/AD account to fields in the ScienceLogic user account.

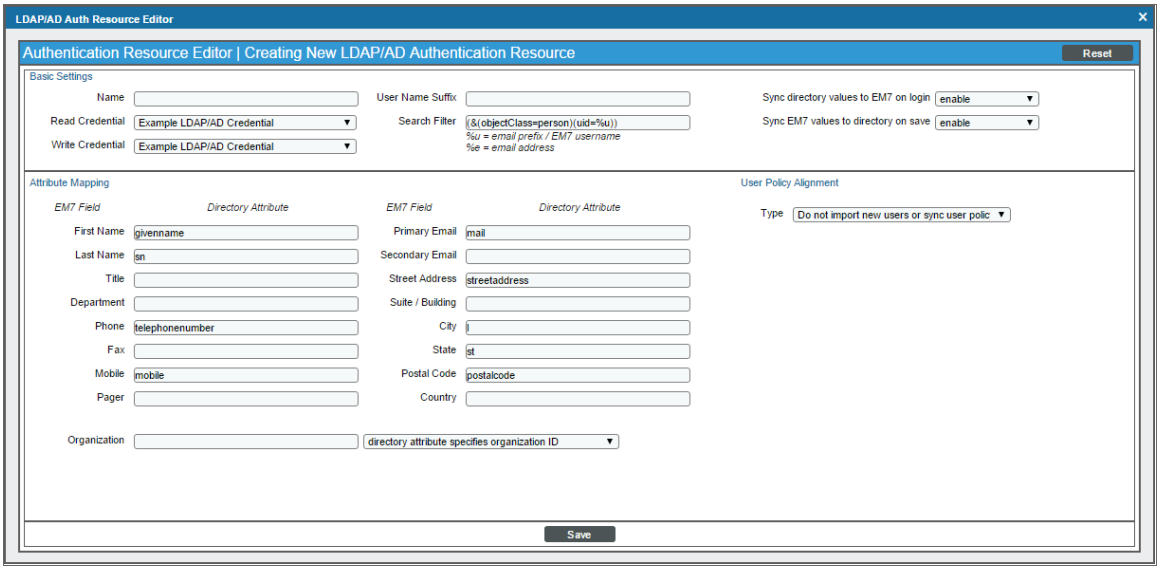
ScienceLogic administrators can use LDAP or Active Directory to authenticate ScienceLogic users. There are two ways to use LDAP or Active Directory authentication with SL1:

- You can configure SL1 to automatically create user accounts for existing LDAP or Active Directory users and then always use LDAP or Active Directory to authenticate those users when they log in to SL1.
- You can use LDAP or Active Directory to authenticate one or more ScienceLogic users when they log in to SL1.

To create an LDAP/AD authentication resource:

1. Go to the **Authentication Resource Manager** page (System > Settings > Authentication > Resources).

2. Click the **[Actions]** menu and then select *Create LDAP/AD Resource*. The **LDAP/AD Auth Resource Editor** modal page appears.



3. Enter values in the following fields:

Basic Settings

- ***Name***. Name of the LDAP/AD authentication resource.
- ***Read Credential***. Credential that allows SL1 to read data from an LDAP or Active Directory server. Select from a list of all LDAP and Active Directory credentials to which you have access. If this field has been set to a credential to which you do not have access, this field will display the value *Restricted Credential*. If you set this field to a different credential, the entry for *Restricted Credential* will be removed from the field; you will not be able to re-align the field with the *Restricted Credential*.
- ***Write Credential***. Credential that allows SL1 to write data to an LDAP or Active Directory server. Select from a list of all LDAP and Active Directory credentials to which you have access. If this field has been set to a credential to which you do not have access, this field will display the value *Restricted Credential*. If you set this field to a different credential, the entry for *Restricted Credential* will be removed from the field; you will not be able to re-align the field with the *Restricted Credential*.

NOTE: Your organization membership(s) might affect the list of credentials you can see in the ***Read Credential*** field and the ***Write Credential*** field. For details, see the ***Discovery & Credentials*** manual.

- ***User Name Suffix***. Optional field. Because SL1 can authenticate against multiple LDAP or Active Directory servers, there is a risk of collision among user names. In this field, you can enter a string to append to the user name to minimize the risk of collision. For example:
    - Suppose we entered ***@ad.local*** in this field.

- Suppose the next LDAP/AD user logs in to SL1 with the user name ***bishopbrennan***.
- SL1 will log that user in as ***bishopbrennan@ad.local***.

NOTE: A best practice to avoid collisions is to use email addresses as user names.

- ***Search Filter***. Specifies where to find the user's account information in LDAP or Active Directory. You must tell SL1 where to find the LDAP or AD attribute that maps to the user's account name in SL1.

  For example, an LDAP user might use his/her uid value to log in to SL1. In the ScienceLogic account, that uid value will then become the user's ***Account Login Name***.

  You can use the following variables in the search filter:

  - %u. ScienceLogic login name.
  - %e. Email address.
  - An example search filter for LDAP might be:

```
(&(objectClass=person)(uid=%u))
```

  This says to search in the object class called "person" for the uid that matches the ScienceLogic login name (entered when the user logs in to SL1 and then stored in the variable %u).

  - An example search filter for Active Directory might be:

```
(samaccountname=%u)
```

  This says to search for the samaccountname attribute that matches the ScienceLogic login name (entered when the user logs in to SL1 and then stored in the variable %u).

  - For more information on the syntax of LDAP and AD search filters, see RFC 4515.

- ***Sync directory values to EM7 on login***. If an LDAP or AD administrator makes changes to an LDAP or AD account, SL1 will automatically retrieve those updates and apply them to the user's account in SL1 (in the **Account Properties** page) the next time the user logs in to SL1. (For more information about user account properties, see the ***Organizations & Users*** manual.)
- ***Sync EM7 values to directory on save***. If a ScienceLogic administrator made changes to the ScienceLogic account, SL1 will automatically write those changes to the user's account in LDAP or Active Directory.

NOTE: The ***Sync EM7 values to directory on save*** option requires a write credential.

Attribute Mapping

If you have configured SL1 to automatically create ScienceLogic accounts for LDAP or AD users, these fields specify the LDAP or AD attribute value that will be automatically inserted into each field in each user's **Account Properties** page. (For more information about user account properties, see the ***Organizations & Users*** manual.)

SL1 automatically populates as many of these fields as possible. You can edit or delete the default values provided by SL1. For example, SL1 automatically inserts the value of the LDAP/AD attribute "sn" (surname) into the ***Last Name*** field in each user's **Account Properties** page.

NOTE: SL1 requires that the LDAP or AD attribute name that you specify in each field uses ***all lower-case characters***.

- ***First Name***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***First Name*** field in each user's **Account Properties** page. By default, SL1 inserts the value of the LDAP/AD attribute "givenname" into this field.
- ***Last Name***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***Last Name*** field in each user's **Account Properties** page. By default, SL1 inserts the value of the LDAP/AD attribute "sn" into this field.
- ***Title***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***Title*** field in each user's **Account Properties** page.
- ***Department***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***Department*** field in each user's **Account Properties** page.
- ***Phone***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***Phone*** field in each user's **Account Properties** page. By default, SL1 inserts the value of the LDAP/AD attribute "telephonenumber" into this field.
- ***Fax***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***Fax*** field in each user's **Account Properties** page.
- ***Mobile***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***Mobile*** field in each user's **Account Properties** page. By default, SL1 inserts the value of the LDAP/AD attribute "mobile" into this field.
- ***Pager***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***Pager*** field in each user's **Account Properties** page.
- ***Primary Email***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***Primary Email*** field in each user's **Account Properties** page. By default, SL1 inserts the value of the LDAP/AD attribute "mail" into this field.
- ***Secondary Email***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***Secondary Email*** field in each user's **Account Properties** page.
- ***Street Address***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***Street Address*** field in each user's **Account Properties** page. By default, SL1 inserts the value of the LDAP/AD attribute "streetaddress" into this field.
- ***Suite/Building***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***Suite/Building*** field in each user's **Account Properties** page.

- ***City***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***City*** field in each user's **Account Properties** page. By default, SL1 inserts the value of the LDAP/AD attribute "l" into this field.
- ***State***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***State*** field in each user's **Account Properties** page. By default, SL1 inserts the value of the LDAP/AD attribute "st" into this field.
- ***Postal Code***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***Postal Code*** field in each user's **Account Properties** page. By default, SL1 inserts the value of the LDAP/AD attribute "postalcode" into this field.
- ***Country***. Specifies the LDAP or AD attribute value that will be automatically inserted into the ***Country*** field in each user's **Account Properties** page.
- ***Organization***. Specifies the LDAP or AD attribute value that will be used to automatically define the ***Primary Organization*** field in each user's **Account Permissions** page. You must also specify one of the following:
    - *directory attribute specifies organization ID*. If selected, the attribute in the ***Organization*** field specifies an organization ID.
    - *directory attribute specifies organization name*. If selected, the attribute in the ***Organization*** field specifies an organization name.
    - *directory attribute specifies organization CRM ID*. If selected, the attribute in the ***Organization*** field specifies the CRM ID of an organization.

NOTE: To use Attribute Mapping for ***Organization***, your LDAP/AD schema must include an attribute that maps to ScienceLogic Organization names, Organization IDs, or Organization CRM IDs.

NOTE: When you create a new LDAP/AD user, you must align a user policy with that user. If the aligned user policy specifies an organization for the user, the value from the user policy will overwrite the value from Attribute Mapping.

User Policy Alignment

- ***Type***. Specifies whether SL1 should automatically create ScienceLogic accounts for each LDAP or Active Directory user in the search base (which is specified in the credential), whether SL1 should simply use LDAP or Active Directory to authenticate one or more users, or whether SL1 will refuse to authenticate specific users. Choices are:
    - *Do not authenticate new users from directory*. Only those users who have an account already created in SL1 can log in to SL1. However, if one or more users' **Account Permissions** page specifies *LDAP /Active Directory* in the ***Authentication Method*** field, SL1 will authenticate those users with either LDAP or Active Directory, using the settings and credentials specified in this page.
    - *Static policy alignment*. If an LDAP or AD user logs in to SL1 using the LDAP or AD attribute specified in the ***Search Filter*** field, SL1 will automatically create an account for that user. SL1 will

use ***one user policy*** (specified in the ***Policy*** field) to create all imported LDAP or AD user accounts. SL1 will also use the settings and credentials specified in this page when creating the account.

- *Dynamic policy alignment*. If an LDAP or AD user logs in to SL1 using the LDAP or AD attribute specified in the ***Search Filter*** field, SL1 will automatically create an account for that user. SL1 will ***choose from among multiple user policies*** to create imported LDAP or AD user accounts. For example, some imported user accounts might use "user policy A"; other imported user accounts might use "user policy B". SL1 will also use the settings and credentials specified in this page when creating the account.

NOTE: If you selected *Static policy alignment* in the ***Type*** field, you must supply a value in the ***Policy*** field:

- ***Policy***. Specifies the user policy to use to automatically create a ScienceLogic account for each LDAP or AD user. Select from a list of all user policies that specify *LDAP /Active Directory* in the ***Authentication Method*** field.

NOTE: If you selected *Dynamic policy alignment* in the ***Type*** field, you must supply values in the ***Attribute***, ***Value***, and ***Policy*** fields.

- ***Attribute***. Specifies the LDAP or AD attribute you want to use to differentiate imported user accounts. For example, you could select the attribute "department" and then assign different user policies to import user accounts from different departments. You can also use this field to exclude LDAP or AD accounts for which you do not want to create a ScienceLogic account.
- ***Value***. Specifies the LDAP or AD attribute value. That is, you specify one of the possible values for the attribute (specified in the ***Attribute*** field). SL1 will compare the value in this field to the retrieved value for the ***Attribute***.
- ***Policy***. Choose one of the following:
  - *Do Not Authenticate*. If selected, if the retrieved value of the specified ***Attribute*** matches the value in the ***Value*** field, the user is not authenticated. This setting applies to new users for whom LDAP or Active Directory would have to create a new account in SL1 and for users who already have an account in SL1.
  - *the policy you want to associate with that value*. Select from a list of all user policies that specify *LDAP /Active Directory* in the ***Authentication Method*** field.
    - For example, suppose you specified "department" in the ***Attribute*** field. Suppose that the "department" attribute could have two possible values: "Sales" or "NOC".
    - Suppose you created two user policies. One user policy, called "Sales User Policy", includes the appropriate ticket queues and access keys for Sales personnel. Another user policy, called "NOC User Policy", include the appropriate ticket queues and access keys for NOC personnel.
    - In one of the ***Value*** fields, you could specify "Sales". In the corresponding ***Policy*** field, you could then specify "Sales User Policy".

- In the next ***Value*** field, you could specify "NOC". In the corresponding ***Policy*** field, you could specify "NOC User Policy.
- After defining these two ***Value*** fields and corresponding ***Policy*** fields, user accounts from the Sales department would be imported into SL1 using the Sales User Policy. User accounts from the NOC department would be imported into SL1 using the NOC User Policy.

- To define additional ***Value*** and ***Policy*** fields, click on the green plus-sign ( ) icon.

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

Creating an SSO Authentication Resource

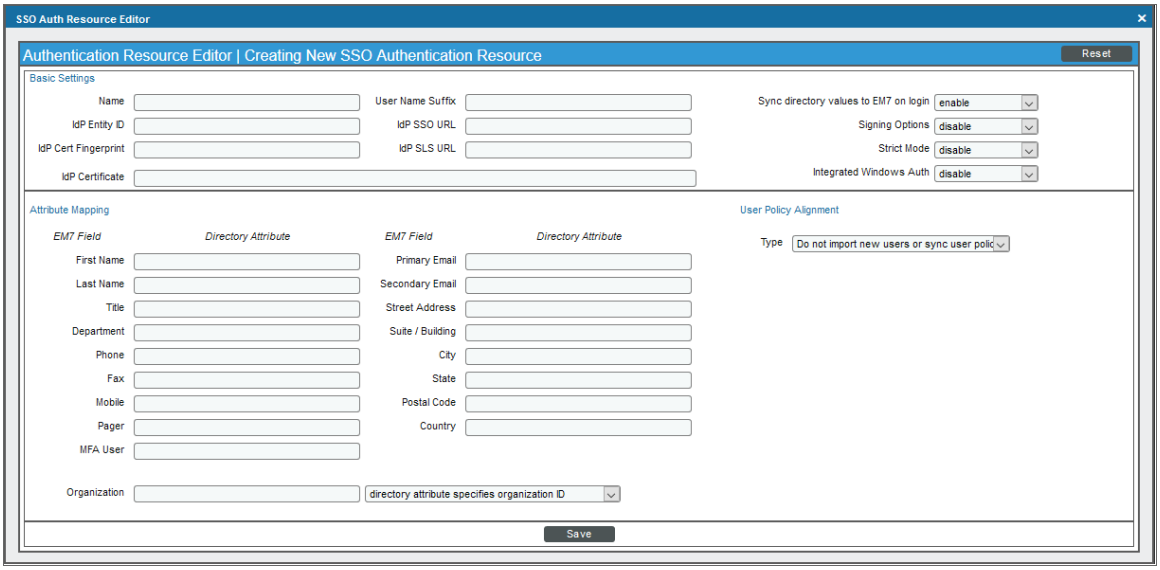
The **SSO Auth Resource Editor** page allows you to define an authentication resource for use with a SAML IdP. An SSO authentication resource specifies the connector (communication software) to use to communicate with the SAML IdP and the URLs to use to send and retrieve information from the SAML IdP. An SSO authentication resource can also maps attributes from the user's SSO account to fields in the ScienceLogic user account.

ScienceLogic administrators can use SSO to authenticate ScienceLogic users. There are two ways to use SSO authentication with SL1:

- You can configure SL1 to automatically create user accounts for existing SSO users and then always use SSO to authenticate those users when they log in to SL1.
- You can use SSO to authenticate one or more ScienceLogic users when they log in to SL1.

To create an SSO authentication resource:

1. Go to the **Authentication Resource Manager** page (System > Settings > Authentication > Resources).
2. Click the **[Actions]** menu and then select *Create SSO Resource*. The **SSO Auth Resource Editor** page appears.



3. Enter values in the following fields:

Basic Settings

- ***Name***. Name of the SSO authentication resource.
- ***IdP Entity ID***. Globally unique name for the identity provider or service provider, in the format of an absolute URL.
- ***IdP Cert Fingerprint***. The SHA1 certificate fingerprint, provided by the identity provider or service provider.
- ***User Name Suffix***. Optional field. Because a user can authenticate against multiple SSO servers, there is a risk of collision among user names. In this field, you can enter a string to append to the ScienceLogic user name to minimize risk of collision. For example:
  - Suppose we entered ***@ad.local*** in this field.
  - Suppose the next LDAP/AD user logs in to SL1 with the user name ***bishopbrennan***.
  - SL1 will log in that user as ***bishopbrennan@ad.local***.

NOTE: A best practice to avoid collisions is to use email addresses as user names.

- ***IdP SSO URL***. The URL to which SL1 will send login requests to the IdP. This field must contain an absolute URL.
- ***IdP SLS URL***. Optional field. If you want each user to be automatically logged out of the IdP when that user logs out of SL1, enter the URL to which SL1 will post the logout request to the IdP. If you leave this field blank, a user can log out of SL1 without automatically logging out of the IdP.
- ***Sync directory values to EM7 on login***. If an SSO administrator makes changes to an SSO account, SL1 will automatically retrieve those updates and apply them to the user's account in SL1 (in the **Account Properties** page) the next time the user logs in to SL1. (For more information about user account properties, see the ***Organizations & Users*** manual.)

Attribute Mapping

If you have configured SL1 to automatically create ScienceLogic accounts for SSO users, these fields specify the SAML attribute value that will be automatically inserted into each field in each user's **Account Properties** page. (For more information about user account properties, see the ***Organizations & Users*** manual.)

SL1 automatically populates as many of these fields as possible. You can edit or delete the default values provided by SL1. For example, SL1 automatically inserts the value of the SAML attribute "sn" (surname) into the ***Last Name*** field in each user's **Account Properties** page.

NOTE: SL1 requires that the SAML attribute name that you specify in each field uses all lowercase characters.

- ***First Name***. Specifies the SAML attribute value that will be automatically inserted into the ***First Name*** field in each user's **Account Properties** page. By default, SL1 inserts the value of the SAML attribute "givenname" into this field.
- ***Last Name***. Specifies the SAML attribute value that will be automatically inserted into the ***Last Name*** field in each user's **Account Properties** page. By default, SL1 inserts the value of the SAML attribute "sn" into this field.
- ***Title***. Specifies the SAML attribute value that will be automatically inserted into the ***Title*** field in each user's **Account Properties** page.
- ***Department***. Specifies the SAML attribute value that will be automatically inserted into the ***Department*** field in each user's **Account Properties** page.
- ***Phone***. Specifies the SAML attribute value that will be automatically inserted into the ***Phone*** field in each user's **Account Properties** page. By default, SL1 inserts the value of the SAML attribute "telephonenumber" into this field.
- ***Fax***. Specifies the SAML attribute value that will be automatically inserted into the ***Fax*** field in each user's **Account Properties** page.
- ***Mobile***. Specifies the SAML attribute value that will be automatically inserted into the ***Mobile*** field in each user's **Account Properties** page. By default, SL1inserts the value of the SAML attribute "mobile" into this field.
- ***Pager***. Specifies the SAML attribute value that will be automatically inserted into the ***Pager*** field in each user's **Account Properties** page.
- ***Primary Email***. Specifies the SAML attribute value that will be automatically inserted into the ***Primary Email*** field in each user's **Account Properties** page. By default, SL1 inserts the value of the SAML attribute "mail" into this field.
- ***Secondary Email***. Specifies the SAML attribute value that will be automatically inserted into the ***Secondary Email*** field in each user's **Account Properties** page.
- ***Street Address***. Specifies the SAML attribute value that will be automatically inserted into the ***Street Address*** field in each user's **Account Properties** page. By default, SL1 inserts the value of the SAML attribute "streetaddress" into this field.
- ***Suite/Building***. Specifies the SAML attribute value that will be automatically inserted into the ***Suite/Building*** field in each user's **Account Properties** page.
- ***City***. Specifies the SAML attribute value that will be automatically inserted into the ***City*** field in each user's **Account Properties** page. By default, SL1 inserts the value of the SAML attribute "l" into this field.

- ***State***. Specifies the SAML attribute value that will be automatically inserted into the ***State*** field in each user's **Account Properties** page. By default, SL1 inserts the value of the SAML attribute "st" into this field.
- ***Postal Code***. Specifies the SAML attribute value that will be automatically inserted into the ***Postal Code*** field in each user's **Account Properties** page. By default, SL1 inserts the value of the SAML attribute "postalcode" into this field.
- ***Country***. Specifies the SAML attribute value that will be automatically inserted into the ***Country*** field in each user's **Account Properties** page.
- ***Organization***. Specifies the SAML attribute value that will be used to automatically define the ***Primary Organization*** field in each user's **Account Permissions** page. You must also specify one of the following:
    - *directory attribute specifies organization ID*. The attribute in the ***Organization*** field specifies an organization ID.
    - *directory attribute specifies organization name*. The attribute in the ***Organization*** field specifies an organization name.
    - *directory attribute specifies organization CRM ID*. The attribute in the ***Organization*** field specifies the CRM ID of an organization.

NOTE: To use Attribute Mapping for ***Organization***, your SAML schema must include an attribute that maps to All-In-One Appliance Organization names, Organization IDs, or Organization CRM IDs.

NOTE: When you create a new SSO user, you must align a user policy with that user. If the aligned user policy specifies an organization for the user, the value from the user policy will overwrite the value from Attribute Mapping.

User Policy Alignment

- ***Type***. Specifies whether SL1 should automatically create ScienceLogic accounts for each SSO user, whether SL1 should simply use SSO to authenticate one or more users, or whether SL1 will refuse to authenticate specific users. Choices are:
    - *Do not authenticate new users*. Only those users who have an account already created in SL1 can log in to SL1, which will authenticate those users with SSO using the settings specified in this page.
    - *Static policy alignment*. If an SSO user tries to access SL1, SL1 will automatically create an account for that user. SL1 will use **one user policy** (specified in the ***Policy*** field) to create the imported SSO user accounts for this authentication resource. SL1 will also use the settings specified in this page when creating the account.

- *Dynamic policy alignment*. If an SSO users tries to access SL1, SL1 will automatically create an account for that user. SL1 will choose from among **multiple user policies** to create imported SSO user accounts for this authentication resource. For example, some imported user accounts might use "user policy A"; other imported user accounts might use "user policy B". SL1 will also use the settings specified in this page when creating the account.

NOTE: If you selected *Static policy alignment* in the ***Type*** field, you must supply a value in the ***Policy*** field.

- ***Policy***. Specifies the user policy to use to automatically create a ScienceLogic account for each SSO user. Select from a list of all user policies.

NOTE: If you selected *Dynamic policy alignment* in the ***Type*** field, you must supply values in the ***Attribute***, ***Value***, and ***Policy*** fields.

- ***Attribute***. Specifies the SAML attribute you want to use to differentiate imported user accounts. For example, you could select the attribute *department* and then assign different user policies to import user accounts from different departments. You can also use this field to exclude SSO accounts for which you **do not want to allow authentication**.
- ***Value***. Specifies the SAML attribute value. That is, you specify one of the possible values for the attribute (specified in the ***Attribute*** field). SL1 will compare the value in this field to the retrieved value for the ***Attribute***.
- ***Policy***. Choose one of the following:
  - *Do Not Authenticate*. If the retrieved value of the specified ***Attribute*** matches the value in the ***Value*** field, the user is not authenticated. This setting applies to new users for whom SSO would have to create a new account in SL1 and for users who already have an account in SL1.
  - *the policy you want to associate with that value*. Select from a list of all user policies that specify *SSO* in the ***Authentication Method*** field.
    - For example, suppose you specified *department* in the ***Attribute*** field. Suppose that the *department* attribute could have two possible values: *Sales* or *NOC*.
    - Suppose you created two user policies. One user policy, called *Sales User Policy*, includes the appropriate ticket queues and access keys for Sales personnel. Another user policy, called *NOC User Policy*, includes the appropriate ticket queues and access keys for NOC personnel.
    - In one of the ***Value*** fields, you could specify *Sales*. In the corresponding ***Policy*** field, you could then specify *Sales User Policy*.
    - You could then click on the plus-sign icon () and add another ***Value*** field and another ***Policy*** field.
    - In the next ***Value*** field, you could specify *NOC*. In the corresponding ***Policy*** field, you could specify *NOC User Policy*.

- After defining these two ***Value*** fields and the corresponding ***Policy*** fields, user accounts from the *Sales* department would be imported into SL1 using the *Sales User Policy*.
- User accounts from the *NOC* department would be imported into SL1 using the *NOC User Policy*.

- To define additional ***Value*** and ***Policy*** fields, click on the green plus-sign icon ( ).

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

Editing an Authentication Resource

The **Authentication Resource Manager** page allows you to edit an existing authentication resource. To do so:

1. Go to the **Authentication Resource Manager** page (System > Settings > Authentication > Resources).
2. Find the authentication resource that you want to edit. Click its wrench icon ( ).
   - For LDAP/AD Resources, the **LDAP/AD Auth Resource Editor** page appears. In this page, you can you can edit the values for one or more fields. For more information, see the *Creating an LDAP/AD Authentication Resource* section.
   - For SSO Resources, SSO Auth Resource Editor page appears. In this page, you can you can edit the values for one or more fields. For more information, see the *Creating an SSO Authentication Resource* section.
3. Click the **[Save]** button to save your changes to the authentication resource.

Deleting an Authentication Resource

The **Authentication Resource Manager** page allows you to delete one or more authentication resources from SL1. To do so:

1. Go to the **Authentication Resource Manager** page (System > Settings > Authentication > Resources).
2. Select the checkbox ( ) of each authentication resource that you want to delete.
3. Click the ***Select Actions*** menu (in the lower right), select *DELETE Authentication Resource*, and then click the **[Go]** button. The selected authentication resources will be deleted.

NOTE: You cannot delete the *EM7 Internal* authentication resource.

Chapter 13

Managing Host Files

Overview

The **Host File Entry Manager** page allows you to edit and manage host files for all of the Data Collectors from a single page in the SL1 system. When you create or edit an entry in the **Host File Entry Manager** page, SL1 automatically sends an update to every Data Collector in the specified Collector Group.

The **Host File Entry Manager** page is helpful when:

- The SL1 system does not reside in the end-customer's domain
- The SL1 system does not have line-of-sight to an end-customer's DNS service
- A customer's DNS service cannot resolve a host name for a device that the SL1 system monitors

You can create host file entries for each device managed by the SL1 system. You can create duplicate host file entries, one for each Collection Group, to ensure that all Collection Groups can resolve all host names for monitored devices.

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

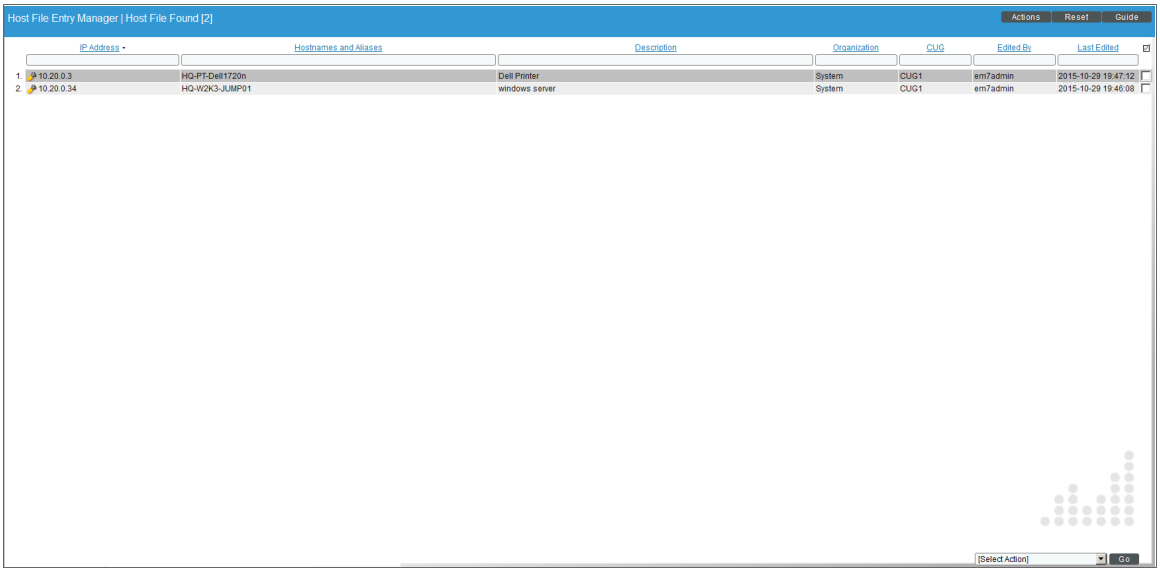
- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon ( ).

This chapter includes the following topics:

Viewing the List of Host Entries

To view the list of host entries, perform the following steps:

1. Go to the **Host File Entry Manager** page (System > Customize > Host Files).



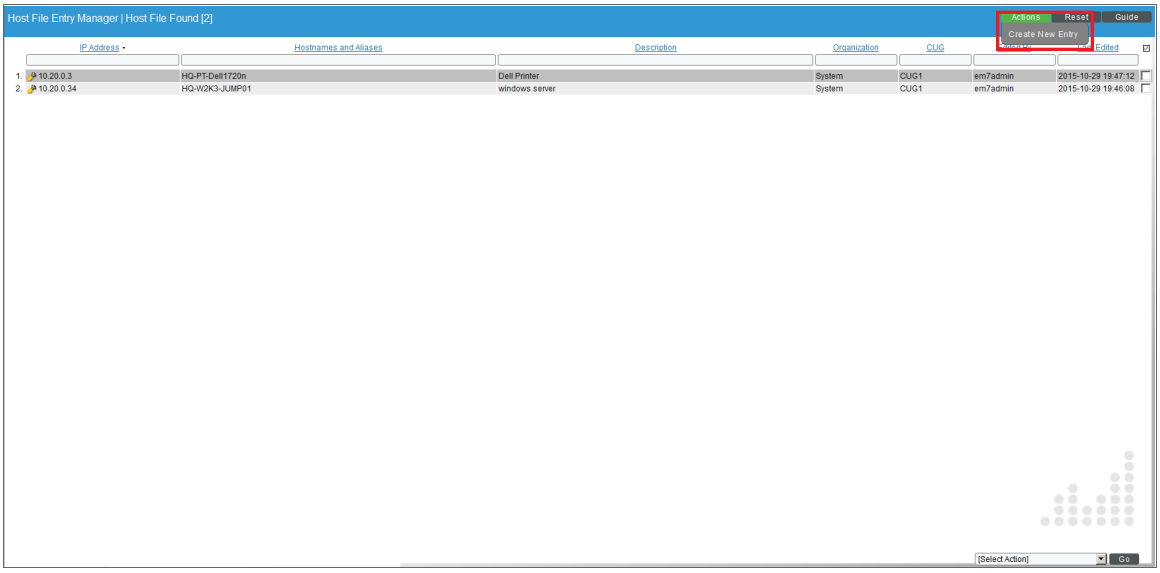
2. The **Host File Entry Manager** page displays the following about each host entry:

   - ***IP Address***. The IP address to resolve with the host name.
   - ***Hostnames and Aliases***. The host name to align with the specified IP address. You can also include a space-delimited list of aliases for the host name.
   - ***Description***. Description of the host entry.
   - ***Organization***. Organization associated with the host.
   - ***CUG***. The Collector Group to which SL1 will send the host entry. The host entry will be added to the host file on each Data Collection Server in the Collector Group.
   - ***Edited By*** . User who created or last edited the host entry.
   - ***Last Edit***. Date the host entry was created or last edited.

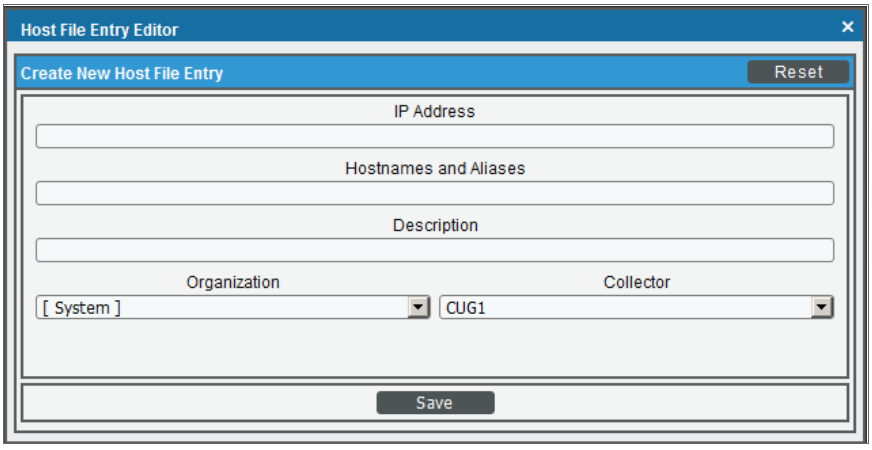
Creating a New Host Entry

To create a host file entry:

1. Go to the **Host File Entry Manager** page (System > Customize > Host Files).



2. Click the **[Action]** menu and choose ***Create New Entry***. The **Create New Host File Entry** modal page appears.



3. In the **Create New Host File Entry** modal page, supply values in the following fields:

   - ***IP Address***. The IP address to resolve with the hostname.

NOTE: Server hostnames should be aligned to external IP addresses when supporting Network Address Translation (NAT) environments.

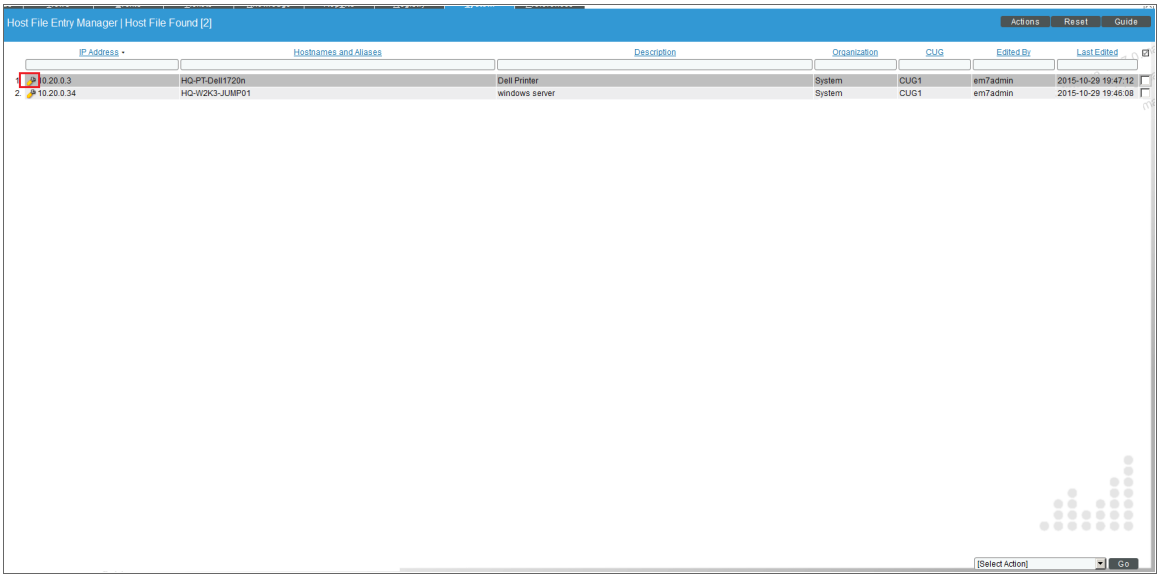
- ***Hostnames and Aliases***. The hostname to align with the specified IP address. You can also include a space-delimited list of aliases for the host name.
- ***Description***. Description of the host entry. This field is not written to the host file. This field is for administrators to use when managing host file entries.
- ***Organization***. Organization associated with the host. You can select from a list of all existing organizations. This field is not written to the host file. This field is for administrators to use when managing host file entries. For example, a service provider could assign each customer its own organization and then use this field to manage host file entries for each customer.

4. Click the **[Save]** button to save the new host entry.

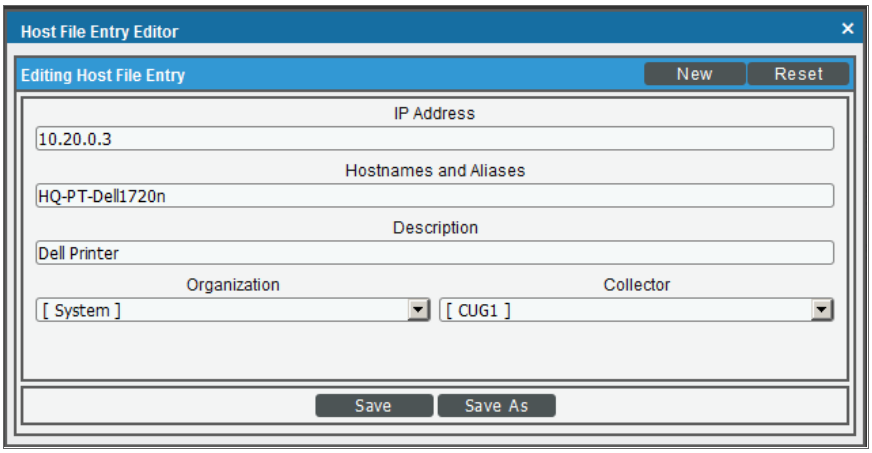
Editing a Host Entry

To edit a host entry, perform the following steps:

1. Go to the **Host File Entry Manager** page (System > Customize > Host Files).



2. Click the wrench icon ( ) for the host file entry you want to edit. The **Editing Host File Entry** modal page appears, populated with values from the selected host file entry.



3. In the **Editing Host File Entry** modal page, you can edit one or more of the following fields:

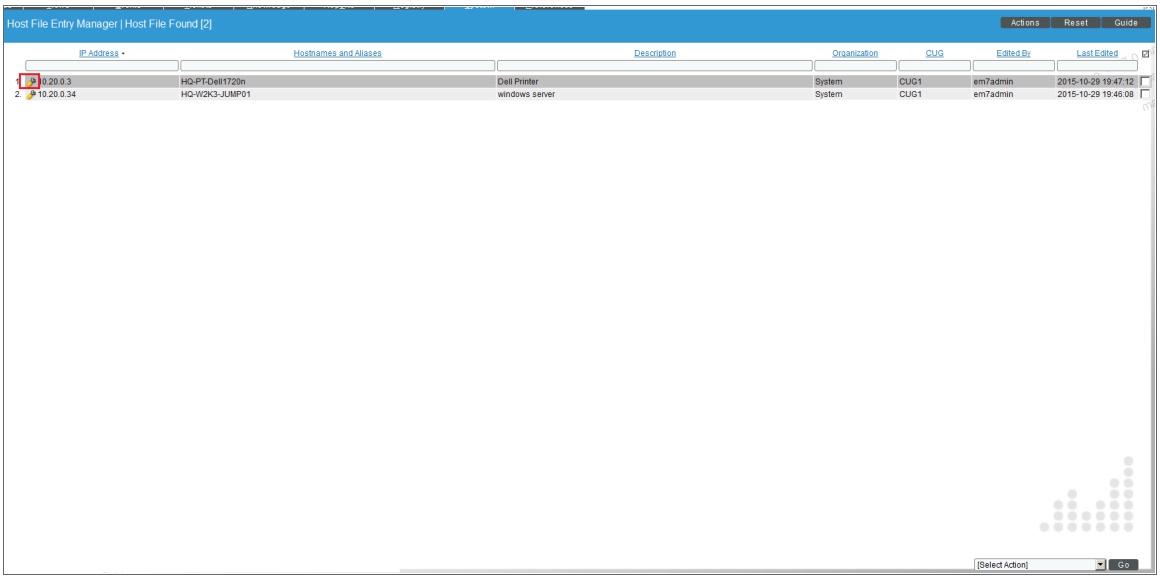
   - ***IP Address***. The IP address to resolve with the host name.
   - ***Hostnames and Aliases***. The host name to align with the specified IP address. You can also include a space-delimited list of aliases for the host name.
   - ***Description***. Description of the host entry. This field is not written to the host file. This field is for administrators to use when managing host file entries.
   - ***Organization***. Organization associated with the host. You can select from a list of all existing organizations. This field is not written to the host file. This field is for administrators to use when managing host file entries. For example, a service provider could assign each customer its own organization and then use this field to manage host file entries for each customer.

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

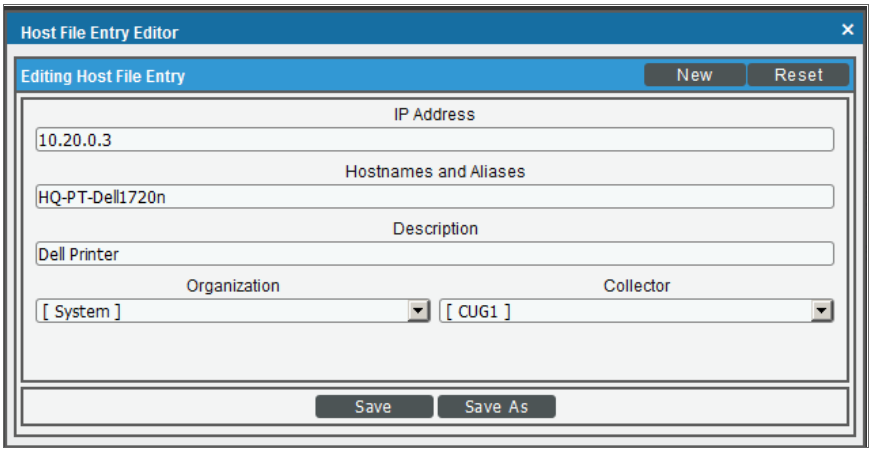
Using an Existing Host File Entry to Create a New Host File Entry (Save As)

To create a new host entry, using an existing host entry as the template:

1. Go to the **Host File Entry Manager** page (System > Customize > Host Files).



2. Click the wrench icon ( ) for the host file entry you want to edit. The **Editing Host File Entry** modal page appears, populated with values from the selected host file entry.



3. In the **Editing Host File Entry** modal page , you can edit one or more of the following fields:

   - ***IP Address***. The IP address to resolve with the host name.

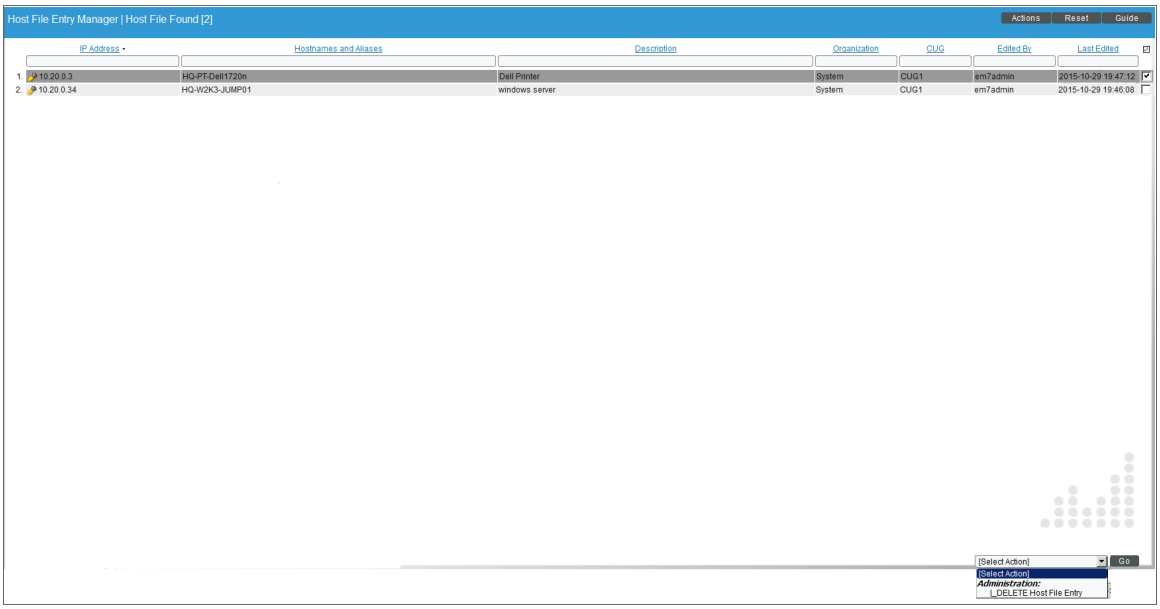
- ***Hostnames and Aliases***. The host name to align with the specified IP address. You can also include a space-delimited list of aliases for the host name.
- ***Description***. Description of the host entry. This field is not written to the host file. This field is for administrators to use when managing host file entries.
- ***Organization***. Organization associated with the host. You can select from a list of all existing organizations. This field is not written to the host file. This field is for administrators to use when managing host file entries. For example, a service provider could assign each customer its own organization and then use this field to manage host file entries for each customer.

4. Click the **[Save As]** button to save your changes as a new host file entry. A pop-up message appears, asking if you want to save your edits as a new entry. Click the **[OK]** button.

Deleting One or More Host Entries

To delete one or more host entries, perform the following steps:

1. Go to the **Host File Entry Manager** page (System > Customize > Host Files).



2. Select the checkbox (☐) for each host file entry you want to delete.
3. Click the ***Select Action*** field in the lower right, then select *DELETE Host File Entry*. Click the **[Go]** button.

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