STORMSHIELD

GUIDE

STORMSHIELD LOG SUPERVISOR

SYSTEM CONFIGURATION GUIDE

Version 2

Document last updated: July 4, 2024

Reference: sls-en_system_configuration_gde

Table of contents

Change log

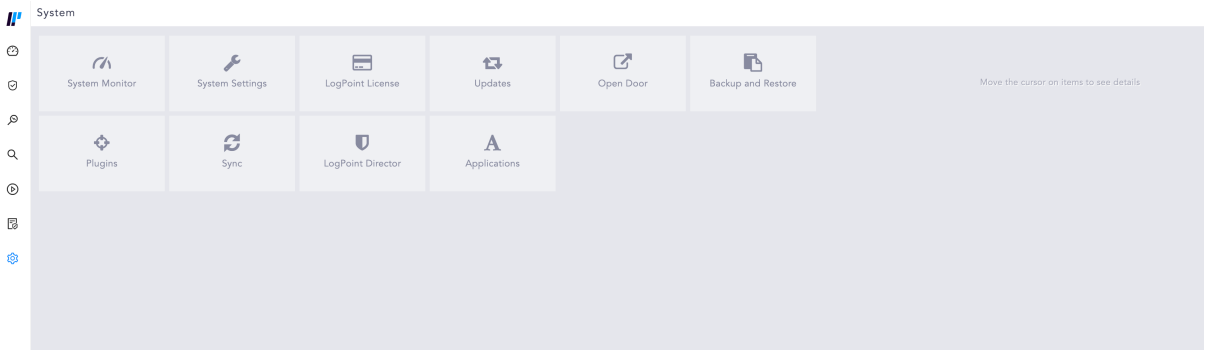
Date	Description
July 4, 2024	New document

Getting started

Welcome to the SLS version 2 System Configuration Guide.

System Configuration incorporates all the system-related processes to configure SLS. You can use **System Settings** to configure settings and make changes in the functional operation of the system. You can monitor the resources used by the SLS using the **System Monitor**. **System Notifications** enables you to configure Disk, CPU, and Memory Notifications.

Using **Export Management**, you can export raw logs to a remote target. **Sync** setting item allows you to synchronize configurations between SLSs. You can also customize general settings, search-related settings, date/time settings, notification settings, and change the system password from the **My Preferences** section.



This guide helps you to understand and perform the following tasks:

- Configure SMTP to send e-mails from the SLS.
- Update the settings under the **General** tab.
- Synchronize the system time with network timeserver.
- Secure the server connection to access SLS from the Internet.
- Create an encrypted end-to-end communication channel between the **SLS** and the **SLS** support.
- Operate SLS as a **SLS Collector**.
- Operate SLS as a **Syslog Forwarder**.
- Get notified about the total disk usage by the SLS file systems.
- Get notified about the CPU usage.
- Get notified about the Memory usage.
- Add a target to export raw logs from the **Search** results.
- Replicate the configurations in other SLS(s).

In this document, Stormshield Log Supervisor is referred to in its short form SLS. Images used in this document are from the partner vendor's (Logpoint) software program. In your SLS, the graphics may vary but user experience is exactly the same.

System Monitor

System monitor tracks what programs are running, how resources are used, and system status information. It also regularly tests services meant to be running and automatically generates alerts for problems so you can address them quickly.

Go to `Settings >> System Settings` from the navigation bar and click **System Monitor**.

Services

It lists all running services and their status. You can stop, start, or restart them if you need to.

Starting Services

Click the **Start Service** icon from **Actions**.

To start all the services, click **Start All**.

Stopping Services

Click the **Stop Service** icon from **Actions**.

To stop all the services, click **Stop All**.

Restarting Services

Click the **Restart Service** icon from **Actions**.

To restart all the services, click **Restart All**.

System Processes

It shows all the processes currently running on the operating system where SLS is installed. The process list shows users, memory used by processes, commands on run, and process ids.

You can reload the page by clicking **Reload**.

Network Stack

The **Network Stacks** are used in communication networks.

Routing Table

Displays the routes to particular network destinations.

Address Resolution Protocol (ARP) Table

A protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. This item data lists all the connection status under this protocol.

Network Interface

Displays SLS's network status. It shows the state of all active interfaces such as eth0, lO, he-ipv6, tun0, tun1 and tun10000.

Disk Usage

Displays the total file system disk usage. It lists available disk space, disk usage and location of the file system. SLS generates disk notifications when disk usage reaches 80% and again when the disk usage reaches 90%.

When available disk space falls to less than 2 GB, SLS stops collecting or fetching any logs and resumes only when there is at least 4 GB of available space. When the available space for a partition containing a repo path is less than 250 MB, SLS stops storing log messages in that partition and generates an audit log specifying that there is insufficient disk space available to store logs. SLS resumes data storage when enough space is available.

SNMP Monitoring

In addition to the SLS UI, you can also monitor the status of your SLS using **SNMP walk**. Use the base OID **1.3.6.1.4.1.54322.1** with the provided community string to get a list of all the exposed OIDs and their corresponding details.

> **NOTE**
> You can also use **enterprises.54322.1** as the base OID.

Syntax to monitor SLS using SNMP walk:

```
snmpwalk -v2c -c <Community String> <IP address of SLS>:161 <OID>
```

SLS exposes the following OIDs:

SN	OID	Information
1	1.3.6.1.4.1.54322.1.1	Last recorded messages per second in the normalizer
2	1.3.6.1.4.1.54322.1.2	Average messages per second in the last 5 minutes in the normalizer
3	1.3.6.1.4.1.54322.1.3	Last recorded messages per second in the store handler
4	1.3.6.1.4.1.54322.1.4	Average messages per second in the last 5 minutes in the store handler
5	1.3.6.1.4.1.54322.1.5	Services that are currently down
6	1.3.6.1.4.1.54322.1.6	SLS version
7	1.3.6.1.4.1.54322.1.7	Status of the log collection services

SN	OID	Information
8	1.3.6.1.4.1.54322.1.7.1	CPU consumption in collection (in %)
9	1.3.6.1.4.1.54322.1.7.2	Memory consumption in collection (in %)
10	1.3.6.1.4.1.54322.1.7.3	Queue in collection (in MB)
11	1.3.6.1.4.1.54322.1.8	Status of the normalization services
12	1.3.6.1.4.1.54322.1.8.1	CPU consumption in normalization (in %)
13	1.3.6.1.4.1.54322.1.8.2	Memory consumption in normalization (in %)
14	1.3.6.1.4.1.54322.1.8.3	Queue in normalization (in MB)
15	1.3.6.1.4.1.54322.1.9	Status of enrichment services
16	1.3.6.1.4.1.54322.1.9.1	CPU consumption in enrichment (in %)
17	1.3.6.1.4.1.54322.1.9.2	Memory consumption in enrichment (in %)
18	1.3.6.1.4.1.54322.1.9.3	Queue in enrichment (in MB)
19	1.3.6.1.4.1.54322.1.10	Status of indexing services
20	1.3.6.1.4.1.54322.1.10.1	CPU consumption in indexing (in %)
21	1.3.6.1.4.1.54322.1.10.2	Memory consumption in indexing (in %)
22	1.3.6.1.4.1.54322.1.10.3	Queue in indexing (in MB)
23	1.3.6.1.4.1.54322.1.11	Status of the dashboard and alerting service
24	1.3.6.1.4.1.54322.1.11.1	CPU consumption for dashboards and alerts (in %)
25	1.3.6.1.4.1.54322.1.11.2	Memory consumption for dashboards and alerts (in %)
26	1.3.6.1.4.1.54322.1.11.4	Disk usage by dashboards and alerts
27	1.3.6.1.4.1.54322.1.11.5	Number of active search processes (live searches)
28	1.3.6.1.4.1.54322.1.12	ZFS pool statistics
29	1.3.6.1.4.1.54322.1.12.1	Names of the ZFS pools
30	1.3.6.1.4.1.54322.1.12.2	Status of the ZFS pools
31	1.3.6.1.4.1.54322.1.12.3	Disk allocation for the ZFS pools
32	1.3.6.1.4.1.54322.1.12.4	Free disk space in the ZFS pools
33	1.3.6.1.4.1.54322.1.12.5	Read operations in the ZFS pools
34	1.3.6.1.4.1.54322.1.12.6	Write operations in the ZFS pools
35	1.3.6.1.4.1.54322.1.12.7	Read bandwidth in the ZFS pools
36	1.3.6.1.4.1.54322.1.12.8	Write bandwidth in the ZFS pools
37	1.3.6.1.4.1.54322.1.12.9	Failed disks in the pools (if any)
38	1.3.6.1.4.1.54322.1.13	Statistics for the log size in repos

SN	OID	Information
39	1.3.6.1.4.1.54322.1.13.1	Names of the repos
40	1.3.6.1.4.1.54322.1.13.2	Log size of repos in the previous day
41	1.3.6.1.4.1.54322.1.13.3	Log size of repos in the previous month
42	1.3.6.1.4.1.54322.1.14	Status of LUNs in systems with multipath devices
43	1.3.6.1.4.1.54322.1.14.1	Name of the multipath
44	1.3.6.1.4.1.54322.1.14.2	UUID of the multipath
45	1.3.6.1.4.1.54322.1.14.3	SysFS device-mapper's blocked device name of the multipath
46	1.3.6.1.4.1.54322.1.14.4	Device vendor/product/revision information
47	1.3.6.1.4.1.54322.1.14.5	Total number of detected paths of the multipath
48	1.3.6.1.4.1.54322.1.14.6	Total active paths of the multipath
49	1.3.6.1.4.1.54322.1.14.7	Product information
50	1.3.6.1.4.1.54322.1.14.8	Status of the multipath
51	1.3.6.1.4.1.54322.1.14.9	Size of the multipath
52	1.3.6.1.4.1.54322.1.14.10	Automatic failback configuration of the multipath
53	1.3.6.1.4.1.54322.1.30	Status of the SLS Collector buffer
54	1.3.6.1.4.1.54322.1.30.1	The logs in the buffer not received by the main SLS
55	1.3.6.1.4.1.54322.1.30.2	The time (in seconds) since the last message was received by the main SLS

NOTE
The OIDs for **ZFS pool statistics**, **statistics for the log size in repos**, and **LUN status** provide information for **all** these entities. To retrieve the information for a single one, add an extra number corresponding to the respective pool, repo, or LUN after the provided OID.
For example, you can use **enterprises.54322.1.12.1** to retrieve the names of all the ZFS pools and **enterprises.54322.1.12.1.1** to retrieve the name of the first ZFS pool.

Additionally, you can use the following default OIDs for a Linux-based system:

General Statistics

SN	OID	Information
1	1.3.6.1.4.1.2021.11	CPU and swap information
2	1.3.6.1.2.1.2.2.1	Network interfaces information
3	1.3.6.1.2.1.25.2.3.1.6.2	Disk usage information
4	1.3.6.1.2.1.25.1.1.0	Uptime information

CPU load

SN	OID	Information
1	1.3.6.1.4.1.2021.10.1.3.1	CPU load over the last minute
2	1.3.6.1.4.1.2021.10.1.3.2	CPU load over the last 5 minutes
3	1.3.6.1.4.1.2021.10.1.3.3	CPU load over the last 15 minutes
4	1.3.6.1.4.1.2021.11.9.0	Percentage of CPU time consumed by user
5	1.3.6.1.4.1.2021.11.50.0	Raw CPU time consumed by user
6	1.3.6.1.4.1.2021.11.10.0	Percentage of CPU time used by system
7	1.3.6.1.4.1.2021.11.52.0	Raw CPU time used by system
8	1.3.6.1.4.1.2021.11.11.0	Percentage of idle CPU time
9	1.3.6.1.4.1.2021.11.53.0	Raw idle CPU time
10	1.3.6.1.4.1.2021.11.51.0	Raw nice CPU time

Memory statistics

SN	OID	Information
1	1.3.6.1.4.1.2021.4.3.0	Total swap size
2	1.3.6.1.4.1.2021.4.4.0	Available swap space
3	1.3.6.1.4.1.2021.4.5.0	Total RAM in the machine
4	1.3.6.1.4.1.2021.4.6.0	Total RAM used
5	1.3.6.1.4.1.2021.4.11.0	Total free RAM
6	1.3.6.1.4.1.2021.4.13.0	Total shared RAM
7	1.3.6.1.4.1.2021.4.14.0	Total RAM buffered
8	1.3.6.1.4.1.2021.4.15.0	Total cached memory

Disk statistics

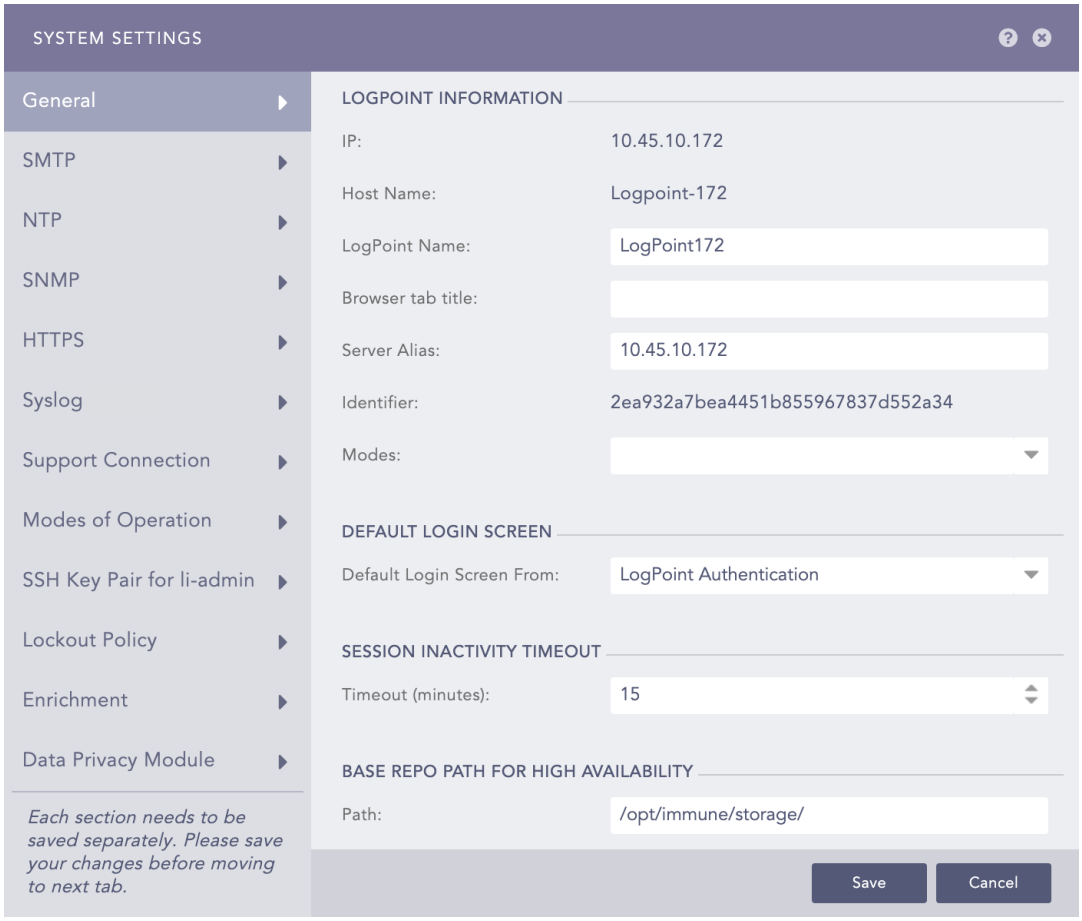
SN	OID	Information
1	1.3.6.1.4.1.2021.9.1.6.1	Total size of the disk or partition (in KB)
2	1.3.6.1.4.1.2021.9.1.7.1	Available space on the disk
3	1.3.6.1.4.1.2021.9.1.8.1	Used space on the disk
4	1.3.6.1.4.1.2021.9.1.9.1	Percentage of used space on the disk
5	1.3.6.1.4.1.2021.9.1.10.1	Percentage of inodes used on the disk
6	1.3.6.1.2.1.1.3.0	System uptime

System Settings

System Settings is used to configure all the system related settings.

General

1. Go to **Settings >> System Settings** from the navigation bar and click **System Settings**.
2. Select **General**.



3. Enter a **SLS Name**.
4. Enter a **Browser tab title**, this title is appended to the title of the tab.
5. Enter or update the **Server Alias**. Updating it does not update the system IP Address or the DNS.

> **NOTE**
> - **Identifier** is the unique value given to each SLS.
> - **Modes** contains the options *Search Head* and *Distributed SLS*. Selecting either of these options does not have any effect on SLS. The **Modes** field is made available for future implementation of the SLS Director (Director Console).

6. Select the **Default Login Screen** for the SLS.
7. In **Session Inactivity Timeout**, **Timeout (minutes)**, enter a specific period of time, in minutes, when SLS users are timed out.

8. Provide the **Base Repo Path for High Availability** to alter the default path **/opt/immune/storage/**. It is the base path for the repos from the remote machine.
9. Select either **Collection Timestamp (col_ts)** or **Log Timestamp (log_ts)** as per your requirement. The *col_ts* denotes the time when the log was collected in SLS, and the *log_ts* denotes the time when a device generated the log. The time conversion of **log_ts** occurs when a *Normalization Policy* is applied to the appropriate **Collectors/Fetchers**. Depending on the selection made in the *Apply Time Range On section*, either **log_ts** or **col_ts** value is displayed on the top of each row of the search results. Similarly, the time displayed in the search graph may either be **log_ts** or **col_ts** depending on the selection made.
10. Choose the **Over Scan Period (in minutes** and a **Time Zone**. The overscan period is the extra period (apart from the selected period) in which SLS searches for logs. Both the *col_ts* and the *log_ts* fields are saved in UTC and displayed according to the selected time zone.

> **NOTE**
> - Both the **log_ts** and **col_ts** key-value pairs are displayed in the search results.
> - The **Time Range** is applied either on the *col_ts* or the *log_ts* across all the distributed SLSs.

9. Select a **Time Zone**.
10. Select **Enable SOAR in SLS** to enable incident investigation with *Playbooks* and *Cases*.

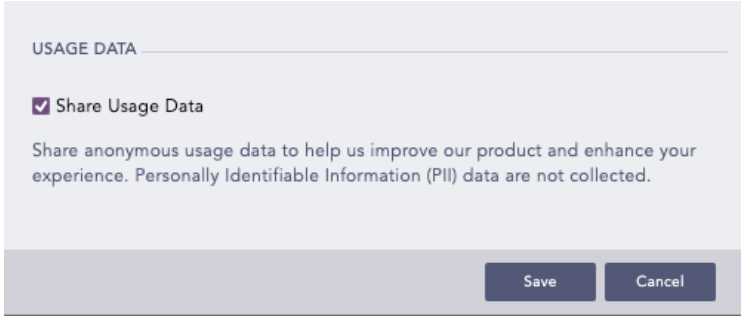
> **NOTE**
> - Enabling or disabling SOAR may take some time depending on available memory.
> - SOAR is always disabled in the SLS Collector and Syslog Forwarder modes.

12. Click **Save**.

Usage Data

SLS collects and analyzes anonymized usage data by default. However, it does not collect Personally Identifiable Information (PII) data. You can also not share usage data by deselecting Share Usage Data. To deselect:

1. Go to **Settings >> System Settings** from the navigation bar and click **System Settings**.
2. Select **General** and scroll down to Usage Data.
3. Deselect **Share Usage Data**. You can also later share data by selecting it.

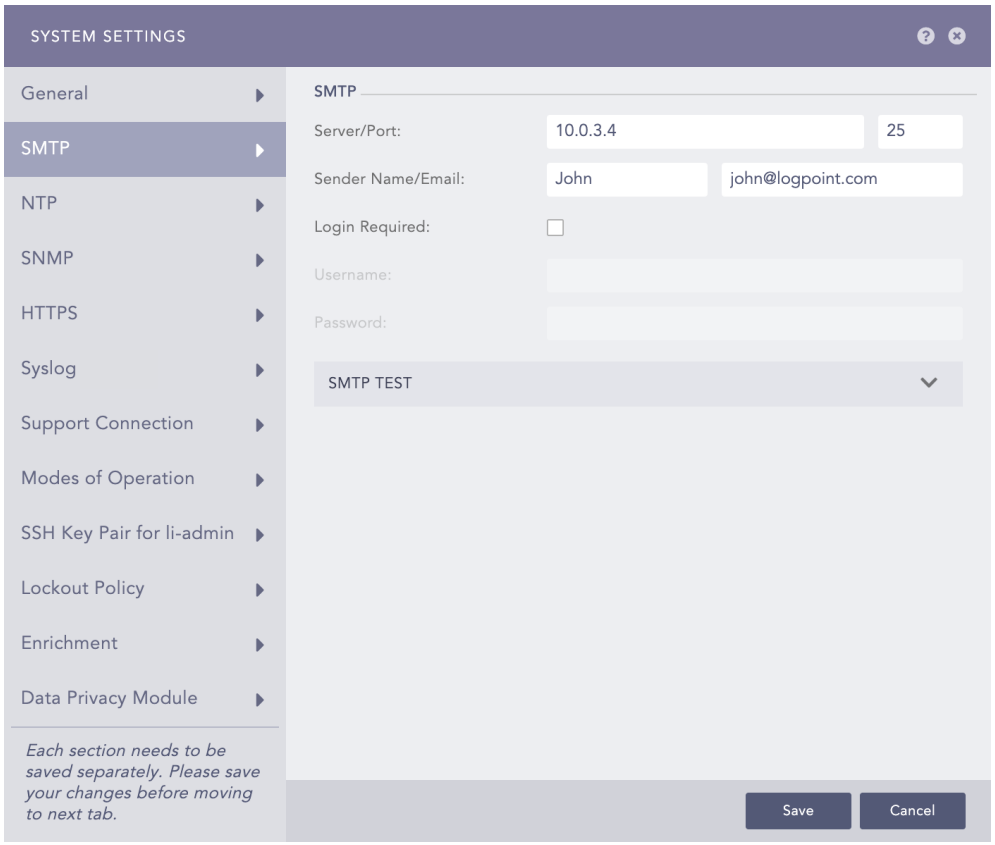


4. Click **Save**.

SMTP

You need to configure SMTP so the alert engine can use it to forward information and SLS can send e-mails. You will also need to configure SMTP before using the **Data Privacy Module**.

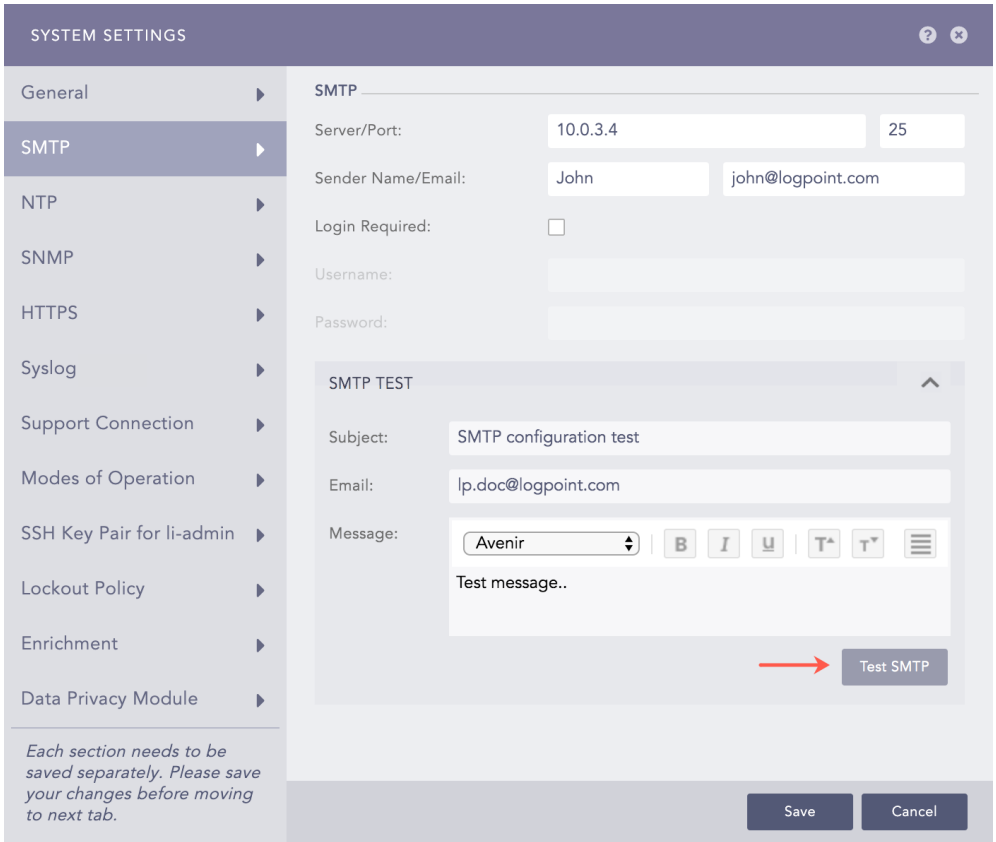
1. Go to **Settings >> System Settings** from the navigation bar and click **System Settings**.
2. Select **SMTP**.



3. Provide the **Server/Port**.
4. Provide a **Sender Name** and an **Email** address.
5. If you enable the **Login Required** option, provide the **Username** and the **Password**.
6. Click **Save**.

To test the configuration, go through the following steps:

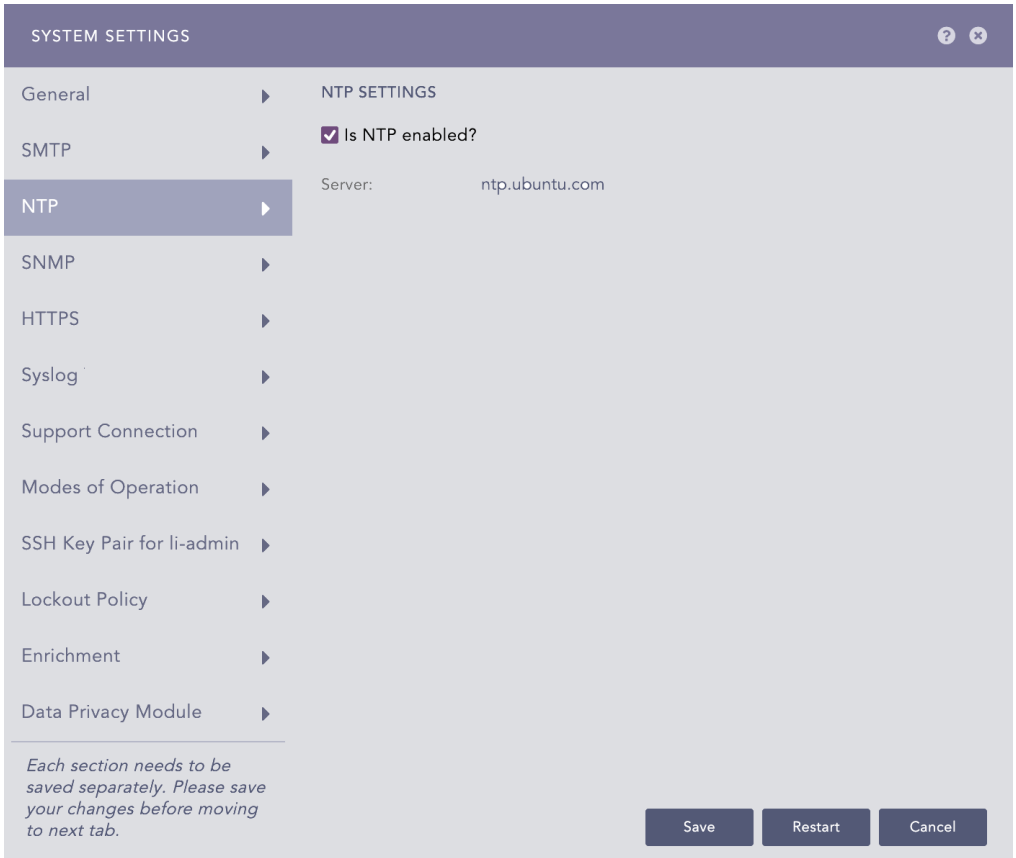
1. Click the **SMTP Test** section.
2. Enter the **Subject** of the test e-mail.
3. Provide an **Email** address.
4. Enter a **Message**.
5. Click **Test SMTP**.



NTP

NTP synchronizes the time of your SLS with a network timeserver.

1. Go to **Settings >> System Settings** from the navigation bar and click **System Settings**.
2. Select **NTP**.



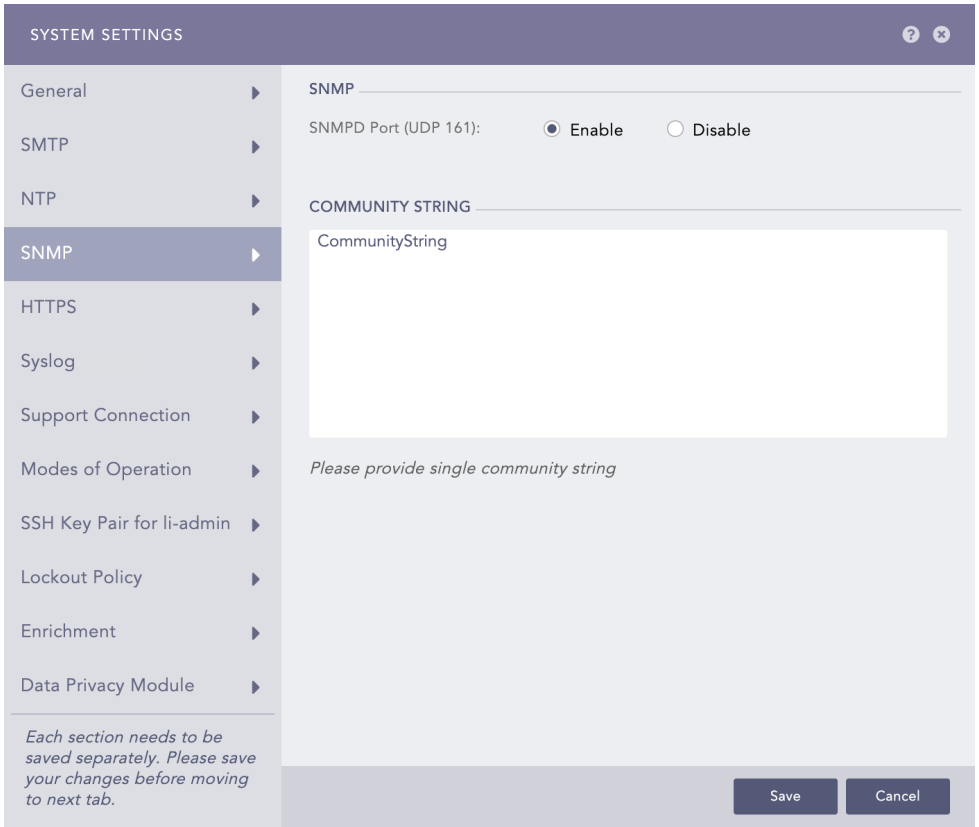
3. Select **Is NTP enable?**.
4. Provide the **Server** address. You can add multiple server addresses by clicking the plus icon.
5. Click **Save**.

SNMP

SNMP allows you to monitor various metrics of SLS. If you enable the **SNMP**, your SLS listens to the **OIDs** that are forwarded to the 161 port.

To enable SNMP:

1. Go to **Settings** >> **System Settings** from the navigation bar and click **System Settings**.
2. Select **SNMP**.



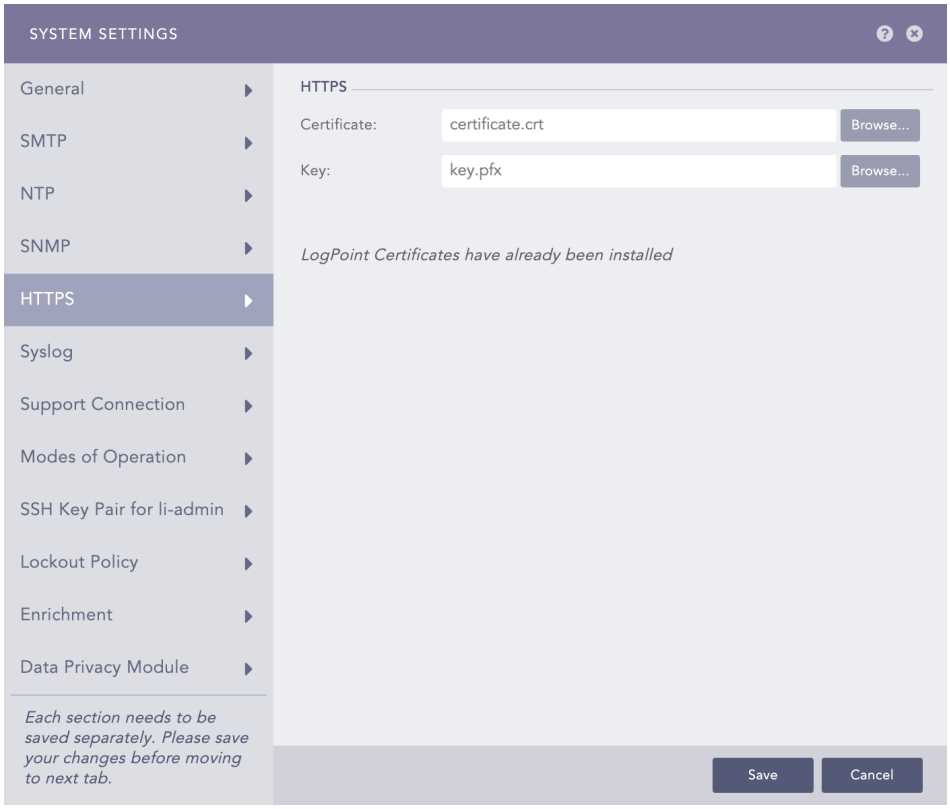
3. Select **Enable**.
4. Enter a **Community String**. The SNMP community string in SLS is a read-only community string that authenticates SLS. Use this community string in your SNMP clients to query SLS and retrieve information.
5. Click **Save**.

HTTPS

HTTPS authenticates SLS and prevents eavesdroppers from accessing the data in the network. **HTTPS** secures the server connection so SLS users can safely access SLS from the Internet.

You must have a certificate and a key to enable the HTTPS.

1. Go to **Settings >> System Settings** from the navigation bar and click **System Settings**.
2. Select **HTTPS**.

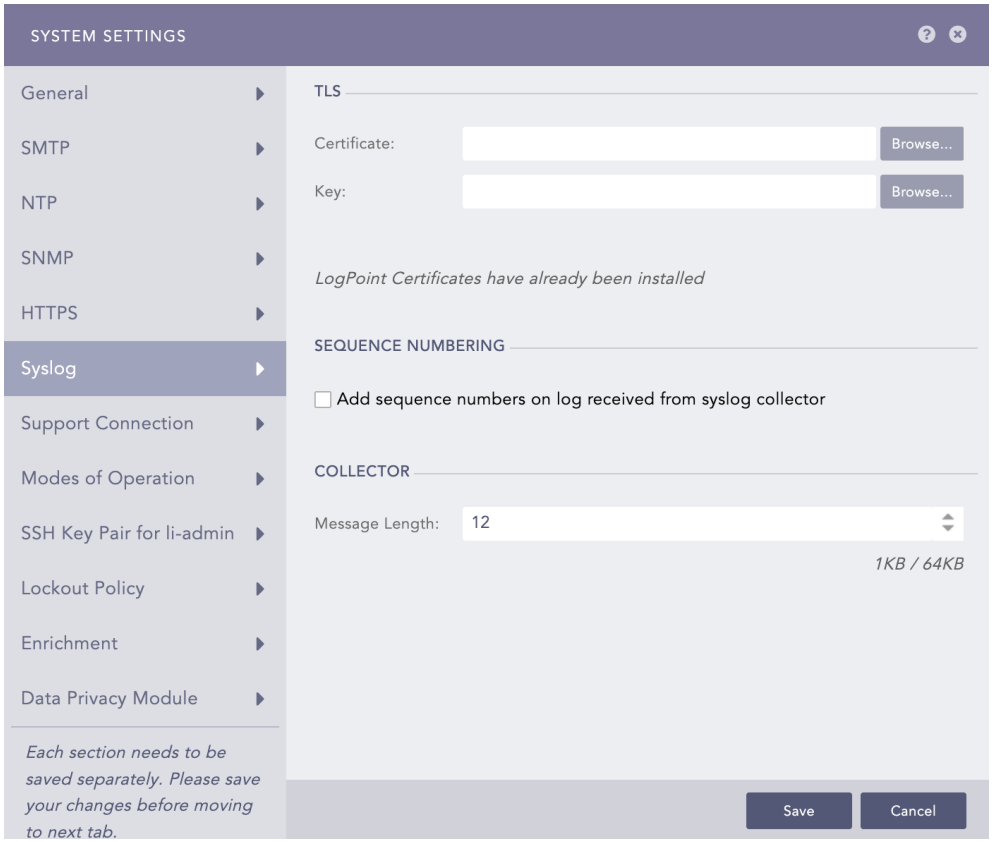


3. Click **Browse** to find and select the **Certificate**. The certificate file must have a .CRT extension and must meet the **PEM encoded x.509** standard. SLS certificates do not replace existing user certificates of 2048 bits.
4. Click **Browse** to find and select the **Key**. The key file must have a .Key extension.
5. Click **Save**.

Syslog

You can add a custom TLS certificate for log collection via Syslog. The added certificate is used by the Syslog collector to collect logs through TLS on port 6514.

1. Go to **Settings >> System Settings** from the navigation bar and click **System Settings**.
2. Select **Syslog**.



3. Upload your **TLS Certificate** and **Key**. The certificate must have the .crt extension and the key must have the .key extension. Only SLS Administrators can add a certificate and key. The certificate must be of **PEM encoded x.509** standard.
4. Enable **Add sequence numbers on log received from syslog collector** to provide a sequence number to the syslogs. The number is assigned on a device per protocol basis to each log collected from the **Syslog Collector**.
5. In **Message length**, you can define the size for Syslog messages. The maximum message size can be 64 KB, with a default size of 12 KB. Any message that exceeds the maximum size is divided into multiple events and truncated at the defined size. For example, if the message length is 40 KB, logs larger than that size are chunked into 40 KB segments.
6. Click **Save**.

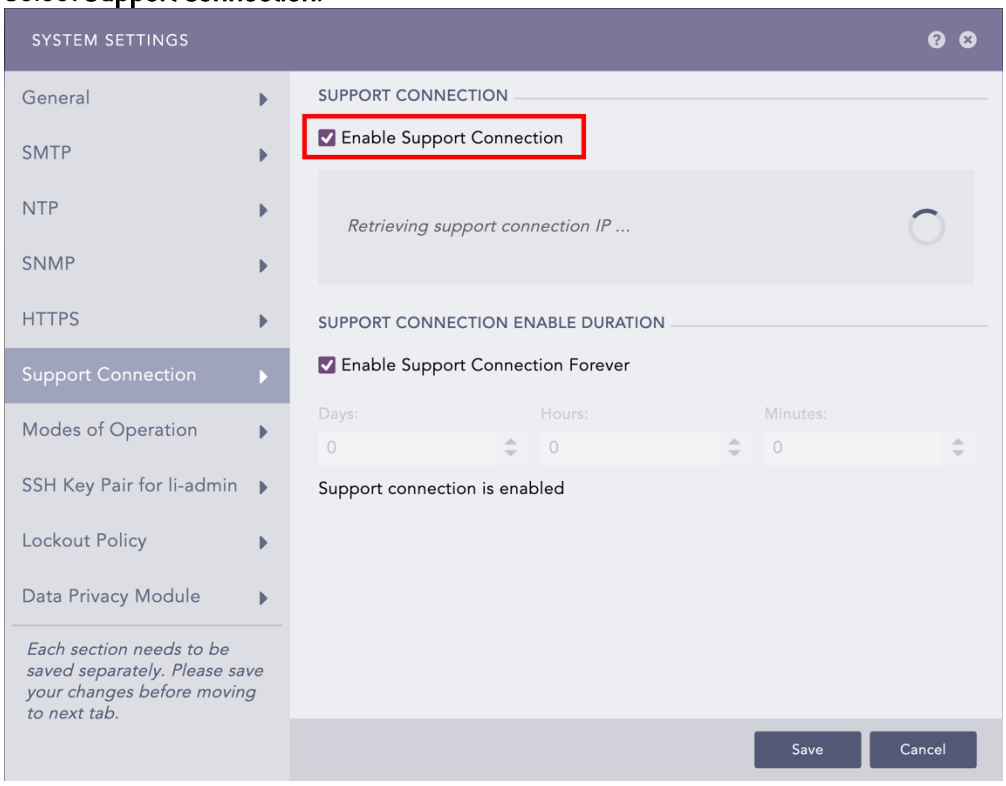
Support Connection

The **Support Connection** creates an encrypted end-to-end communication channel between **SLS** and **SLS** support. It is used by **SLS Support** to understand, troubleshoot, and fix the issues on your deployment issues.

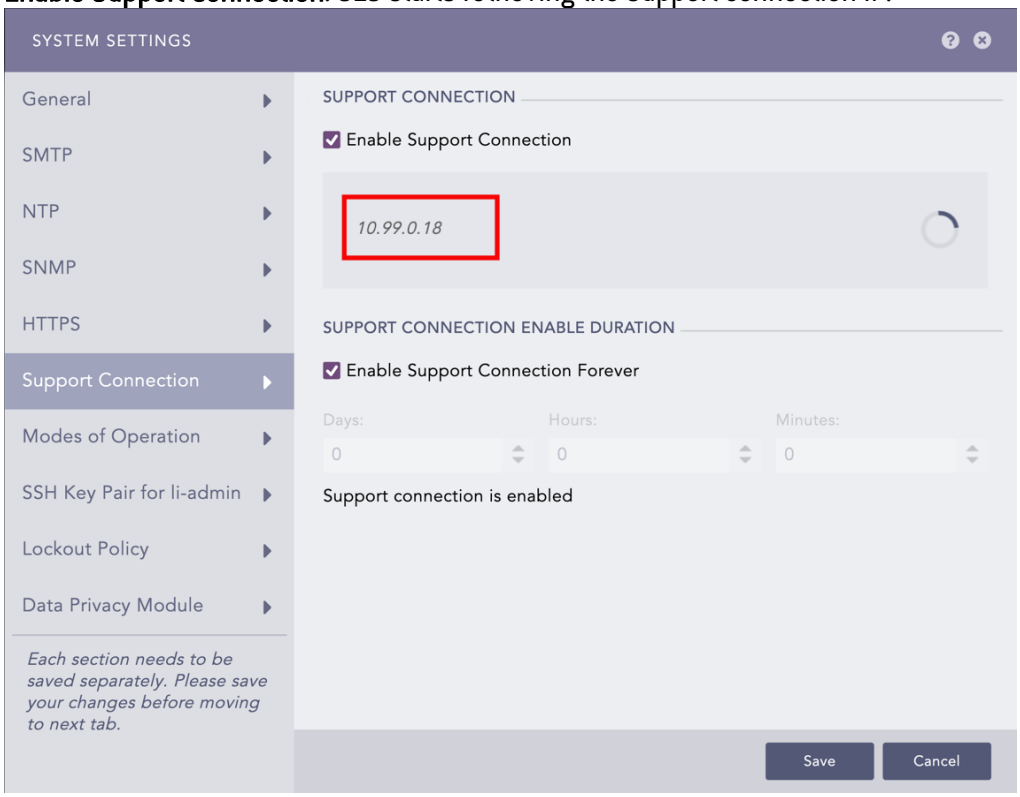
Before enabling support connection, make sure that your firewall is not blocking the connection from your SLS to the following:

Domain	Port
reverse.logpoint.com	1193/UDP
customer.logpoint.com	443/TCP

1. Go to **Settings >> System Settings** from the navigation bar and click **System Settings**.
2. Select **Support Connection**.



3. **Enable Support Connection**. SLS starts retrieving the support connection IP.



4. Provide the retrieved support connection IP to the SLS Support team.
5. Provide the **Support Connection Enable Duration**. The support session expires after it exceeds the duration.

> **NOTE**
> Support connection never expires if you select **0:0:0** as the time duration, or **Enable Support Connection Forever**.

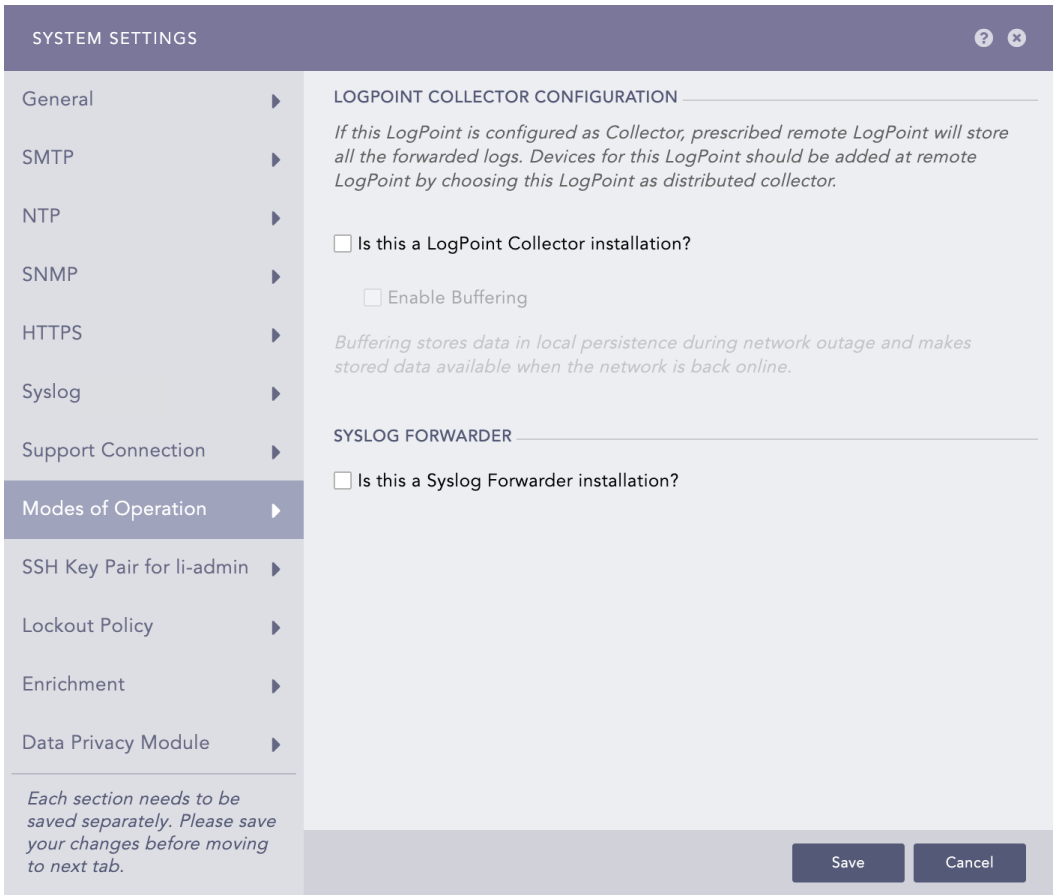
6. Click **Save**.

Modes of Operation

SLS can be operated in two modes using the **Modes of Operation**.

1. SLS Collector
2. Syslog Forwarder

You can convert a regular SLS into either a **SLS Collector** or a **Syslog Forwarder**.



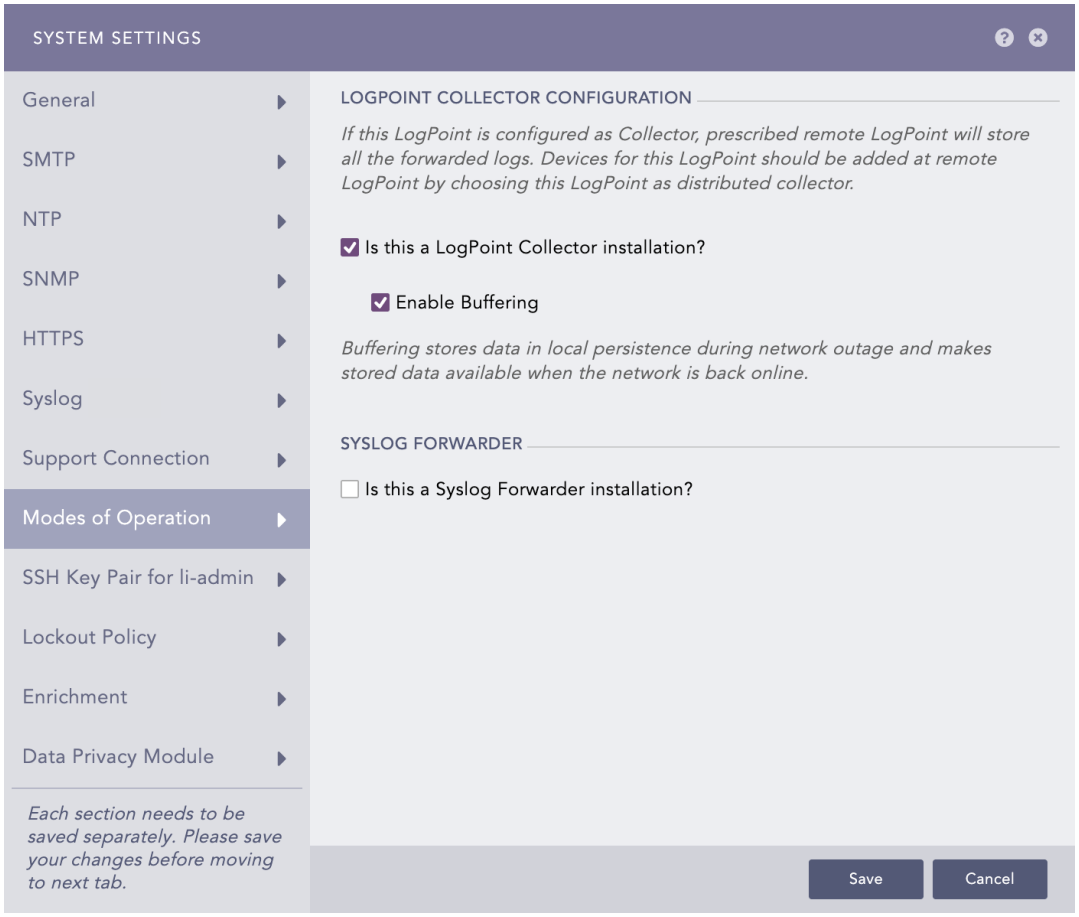
SLS Collector

SLS Collector collects logs from different sources, normalizes them using the signatures applied, and forwards them to a configured remote SLS. The remote SLS configures the sources and the storage locations for the logs. SLS Collector can only collect the logs. Therefore, it does not contain the *Dashboards*, the *Search*, the *Report*, and the *SLS SOAR* sections. The name of each SLS node must be unique in a distributed deployment.

Configuring a SLS to a SLS Collector

You need at least two SLS servers, one as the **Collector** and another as the **Main SLS**.

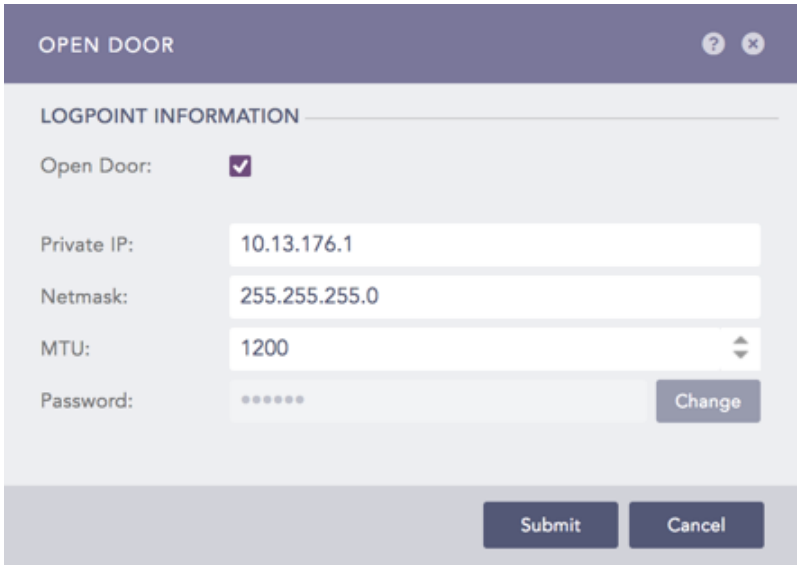
1. Go to **Settings >> System Settings** from the navigation bar and click **System Settings**.
2. Select **Modes of Operation**.



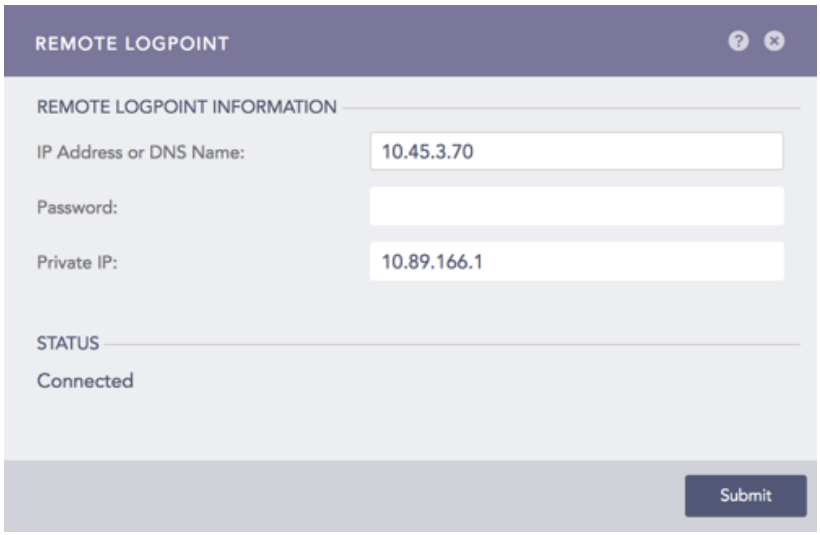
3. In **SLS Collector Configuration**, select **Is this a SLS Collector Installation?**.
4. Select **Enable Buffering** to store the data in local persistence during a network outage.

> **NOTE**
> By default, the logs are stored in the buffer for 7 days. If you want to change the default retention period, contact SLS Support.

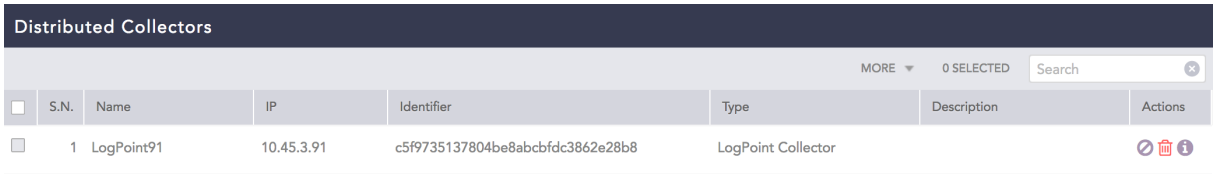
5. Click **Save**.
6. Switch to the **Main SLS**.
   6.1. Go to **Settings >> System Settings** from the navigation bar and click **Open Door**.
   6.2. Enable **Open Door**.
   6.3. Note the **Private IP** and the **Password**.



7. Switch to the **Collector SLS**.
   7.1. Go to **Settings** >> **Configuration** from the navigation bar and click **Remote SLS**.
   7.2. Enter the **IP Address** of the *Main SLS*, the **Password**, and the **Private IP**.



8. The **Collector** is automatically added under **Settings** >> **Configuration** from the navigation bar and click **Distributed Collector** in the **Main SLS**. Activate it from the *Actions* column.



Using a SLS Collector

You can use the **Collector** to collect logs by adding it as a device in the **Main SLS**.

1. In the **Main SLS**, go to **Settings** >> **Configuration** from the navigation bar and click **Devices**.
2. Click **Add**.
3. Specify the **Collector** as a **Distributed Collector**.
4. To verify the connection between the devices, switch to the **Collector SLS**.
   - Go to **View Devices**.

To distinguish logs collected and normalized through the **Collector**, you can use the system defined field, **collected_at** in the search query.

> **NOTE**
>
> - If you disable the **Collector**, make sure that you remove it from the list of devices on the **Main SLS**.
> - If you change the password on the **Collector** machine from **Settings >> Remote SLS**, all the services of the Collector restart. The logs are not collected until the *Collectors and Fetchers* are up and running.

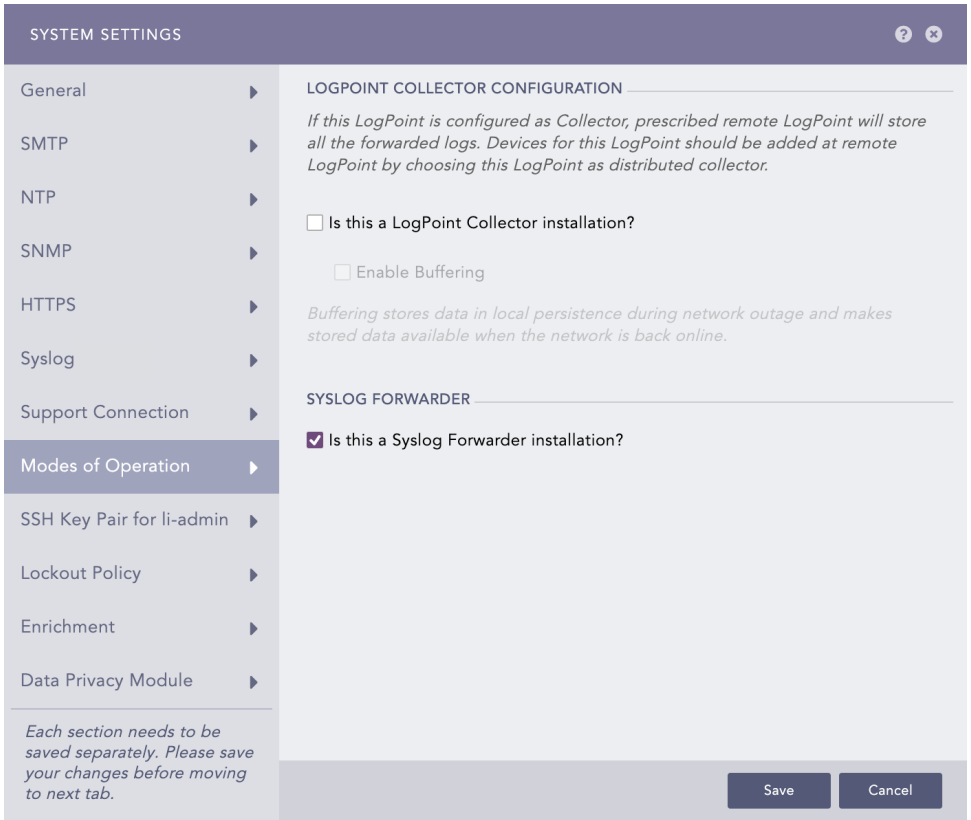
Syslog Forwarder

Syslog Forwarder collects logs from different sources, normalizes them using the signatures applied, and forwards them to a configured SLSs and a target storage. Unlike SLS Collectors, Syslog Forwarder can not act as a buffer.

Syslog Forwarder was implemented to introduce the concept of **Air Gap**. The **Main SLSs** are usually located in high-security zones whereas **Syslog Forwarders** and other devices are in low-security zones.

Converting a SLS to a Syslog Forwarder

1. Go to **Settings >> System settings** from the navigation bar and click **System Settings**.
2. Select **Modes of Operation**.
3. In **Syslog Forwarder**, select the **Is this a Syslog Forwarder installation?**.



4. Click **Save**.

Using a Syslog Forwarder

To use a Syslog Forwarder after converting it, you need to:

1. Exporting a config file
2. Importing the config file
3. Adding target
4. Adding devices

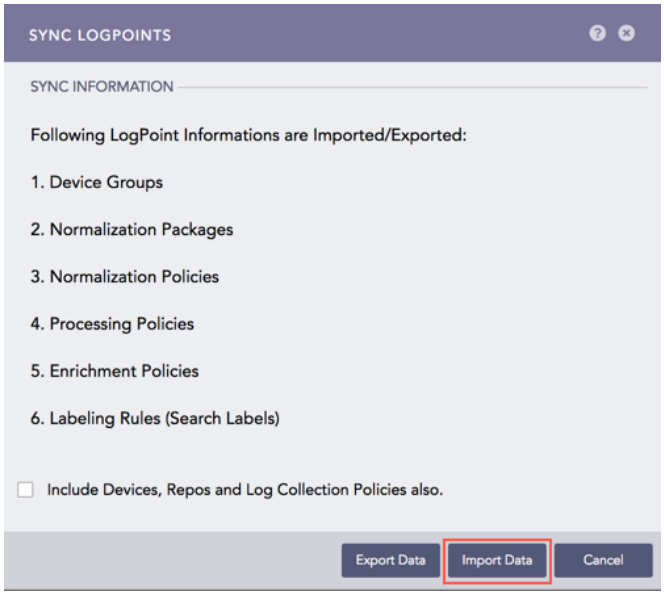
Exporting a config file

1. Switch to the **Main SLS** and go to **Settings** >> **Configuration** from the navigation bar and click **Distributed SLSs**.
2. Add a **Syslog Forwarder**.
3. Click the **Export configuration** icon in the *Actions* column of the concerned **Syslog Forwarder**.

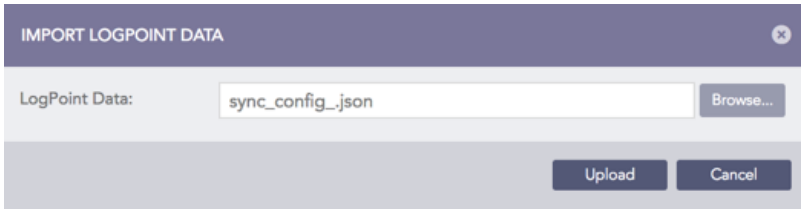
4. The config file is downloaded on your machine.
5. **Save** the config file.

Importing the config file

1. Switch to the **Syslog Forwarder** and go to **Settings** >> **System Settings** from the navigation bar and click **Sync**.



2. Click **Import Data**.



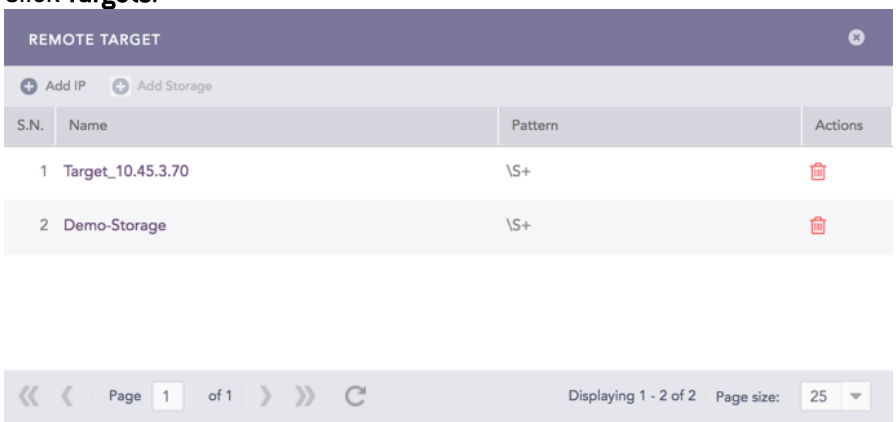
3. Browse for the config file saved earlier.
4. Click **Upload**.

Adding a Target

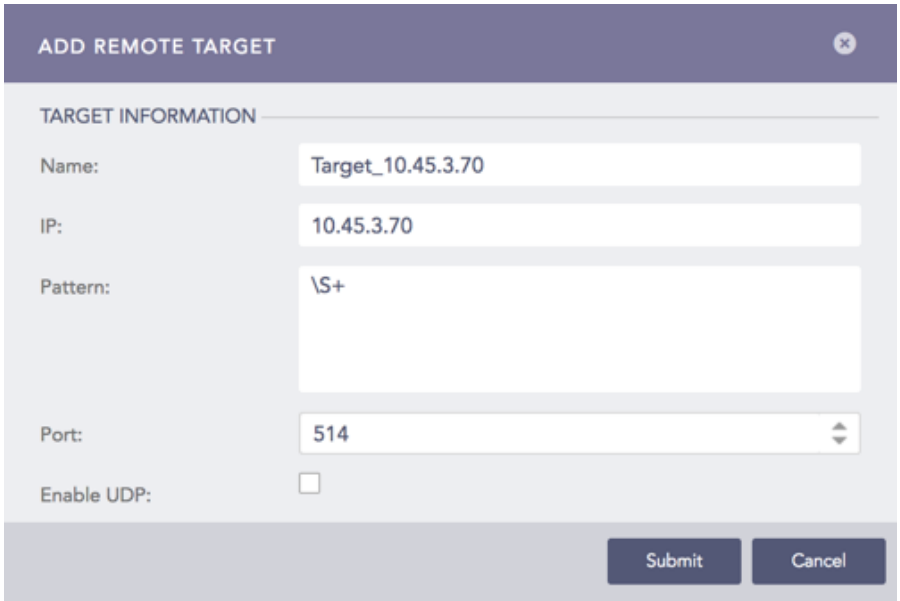
Targets are SLSs that receive logs from Syslog Forwarder.

1. On the **Syslog Forwarder**, go to **Settings** >> **Configuration** from the navigation bar and click **Syslog Forwarder**.

2. Click **Targets**.



3. Click **Add IP**.
4. Enter the **Name** and **IP** address of the target.
5. Specify the **Pattern** of the logs to be forwarded. If you do not specify a pattern, all the logs are forwarded.
6. Provide a **Port** number for the input port of the remote target machine.
7. Mark the **Enable UDP** checkbox to use the User Datagram Protocol (UDP). If you do not select the option, TCP is used.
   - If you *Enable UDP*, choose the **UDP Size (In Bytes)**.



8. Click **Submit**.

Adding a Target Storage

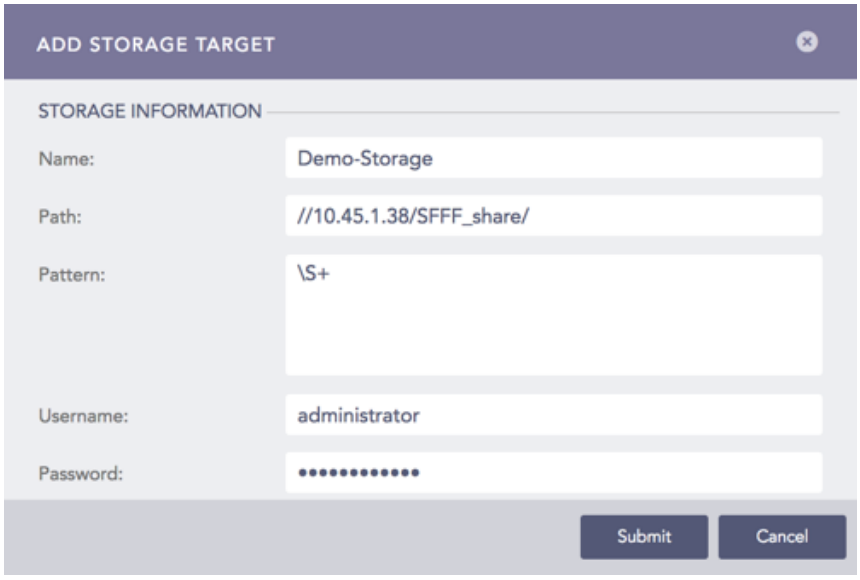
Target storage enables airgap in low-security zones.

1. On the **Syslog Forwarder**, go to **Settings >> Configuration** from the navigation bar and click **Syslog Forwarder**.
2. Click **Targets**. Click **Add Storage**.
3. Provide the **Name** of the storage.

4. Specify the **Path** to the remote storage. The format of the path should be:

   //<IP Address>/<Path>/
   For example: //192.168.2.247/storage/

5. Specify the **Pattern** of the logs to be forwarded. If you do not specify a pattern, all the logs are forwarded.
6. Provide the **Username** and the **Password**.



7. Click **Submit**.

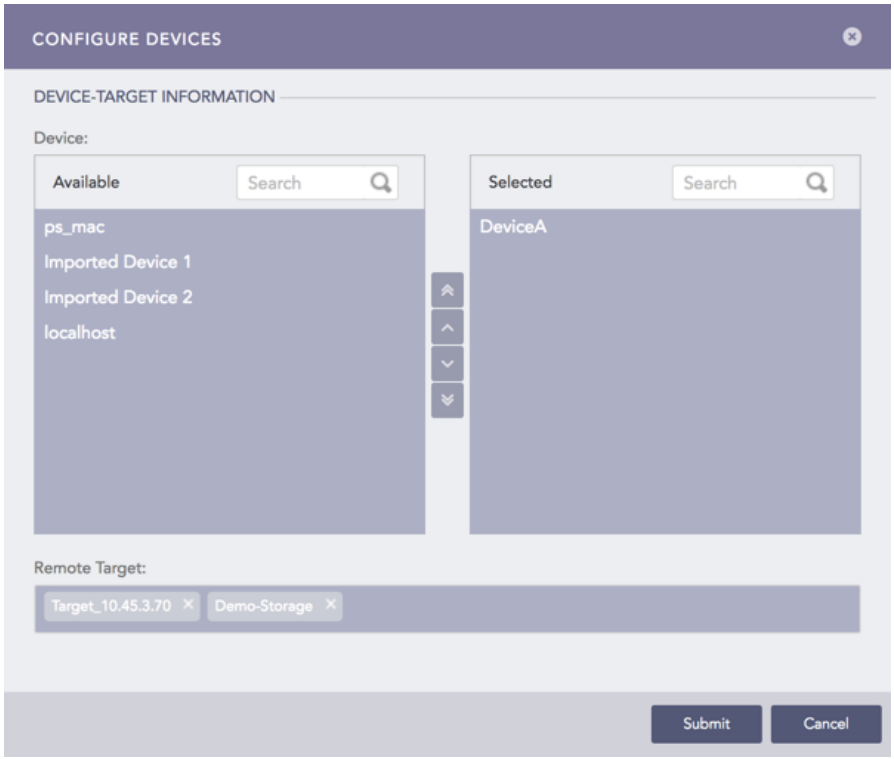
> **NOTE**
> - You can add multiple *Remote Targets* but only **one***Target Storage*. The **Add Storage** option is disabled once the configuration for a target is complete.
> - For each IP added as the Remote Target, add Syslog Forwarder in the respective target SLS.

Adding a Device

1. On the **Syslog Forwarder**, go to **Settings >> Configuration** from the navigation bar and click **Syslog Forwarder**.
2. Click **Add**.

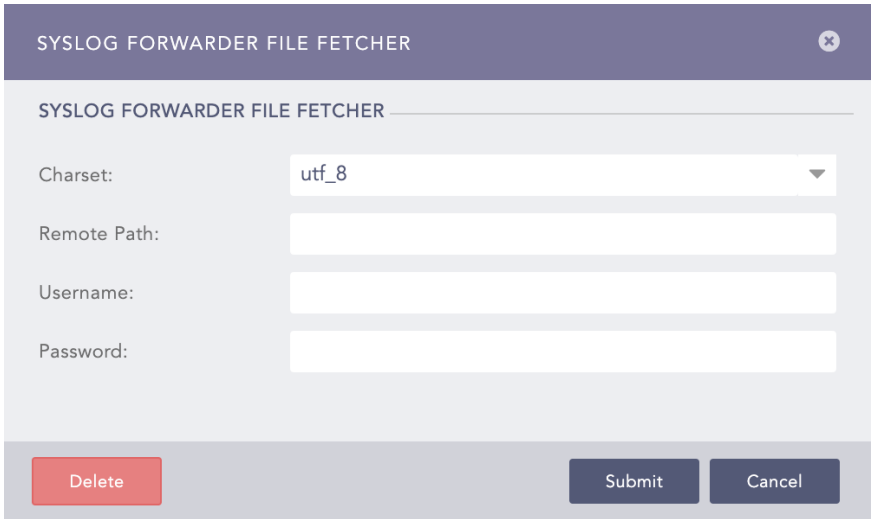
> **NOTE**
> The **Device** section lists all the devices configured as the **Syslog Forwarder** in the **Main SLS**.

3. Select devices by double-clicking on them.
4. Provide **Remote Target**(s). It can be a remote IP or a remote storage.
5. Click **Submit**.



Fetching logs from Remote Storage using Syslog Forwarder File Fetcher

1. Go to **Settings >> Configuration** and click on **Devices**.
2. Find the **Remote Target** and click on the "+" icon in the **Actions** column.
3. Select **Syslog Forwarder File Fetcher**.



4. Add Syslog Forwarder File Fetcher with following details:

   Charset: <desired charset> (utf8 by default)
   Remote Path: <add the path of the remote storgae>
   Username: <username of remote machine>
   Password: <system password of remote machine>

5. Click **Submit**.

> **NOTE**
> The logs stored in storage device contains the device_name="<end device name>". Use search query device_name=<end_device_name> to verify the logs from the remote target.

SSH Key Pair for li-admin

A SLS Administrator can generate **SSH certificates** for the **li-admin**.

1. Go to **Settings >> System Settings** from the navigation bar and click **System Settings**.
2. Select **SSH Key Pair for li-admin**.
3. Provide a **Pass Phrase**.
4. Click **Regenerate Key Pair**.

Lockout Policy

The Lockout Policy lets the admin users control user login and password security.

Lockout threshold: The number of failed login attempts that locks a user account. The default is five attempts. You can set the threshold anywhere from 0 to 999, where 0 means a user account is never locked.

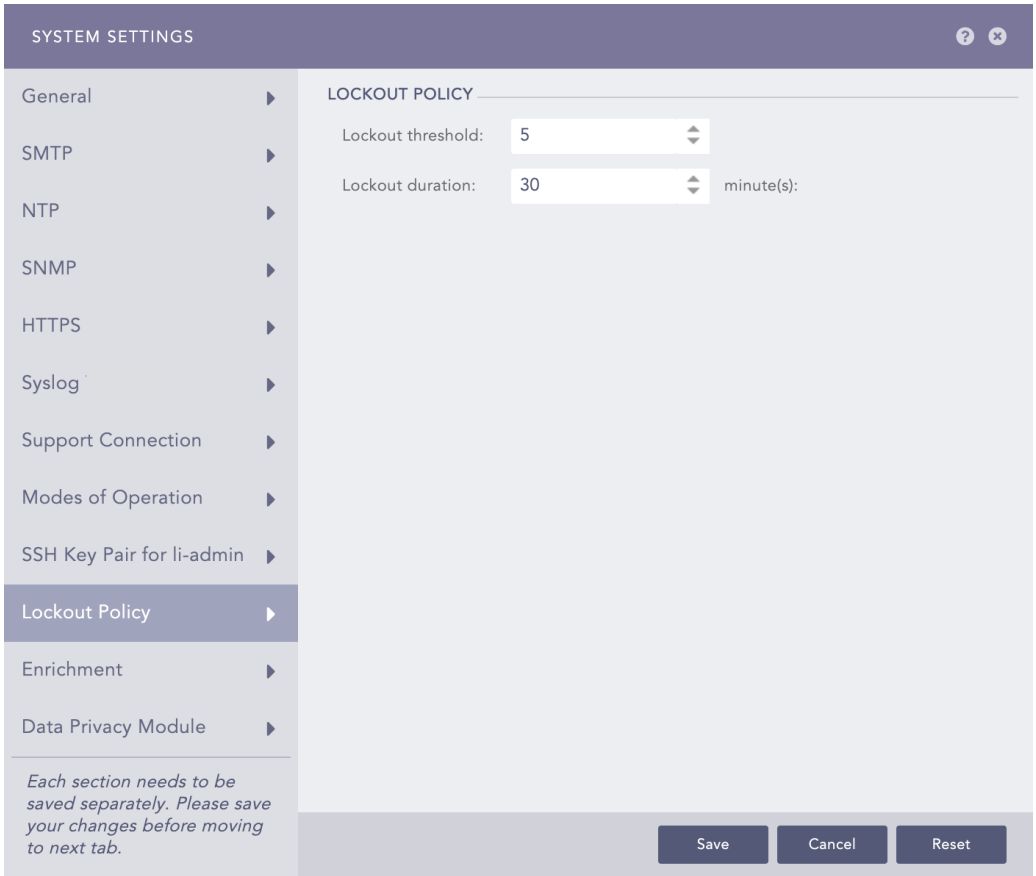
After three consecutive failed login attempts, the use of CAPTCHA authentication in addition to the username and password is required. If there are additional unsuccessful login attempts, due to a wrong username, password, or CAPTCHA authentication, and the specified lockout threshold is reached, an account is locked for the specified lockout duration.

Lockout duration: The number of minutes an account remains locked. By default, the lockout duration is 30 minutes. When the lockout duration is over, there is one more login attempt. If this attempt fails, the account is locked for the additional specified lockout period. This process continues until a user logs in with valid credentials. The lockout duration can be between 1 to 99999.

> **NOTE**
> After a user is locked out, a *User Locked* icon appears in the Actions column of the respective user under **Settings >> User Accounts** from the navigation bar and **Users**. The SLS administrator can unlock the locked users by clicking the icon.

Configuring Lockout Policy

1. Go to **Settings >> System Settings** from the navigation bar and click **System Settings**.
2. Select **Lockout Policy**.



3. Select a **Lockout threshold** from the drop-down list. The default is 5.
4. Enter the **Lockout duration**. The default is 30 minutes.
5. Click **Reset** if you want to reset the values to default.
6. Click **Submit**.

Enrichment

Enrichment settings manage whether you use Standalone Mode and Enrichment Propagation Mode.

Before configuring Enrichment in either of the modes, it is necessary to configure some prerequisites in SLS. These essentials include **Enrichment Sources**, **Enrichment Policies**, **Normalization Policies**, and **Processing Policies**.

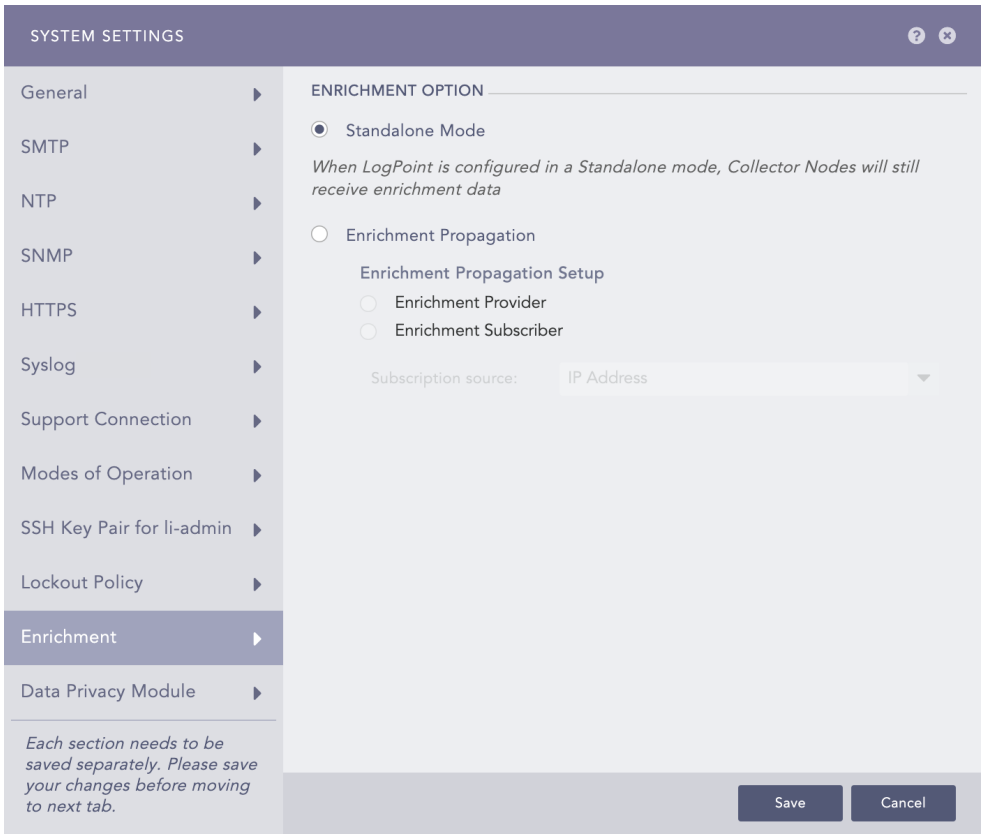
> **NOTE**
> Integrations associated with the enrichment sources need to be installed before adding an enrichment source. For example, if you need to add an ODBC enrichment source, the ODBC Enrichment Source plugin must be present in the SLS.
> Enrichment settings manage whether you use Standalone Mode and Enrichment Propagation.

Standalone Mode

In **Standalone Mode**, you need to add enrichment sources to SLS and perform the enrichment in the same SLS.

Configuring Enrichment in the Standalone Mode

1. Go to **Settings >> System Settings** from the navigation bar and click **System Settings**.
2. Select **Enrichment**.



3. Select the **Standalone Mode**.
4. Click **Save**.

Enrichment Propagation

Enrichment Propagation uses multiple SLSs to perform enrichment tasks. A SLS machine can be either an enrichment provider or an enrichment subscriber. You must set up a distributed SLS connection to configure SLS in the **Enrichment Propagation** mode.

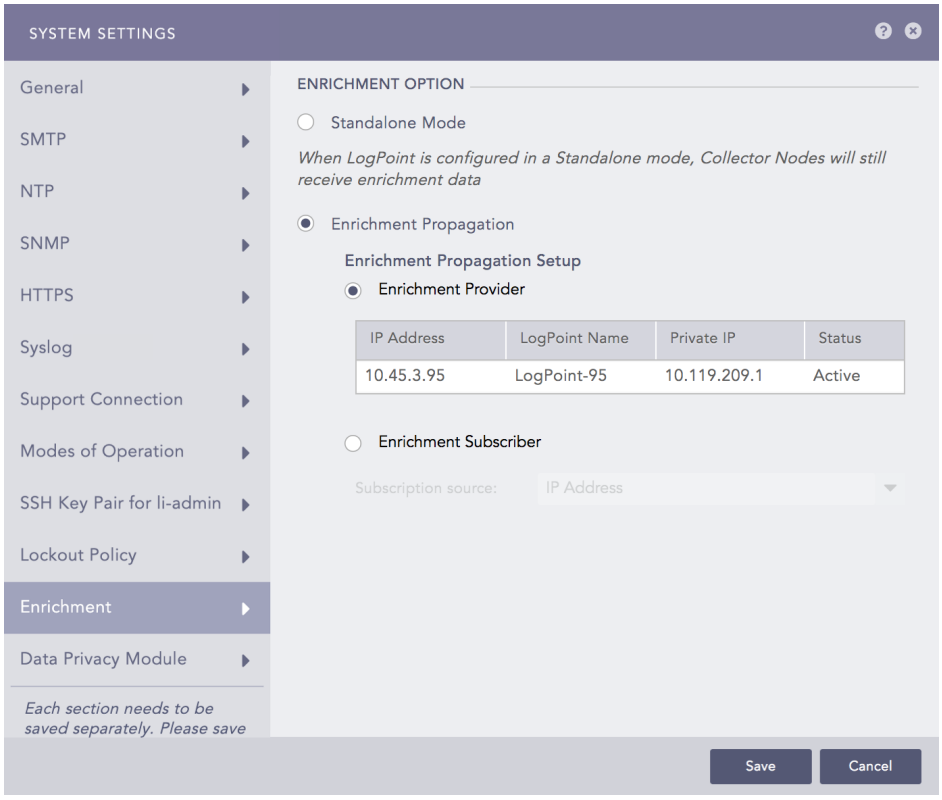
- **Enrichment Provider**: Collects raw data and shares it with enrichment subscribers. It keeps a list of all the *IP Addresses* of enrichment subscribers.
- **Enrichment Subscriber**: Receives enrichment data from an enrichment provider to create rules for the enrichment process. It also acts as a bridge between a *SLS Collector* and an enrichment provider. For Enrichment Subscribers, the *Enrichment Sources* option in [Settings >> Configuration] page is disabled. They have to use the sources of an enrichment provider.
- You can have any number of enrichment subscribers but only one enrichment provider. One enrichment provider can be connected to:
  - A single enrichment subscriber
  - Multiple enrichment subscribers
  - A single enrichment subscriber connected to a SLS Collector
  - Multiple enrichment subscribers connected to multiple SLS Collectors

Configuring Enrichment Propagation

When setting up **Enrichment Propagation**, make sure to configure an **Enrichment Provider** first. After setting up an Enrichment Provider, then setup the **Enrichment Subscribers**. When setting up an existing SLS instance as an Enrichment Subscriber, you need to delete all existing enrichment policies and their dependencies before configuring it as an enrichment subscriber.

> **NOTE**
> While removing the **UEBA_ENRICHMENT_POLICY** and **Threat_Intelligence** enrichment policies, remove *Threat Intelligence* and *UEBA PreConfiguration* too. After successfully removing the enrichment policies, manually install both the applications in the new enrichment subscriber.

1. Go to **Settings >> System Settings** from the navigation bar and click **System Settings**.
2. Select **Enrichment**.
3. Select **Enrichment Propagation**.
4. Select **Enrichment Provider** or **Enrichment Subscriber** as needed. If you select **Enrichment Subscriber**, choose a **Subscription Source**, which is the IP address of an enrichment provider from the drop-down menu.

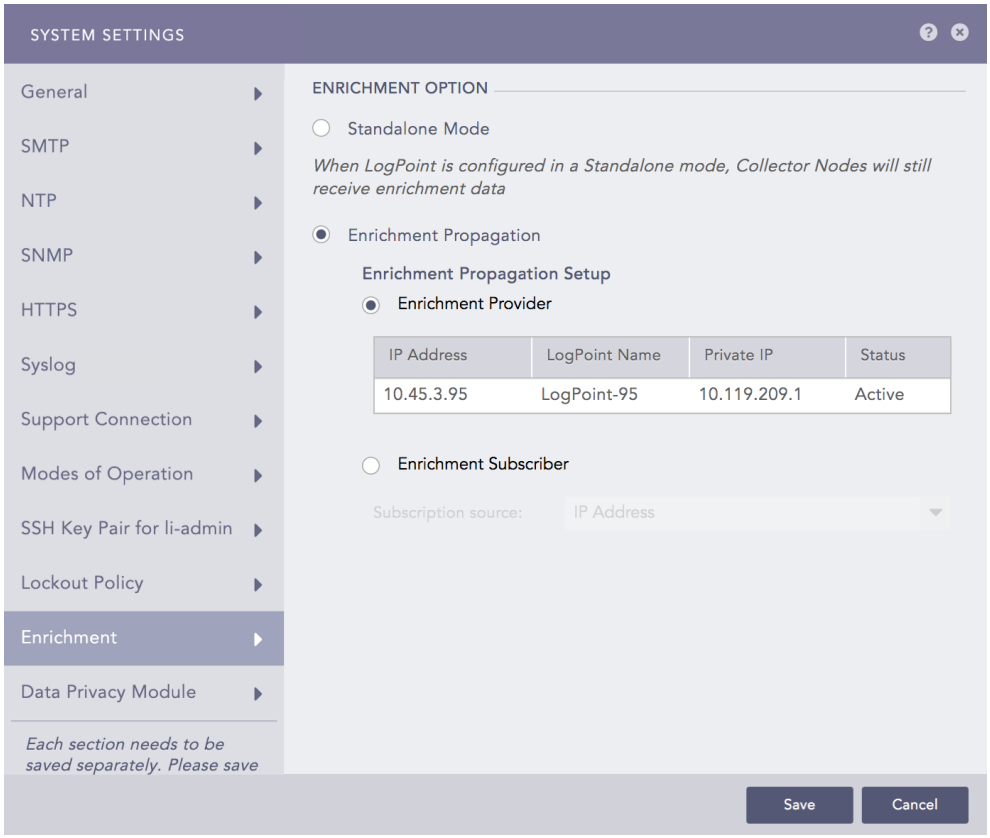


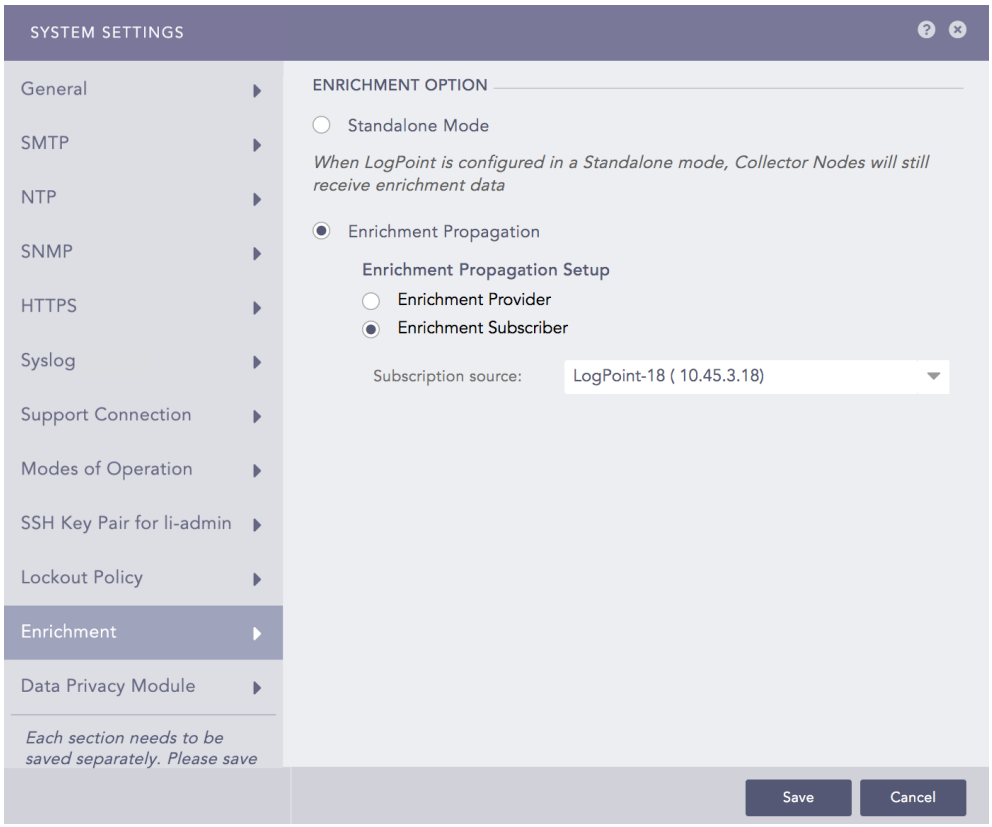
5. Click **Save**.

Enrichment Propagation Working Scenario

The following scenario depicts an enrichment process in the **Enrichment Propagation** mode with a configuration of 2 machines: *Machine 1* and *Machine 2*.

Select **Enrichment Provider** in *Machine 1* and **Enrichment Subscriber** in *Machine 2*.



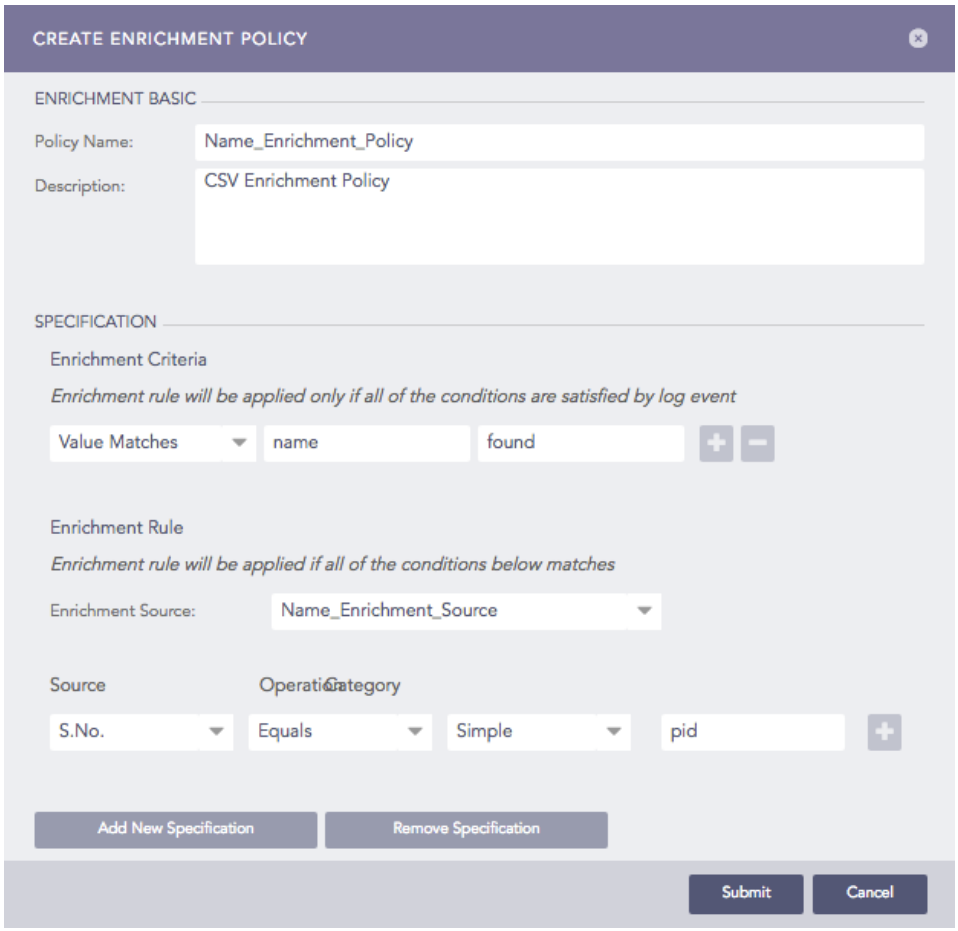


Next, add a *CSV Enrichment Source* to Machine 1 using the data from the following CSV file.

S.No.	Value	Task	Operation
1	read1	write1	RW1
2	read2	write2	RW2
3	read3	write3	RW3
4	read4	write4	RW4
5	read5	write5	RW5
6	read6	write6	RW6
7	read7	write7	RW7

After adding the source, add a normalization package containing log signatures to Machine 2.

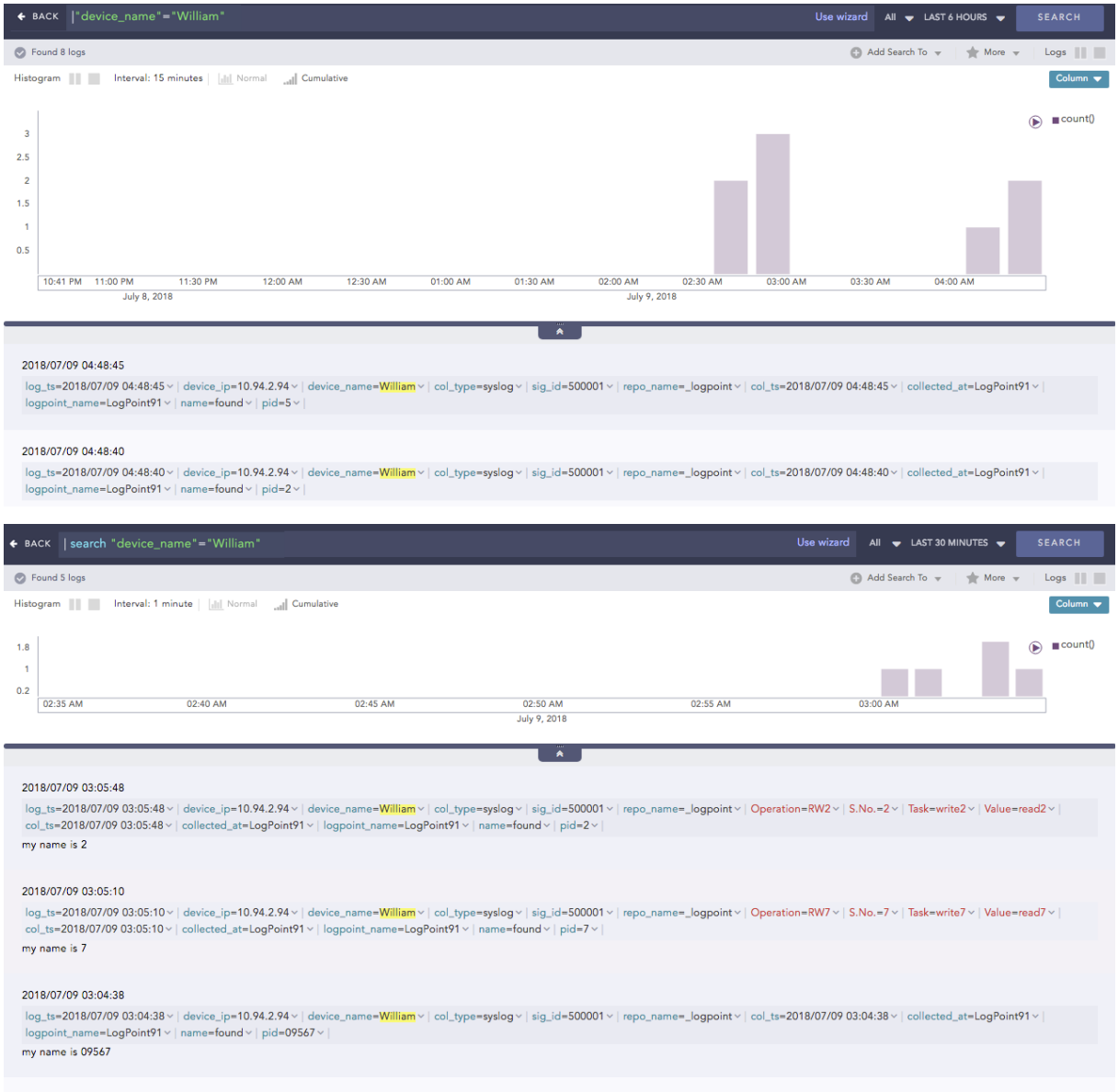
Furthermore, add a normalization policy, enrichment policy, and routing policy to Machine 2.



Finally, add a processing policy to incorporate all the policies earlier created and add it to a device.

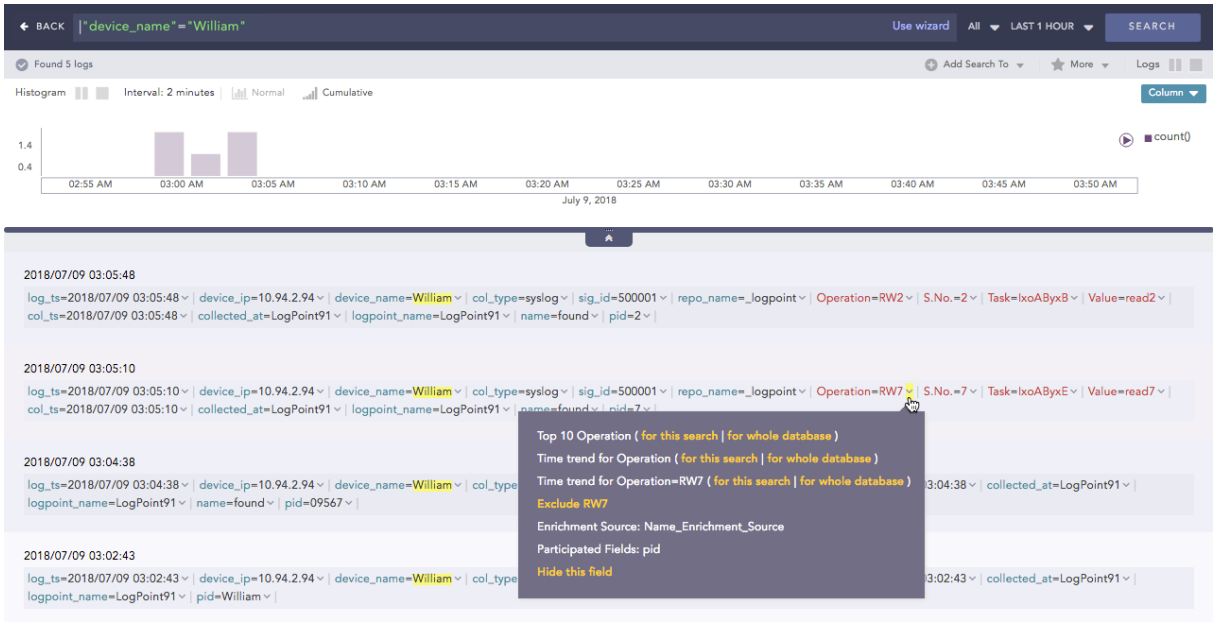
> **NOTE**
> In the **Standalone Mode**, all the above tasks are performed in a single machine.

You can now see the enriched results in the search results of the enrichment subscriber.

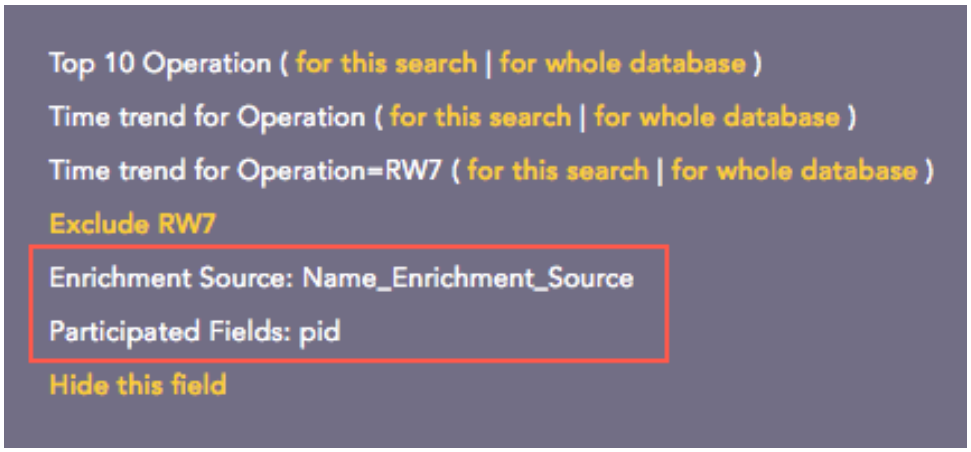


Drilldown Operation in the Enriched Results

Click the drop-down menu on the enriched fields to view the different actions.



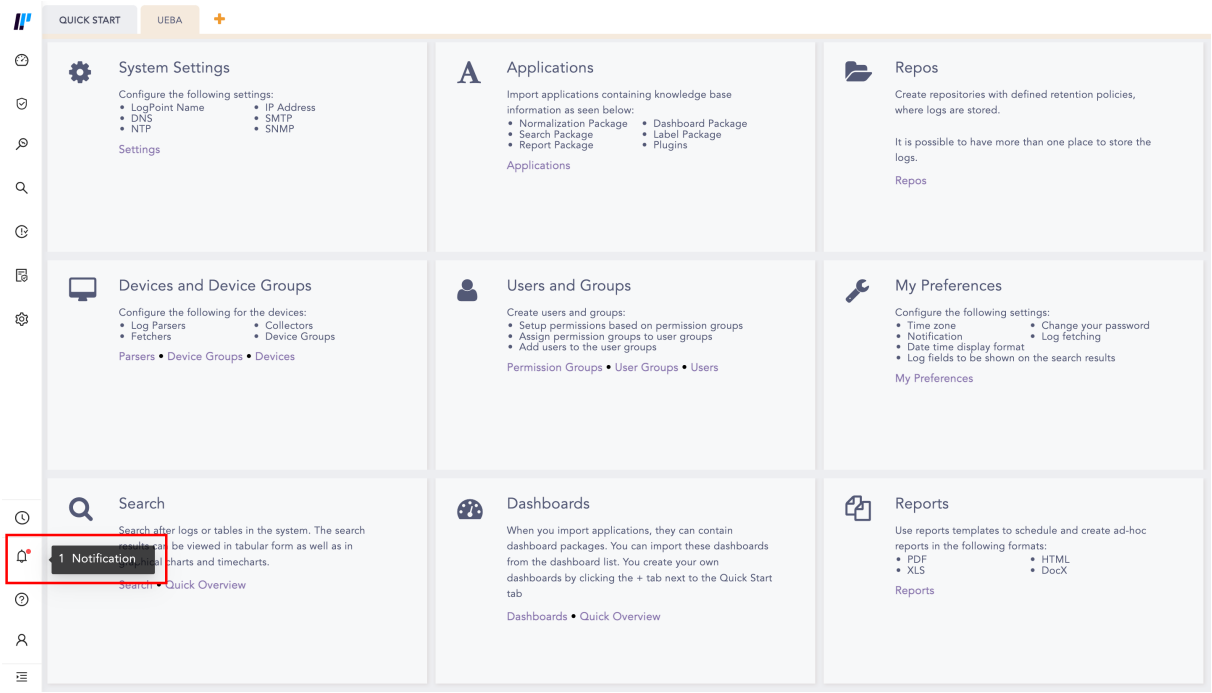
1. **Enrichment Source**: Displays the information of the source file the enriched field belongs to.
2. **Participated Fields**: Displays the field of a log specified in the enrichment rule to enrich the log.



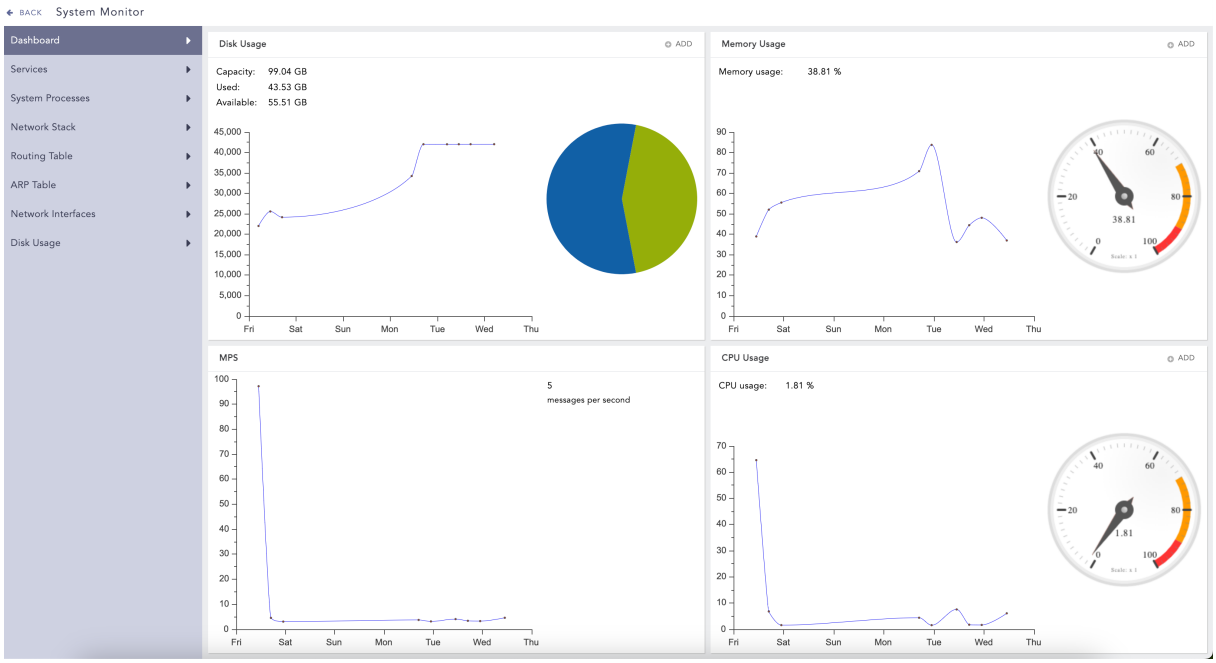
In the above example, the Participated Field *pid* has been specified in the earlier created enrichment rule. The enrichment rule matches the value of the *pid* field in the log to the *S.No.* field in the source and enriches the log.

System Notifications

System Notification notifies you of Disk, CPU, and Memory usage of SLS. When there is a new notification, the navigation bar displays an alert. Click the **Notification** icon to open **Notification Center**.

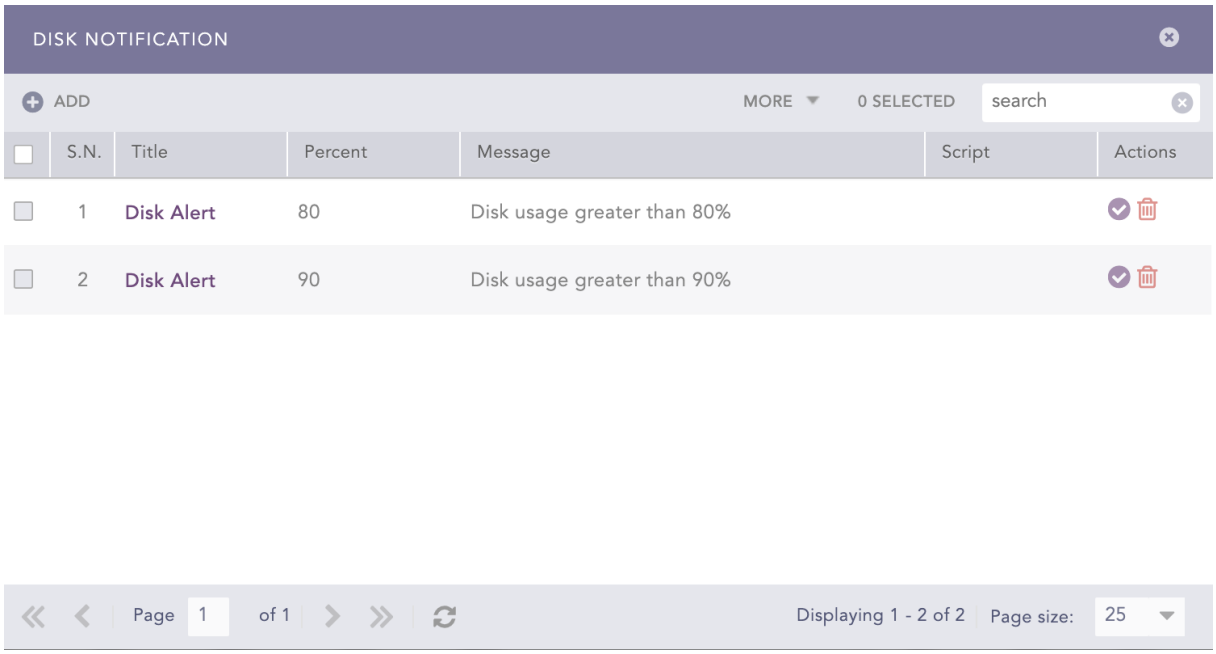


These notifications are configured from `Settings >> System Settings >> System Monitor >> Dashboard`.

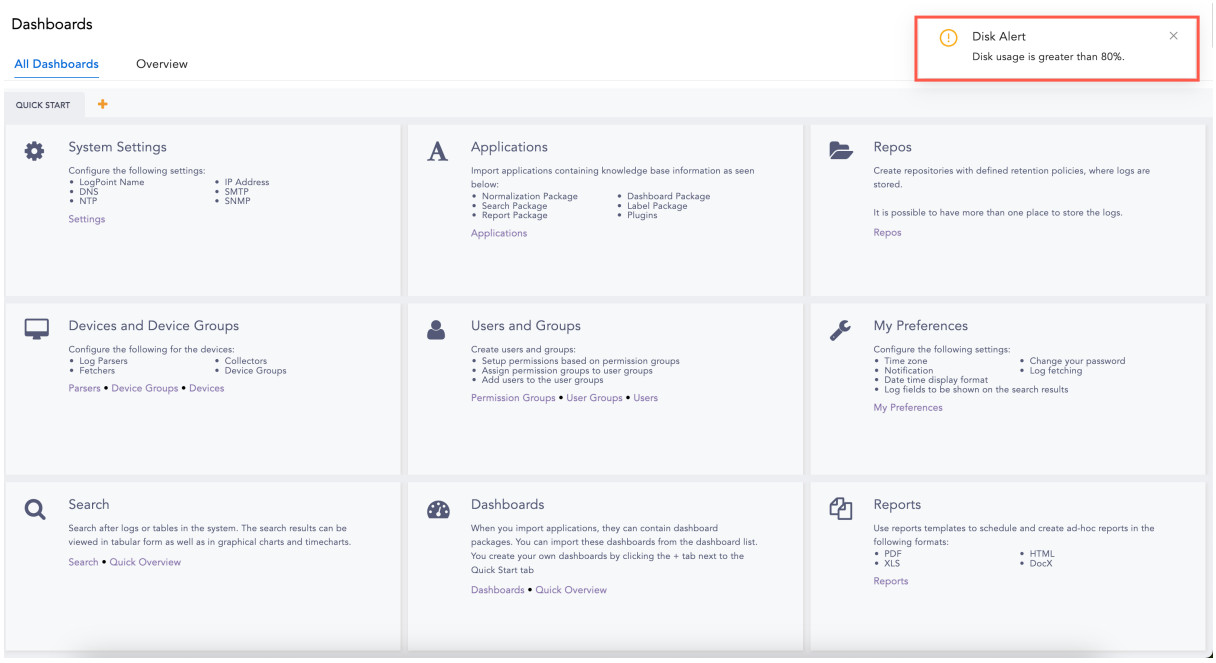


Disk Usage Notification

Two notifications are setup and activated in SLS out-of-the-box. You are notified when the total disk usage reaches 80% and 90%. The values can be configured to trigger the notification at any threshold. To create more disk usage notifications, go to Configure Custom Disk Usage Notification.



You also get a pop-up notification when your disk usage is greater than 80%. This pop-up is displayed even when there are no disk notifications configured.

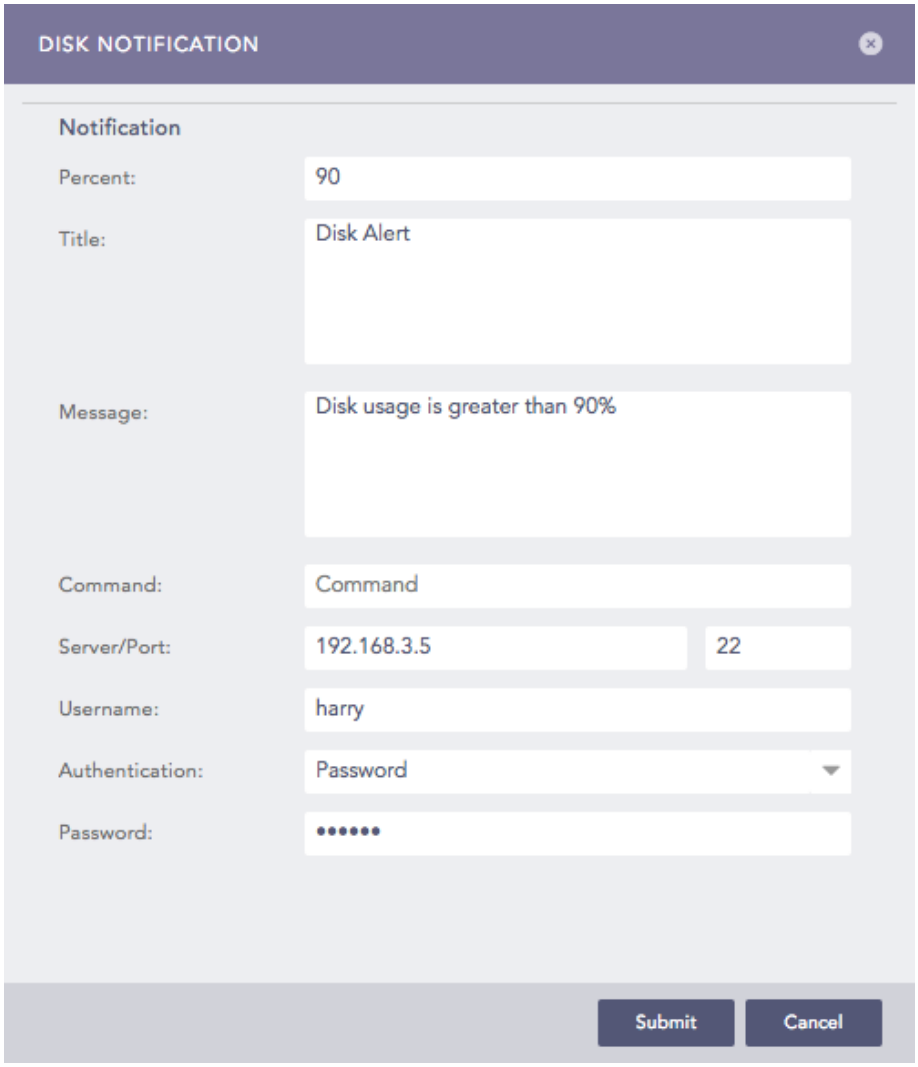


NOTE

- The Disk, CPU, and Memory Notifications use a common SSH Certificate.

Configure Custom Disk Usage Notification

1. Go to `Settings >> System Settings` from the navigation bar and click **System Monitor**.
2. Select **Dashboard**.
3. In **Disk Usage**, Click **Add**.

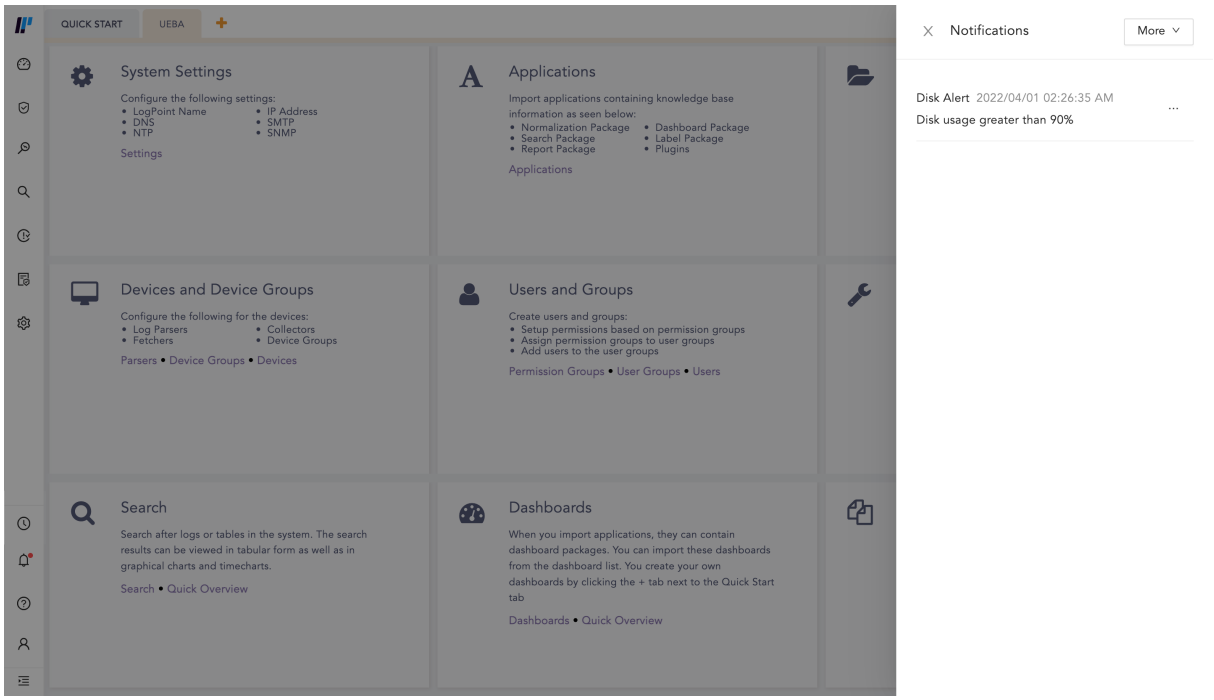


4. Enter the **Percent** of total disk space used that triggers a notification, or at what threshold you want to be notified.
5. Enter the **Title** and **Message** you want the notification to have.
6. If you want to initiate a command at the same time the notification is sent, specify a system **Command**. The command should be an executable bash command. Providing a **Command** is optional.
   For Example: The following Bash command checks for free disk space at **/dev/sda** and also cleans up cached packages at that location:
   ```
   df - Th/dev/sda
    sudo apt-get clean
   ```
7. Enter the address of the remote **Server** and the **Port** number.

8. Select the **Authentication** type of the remote **Server**.
   - If you choose **Password**, enter a **Password**.
   - If you choose **SSH Certificate**, an **SSH Certificate** is automatically generated.

   The password or the SSH certificate key are required for user validation while accessing the remote server. Make sure you are able to remember them.
9. Click **Submit**.

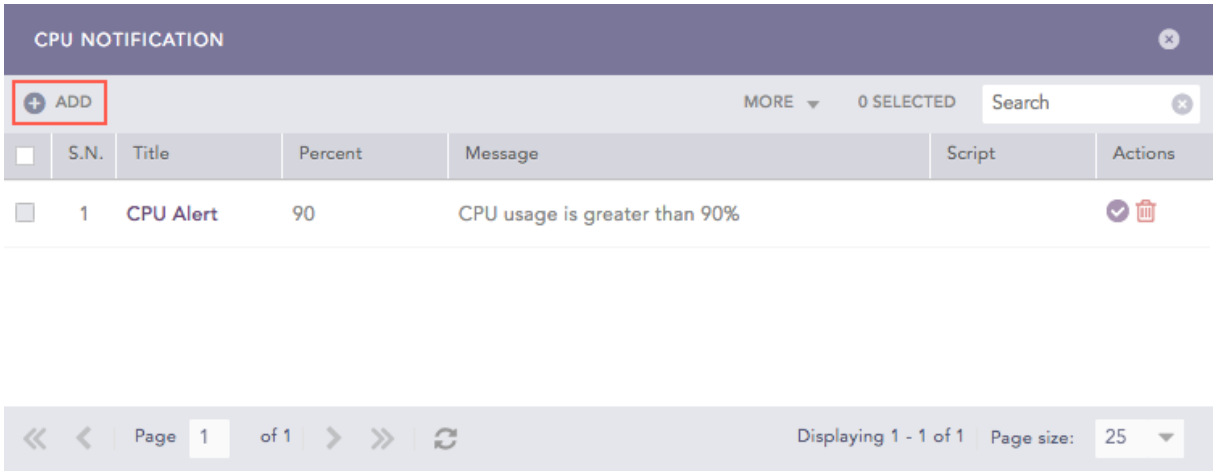
When the notification is triggered, the notification is displayed in the notification center.



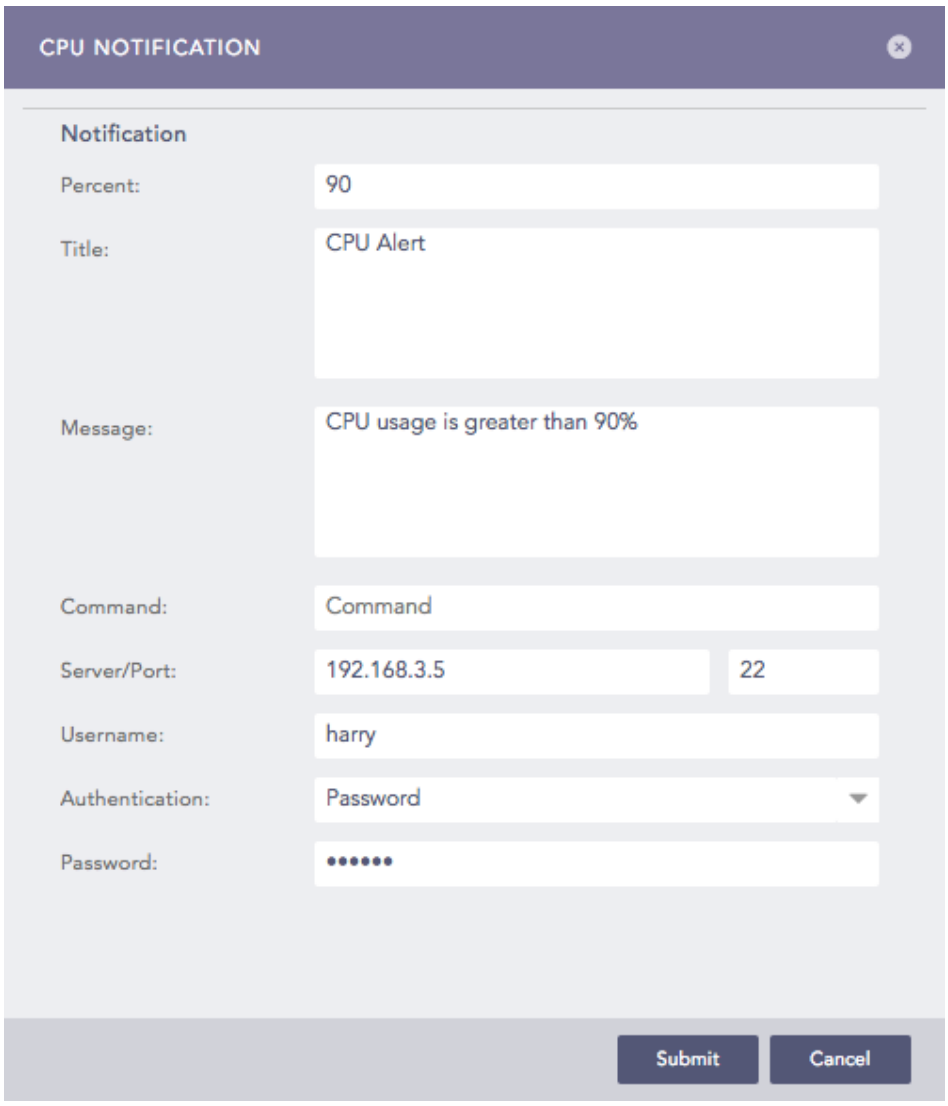
CPU Usage Notification

There are no CPU usage notification setup and activated in SLS out-of-the-box. To configure CPU usage notification:

1. Go to `Settings >> System Settings` from the navigation bar and click **System Monitor**.
2. Select **Dashboard**.
3. In **CPU Usage**, click **Add**.



4. Enter the **Percent** of total disk space used that triggers a notification, or at what threshold you want to be notified.



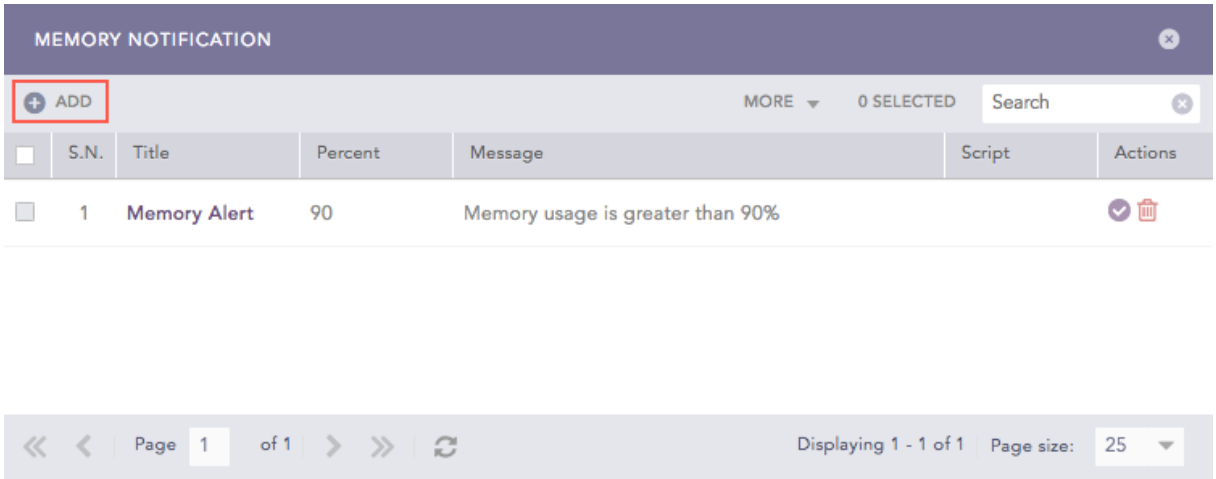
5. Enter the **Title** and **Message** you want the notification to have.
6. If you want to initiate a command at the same time the notification is sent, specify a system **Command**. The command should be an executable bash command. Providing a **Command** is optional.
   For Example: The following command checks for any files greater than 50MB and lists them in the terminal:
   ```
   sudo find / -type f -size +50M -exec ls -lh {} \;
   ```
7. Enter the address of the remote **Server** and the **Port** number.
8. Select the **Authentication** type of the remote **Server**.
   - If you choose **Password**, enter a **Password**.
   - If you choose **SSH Certificate**, an **SSH Certificate** is automatically generated.

   The password or the SSH certificate key are required for user validation while accessing the remote server. Make sure you are able to remember them.
9. Click **Submit**.

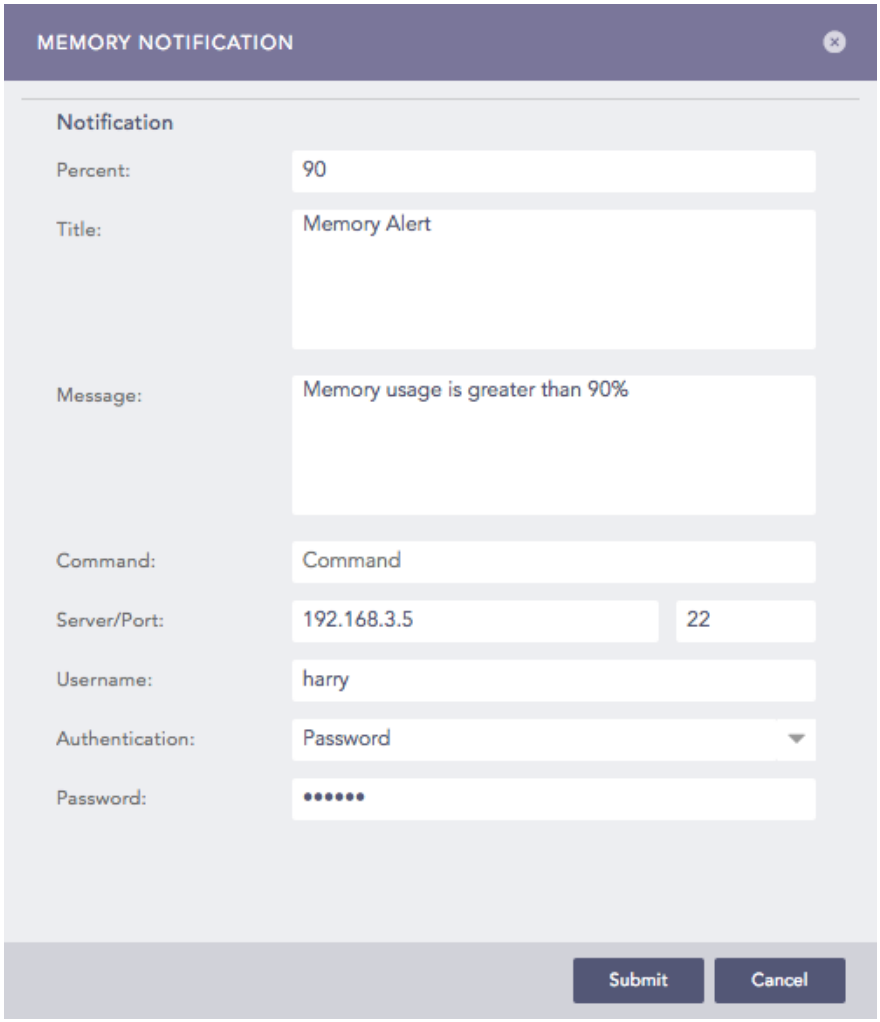
Memory Usage Notification

There are no Memory usage notification setup and activated in SLS out-of-the-box. To configure Memory usage notification:

1. Go to `Settings >> System Settings` from the navigation bar and click **System Monitor**.
2. Select **Dashboard**.
3. In **Memory Usage**, Click **Add**.



4. Enter the **Percent** of total disk space used that triggers a notification, or at what threshold you want to be notified.



5. Enter the **Title** and **Message** you want the notification to have.
6. If you want to initiate a command at the same time the notification is sent, specify a system **Command**. The command should be an executable bash command. Providing a **Command** is optional.
   For Example: The following command clears all the PageCaches in the RAM:
   ```
   # sync; echo 1 > /proc/sys/vm/drop_caches
   ```
7. Enter the address of the remote **Server** and the **Port** number.
8. Select the **Authentication** type of the remote **Server**.
   - If you choose **Password**, enter a **Password**.
   - If you choose **SSH Certificate**, an **SSH Certificate** is automatically generated.

   The password or the SSH certificate key are required for user validation while accessing the remote server. Make sure you are able to remember them.
9. Click **Submit**.

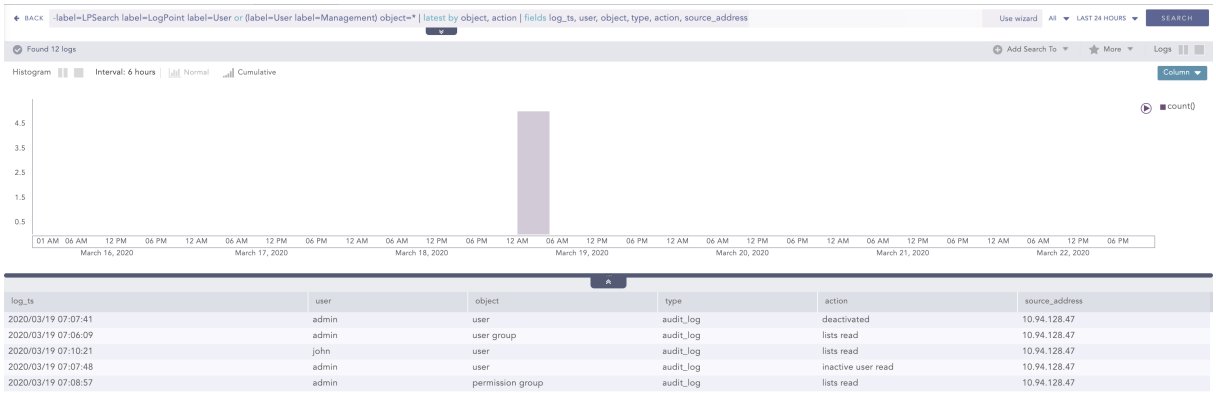
Audit Logs

Audit logs are records of events and activities that occur within SLS. SLS generates various audit logs related to different events for security purposes. Only authorized users can access audit logs.

User management

- Audit logs are generated when you add, edit, or delete users, user groups, and permissions.
- Sample query to view the logs:

```
-label=LPSearch label=SLS label=User or (label=User label=Management)
object=* | latest by object, action | fields log_ts, user, object, type,
action, source_address
```

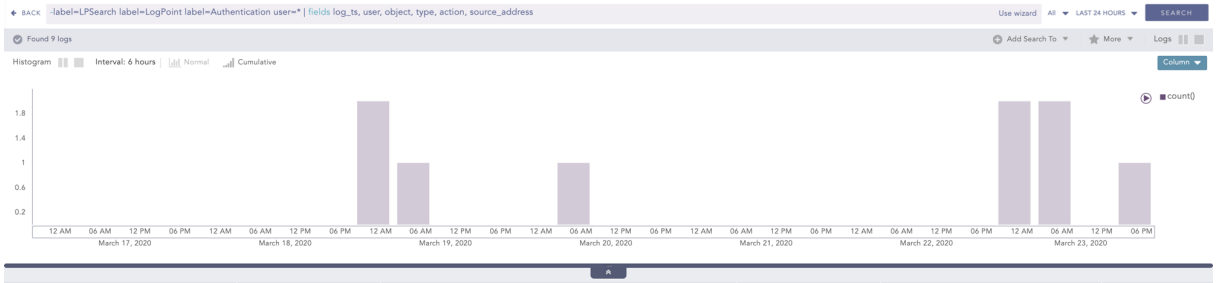


log_ts	user	object	type	action	source_address
2020/03/19 07:07:41	admin	user	audit_log	deactivated	10.94.128.47
2020/03/19 07:06:09	admin	user group	audit_log	lists read	10.94.128.47
2020/03/19 07:10:21	john	user	audit_log	lists read	10.94.128.47
2020/03/19 07:07:48	admin	user	audit_log	inactive user read	10.94.128.47
2020/03/19 07:08:57	admin	permission group	audit_log	lists read	10.94.128.47

Identification and authentication

- Audit logs are generated for login attempts, login success, login failures, and user lock/unlock.
- Sample query to view the logs:

```
-label=LPSearch label=SLS label=Authentication user=* | fields log_ts,
user, object, type, action, source_address
```



log_ts	user	object	type	action	source_address
2020/03/24 01:10:44	admin	plugin logpointauthentication	audit_log	Login - Successful	10.94.128.4
2020/03/23 09:01:21	admin	plugin logpointauthentication	audit_log	Login - Successful	10.94.128.71
2020/03/23 07:36:42	admin	plugin logpointauthentication	audit_log	Login - Successful	10.94.128.71
2020/03/23 05:46:51	admin	plugin logpointauthentication	audit_log	Login - Successful	10.94.128.27
2020/03/23 04:43:27	admin	plugin logpointauthentication	audit_log	Login - Successful	10.94.128.27
2020/03/20 08:38:52	admin	plugin logpointauthentication	audit_log	Login - Successful	10.94.128.22
2020/03/19 10:12:32	admin	plugin logpointauthentication	audit_log	Login - Successful	10.94.128.47
2020/03/19 07:09:50	john	plugin logpointauthentication	audit_log	Login - Successful	10.94.128.47
2020/03/19 07:03:58	admin	plugin logpointauthentication	audit_log	Login - Successful	10.94.128.47

User actions

- Audit logs are generated when you add, edit, or delete Knowledge Base items, Configuration items (Device, Device Group, Log Collection Policies, Repos, Distributed SLS), Search,

Report, Dashboard, and Incident Management, and configure the UEBA Board.

- Sample query to view the logs:

```
-label=LPSearch label=SLS
label=Configuration (label=Change or label=Add or label=Delete or
label=Install or label=Mount) | chart count() by log_ts, user, type,
object, action
```

Inter-TSF trusted channel

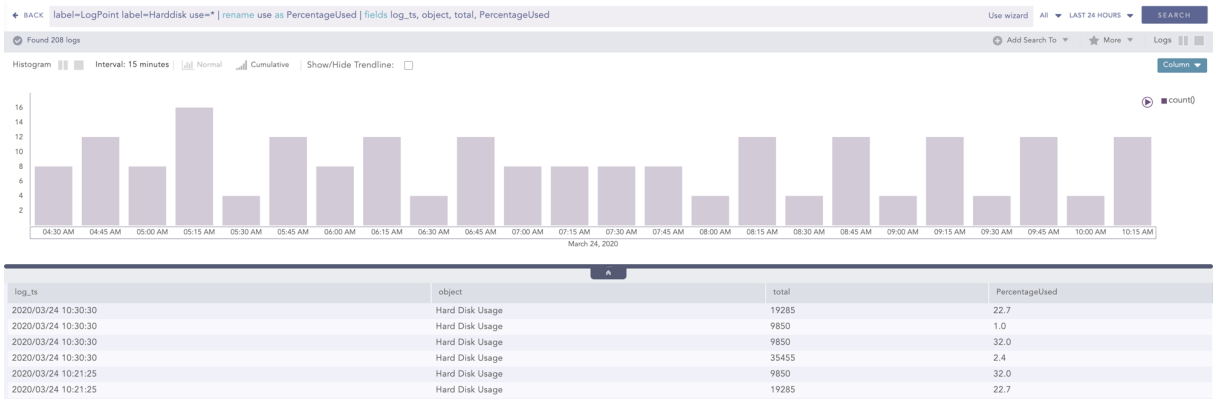
- Audit logs are generated when attempts are made to connect or disconnect from another SLS.
- Sample query to view the logs:

```
-label=LPSearch label=SLS (label=Remote label=Connection) OR (label=DLP
(label=Connect OR label=Disconnect OR label=Initialize)) | chart count()
by log_ts, type, object, user, action
```

System

- Audit logs are generated when disk usage exceeds the predefined limit. The predefined limit for notification is 90% by default, and it is user-configurable. Audit logs are generated every hour.
- Sample query to view the logs:

```
label=SLS label=Harddisk use=* | rename use as PercentageUsed | fields
log_ts, object, total, PercentageUsed
```



Selectable Audit Logs

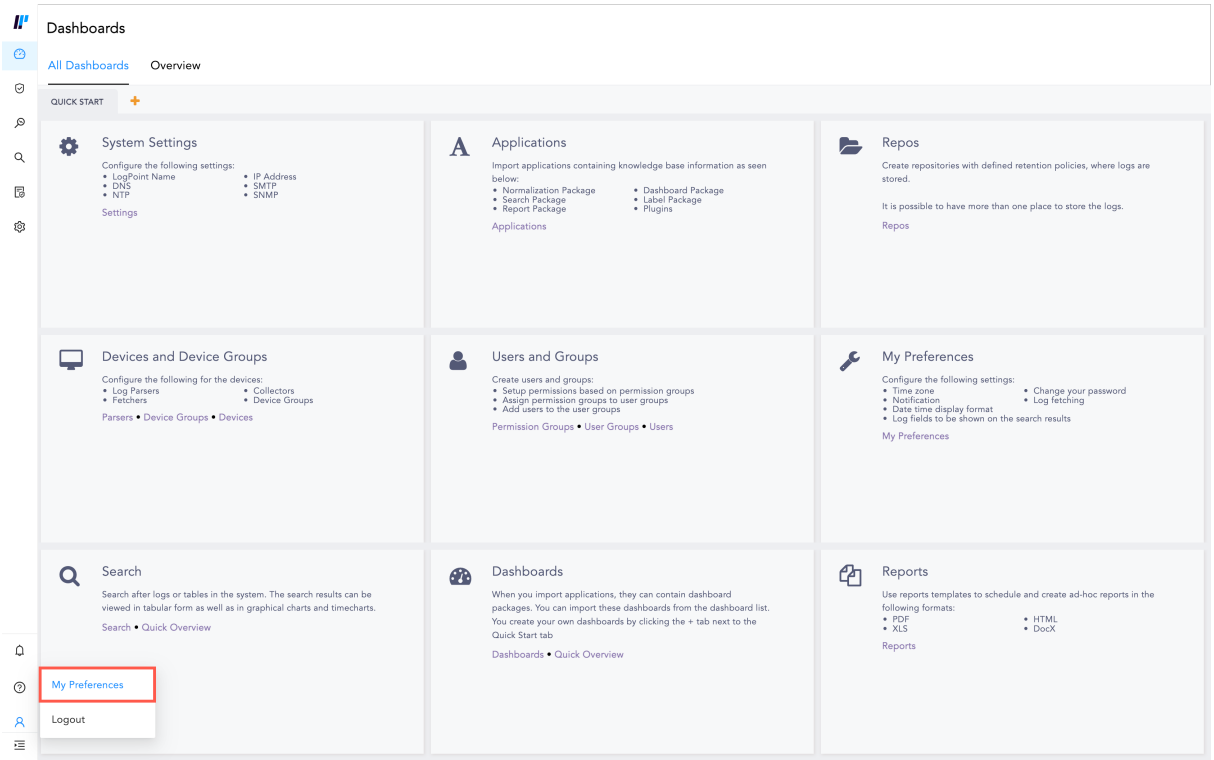
To sort event data, follow these steps:

1. After successful login, click **Search** from the top horizontal menu.
2. Enter a valid query in the search query bar.
3. Click the column header of the results table to sort the logs.

My Preferences

My Preferences lets you customize the SLS UI and update your account settings. It helps you personalize various UI components like result limits, notification positions and help-boxes to improve usability.

Go to `User >> My Preferences` in the navigation bar to access it.



My Preferences is grouped into:

1. **Account**: Update personal details, password, preferred date and time format and API Access Key.
2. **User Interface**: Configure the page limits and search fields, where notification pop-ups are displayed, help-boxes and whether to pre-compute dashboard data. Using the precomputation technique, the system calculates and stores the dashboard data ahead of time and reuses the data to speed up further inquiries.

Account

User Details

You can view your **Full Name** and **Email** in **User Details**.

Change Password

You can change your password in **Change Password**. It is only visible to the users authenticated with SLS's basic authentication.

Date/Time Preferences

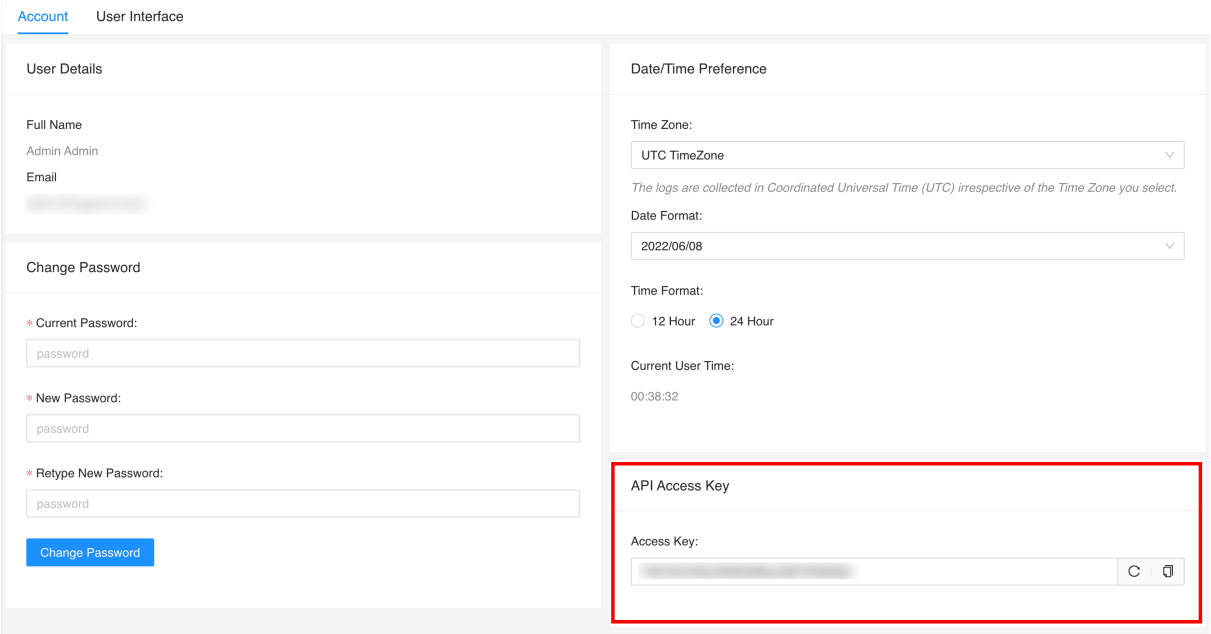
In **Date/Time Preferences**, you can view and edit:

- Time Zone
- Date Format
- Hour Display Format

> **NOTE**
> The logs are collected in Coordinated Universal Time (UTC) irrespective of the **Time Zone** you select.

API Access Key

The **API Access Key** is a unique identification for each user. You can use it to access the API endpoints SLS exposes.



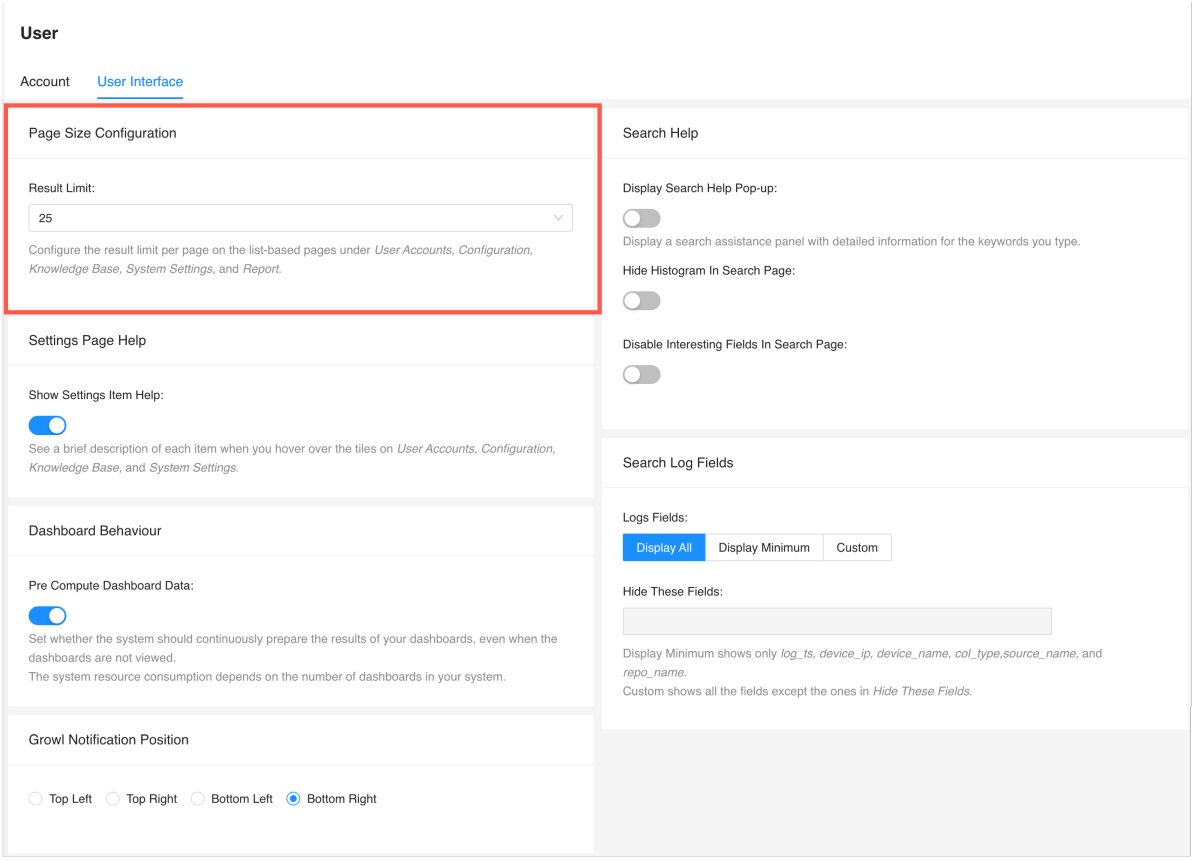
Click **Re-generate Key** ( ) to generate a new access key and **Copy to Clipboard** ( ) to copy your access key to the clipboard.

> **NOTE**
> Once you generate a new access key, the previous key becomes invalid and you cannot use it anymore.

User Interface

Page Size Configuration

Configure the **Result Limit** per page on the **Settings** and **Reports** pages.



Settings Page Help

Select **Show Settings Item Help** to get a description of each setting when you hover your mouse over **User Accounts, Configuration, Knowledge Base** and **System Settings**.

Dashboard Behavior

Controls whether SLS continuously updates dashboard data even when they are not being viewed.

Growl Notification Position

Choose the position where the notifications appear.

Search Help

In **Search Help** you can select:

1. Select **Search Help Pop-up** to get search assistance when you type keywords.
2. Display or hide the histogram on the **Search** page.
3. Display or hide the **Interesting Fields** on the **Search** page.

Search Log Fields

Choose the fields to display in the search results.

1. **Display All** shows all fields in the log.
2. **Display Minimum** shows **log_ts**, **device_ip**, **device_name**, **col_type**, **source_name** and **repo_name** for each log.
3. **Custom** shows all the fields present in the log except the ones you provide in **Hide These Fields**.

Export Management

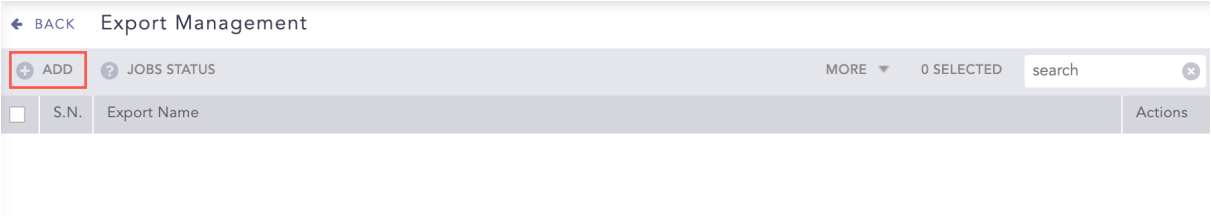
Export Management allows you to export raw logs from Search results to a target (storage location) placed on a remote machine. **Export Management** is only available for simple search queries and not for aggregated queries.

> **NOTE**
> **Export Management** is disabled in **Data Privacy Module** enabled systems.

Adding a Target

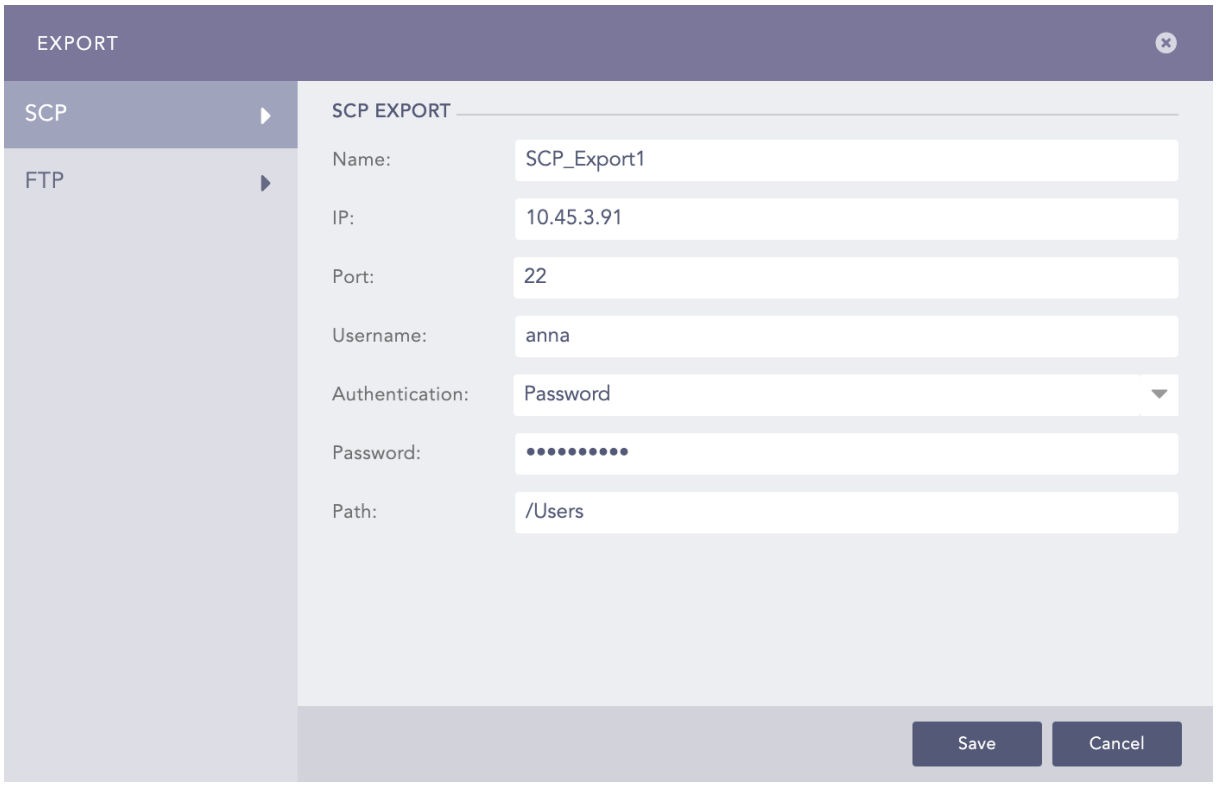
You can create a target either by using **Secure Copy Protocol (SCP)** or **File Transfer Protocol (FTP)**. Before configuring Export Management, you need to create a target. To create a target:

1. Go to `Settings >> Configuration` from the navigation bar and click **Export Management**.



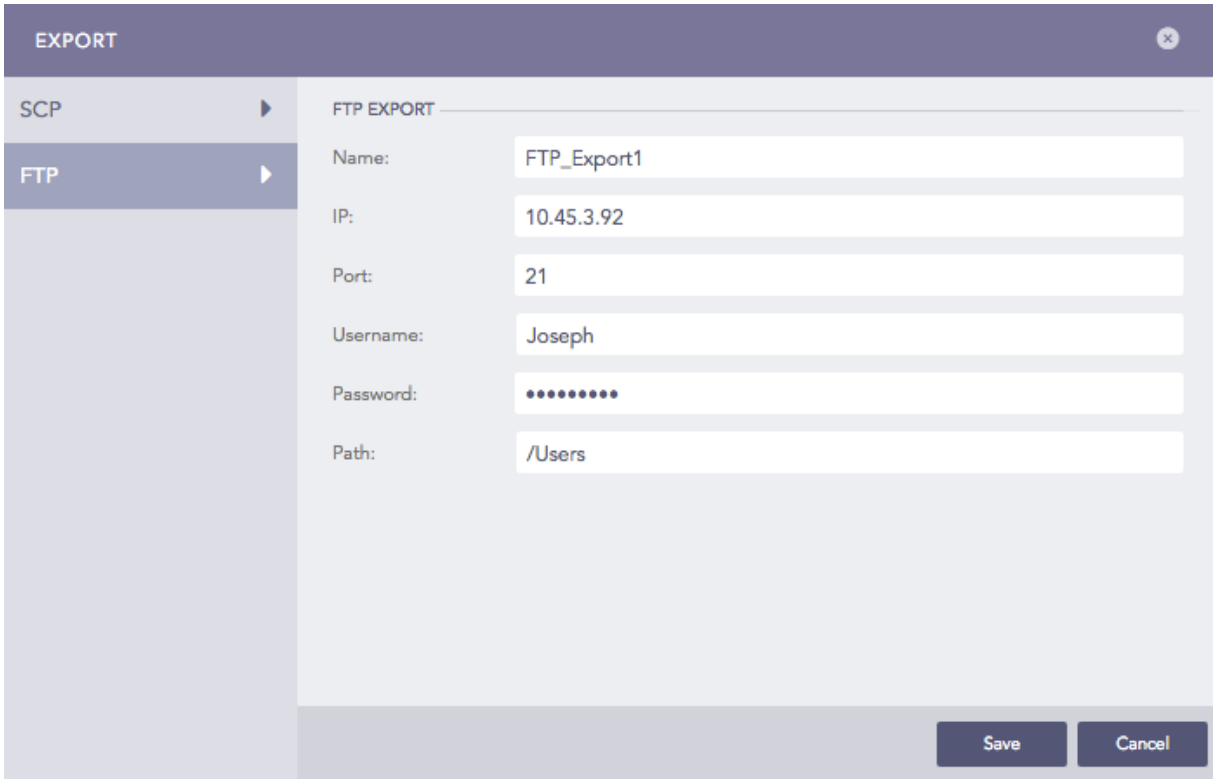
2. Click **Add**. Here, you have an option to add the target using either **SCP** protocol or **FTP** protocol as per your requirement.

For **SCP**:



1. Provide a **Name**.
2. Specify the **IP** address of the remote machine.
3. Enter a **Port** number.
4. Provide the **Username**.
5. Select an **Authentication** mechanism.
6. If you selected **Password**, enter the **Password** for authentication.
7. If you selected **SSH Certificate**, copy the provided key and add it to **authorized keys** in the remote machine.
8. Specify the **Path** in the target machine.

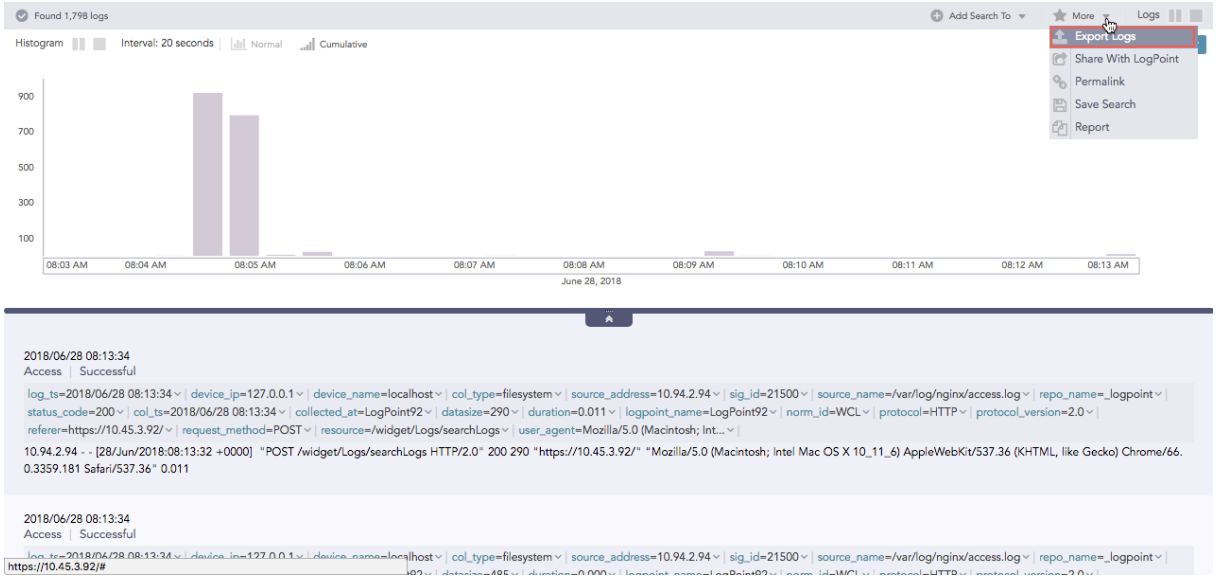
For **FTP**:



1. Provide a **Name** of the export file.
2. Specify a valid **IP** address of the remote machine.
3. Enter a **Port** number.
4. Provide the **Username** and **Password** recognized by the given IP address.
5. Specify the **Path** of the target.
6. Click **Save**.

Accessing a Target

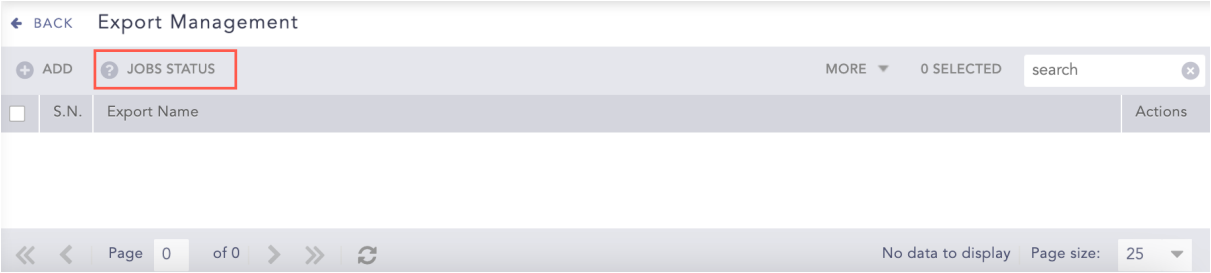
Once you create and configure a target, you can access it via the **Export Logs** option under the **More** drop-down from the **Search** menu. The names of the created targets are populated in the drop-down menu under `Search >> More >> Export Logs >> Target`. Now, you can export the search results of any search query to any target as per the requirement.



> **NOTE**
> If you have configured **SCP Export**, multiple lines of the same log are counted as different logs. Therefore, the number of logs in the search results is different from the number of exported logs.

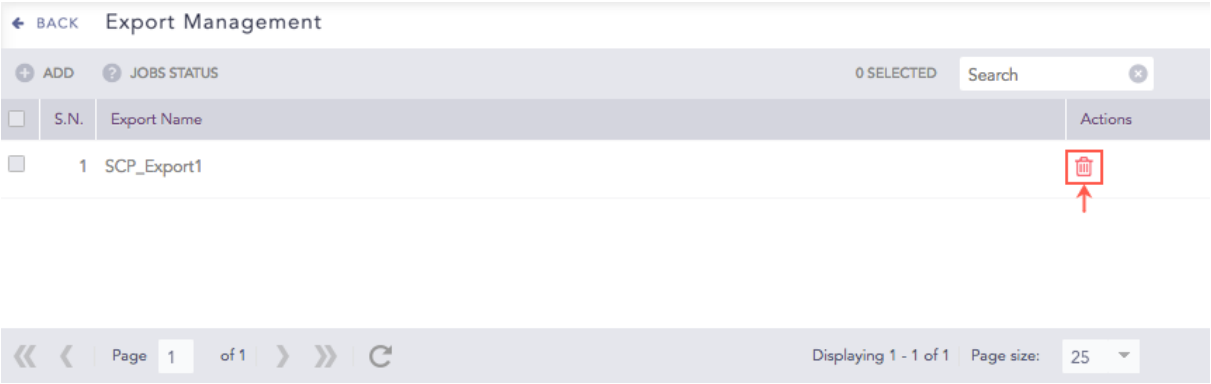
Job Status

This section displays the **Name**, **Type**, **Status**, and **Remarks** of the export log status along with their **Actions**.



Deleting an Export

1. Go to `Settings >> Configuration` from the navigation bar and click **Export Management**.
2. Click the **Delete** icon under the **Actions** column of the concerned export.


BACK
Export Management
ADD
JOBS STATUS
0 SELECTED
Search
S.N.
Export Name
Actions
1
SCP_Export1
Page
1
of 1
Displaying 1 - 1 of 1
Page size:
25

3. Click **Yes**.

Sync

Sync allows you to export and import various configurations which can be synchronized with other SLS(s). It consists of primary and secondary settings.

You can sync the following settings.

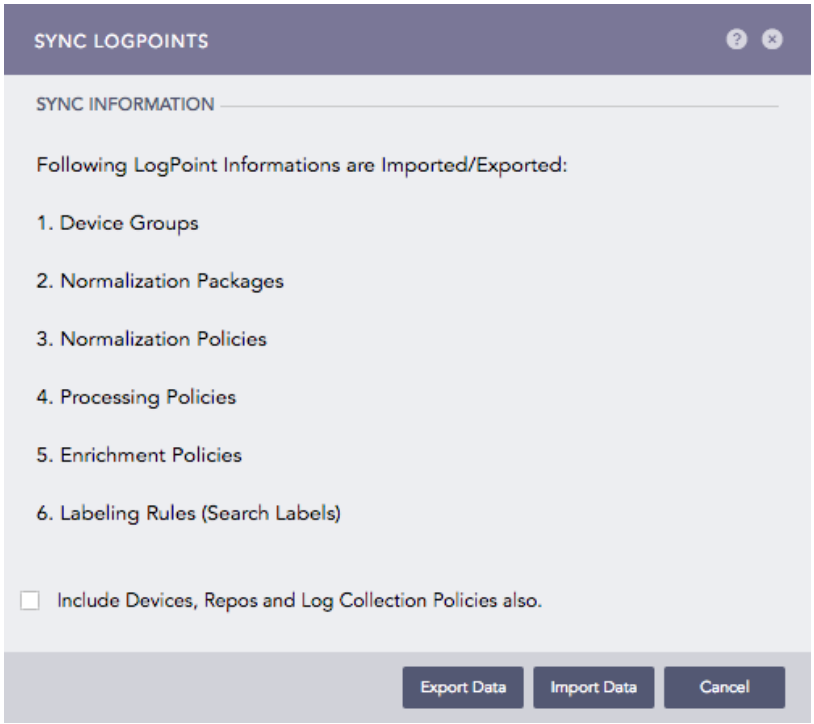
Primary Settings	Secondary Settings
Device Groups	Devices
Normalization Packages	Repos
Normalization Policies	Log Collection Policies
Processing Policies	
Enrichment Policies	
Labeling Rules (Search Labels)	

Using Sync

Before syncing SLSs, there are a few things you should do.

Before importing configurations, install **CSV Enrichment Source** and configure the enrichment source with the same CSV source file in the same way as the SLS used to sync. You should also install **ODBC Enrichment Source**, **LDAP Enrichment Source**, and **Threat Intelligence Enrichment Source**, and should have the exact configuration in each source.

1. Go to `Settings >> System Settings` from the navigation bar and click **Sync**.



2. Select the **Include Devices, Repos, and Log Collection Policies also** if you want to include their configurations as well.

3. Click **Export Data** to export configurations. All the selected configurations are downloaded in your machine in a .json file. In addition, the .json file also includes all configurations about:
   - **User Accounts**, except the **Incident User Groups**.
   - **Configuration**, except the **Distributed Collectors**, **Raw Syslog Forwarder**, /**Distributed SLSs**, and **Export Management**.
   - **Knowledge Base**.
4. Logon to the SLS where you want the same configuration. Go to `Settings >> System Settings` from the navigation bar and click **Sync**.
5. Select the **Include Devices, Repos, and Log Collection Policies also**.
6. Click **Import Data** to import configurations.
   - Click **Import Data**.
   - Browse for the JSON file and click **Upload**.

After successfully importing the data, all the settings saved in the uploaded file are replicated in your machine.

> **NOTE**
> While using the **Import Data**, you can manually remove the configurations from the JSON file according to your requirements. However, remember not to remove important data.

Further reading

Additional information and answers to questions you may have about SLS are available in the Stormshield knowledge base (authentication required).

documentation@stormshield.eu