THALES

# Splunk: Integration Guide

## THALES LUNA HSM

## Document Information

| | |
|---|---|
| **Document Part Number** | 007-013239-001 |
| **Revision** | C |
| **Release Date** | 6 December 2021 |

## Trademarks, Copyrights, and Third-Party Software

# CONTENTS

# Overview

This document guides administrators through the steps for setting up Splunk to monitor Luna HSM devices. Splunk monitors Luna HSMs using syslog and SNMP poll requests, allowing the user to monitor the device status and availability. This provides administrators and users insights into the operational performance and business results.

Integrating the Luna HSM with the Splunk application makes it simple to collect, analyze, and act upon the data generated by the syslog and SNMP poll requests on the Luna HSM appliances. The benefits of using the Splunk application to monitor the status of the Luna Network HSM include:

- Monitor the health status and availability of Luna Network HSM appliances.
- Collect and monitor graphical and statistical information about Luna HSM utilization.
- Configure user alerts for sensors.
- Monitor HSM errors, Lush command frequency, and NTLS response code.
- Gather partition-based information on Luna HSM appliances.

This guide contains the following sections:



# Certified platforms

The following platforms are certified for integrating Splunk with Luna HSM:

| Luna HSM App | Splunk Version | Platforms |
|---|---|---|
| Thales Luna HSM app for Splunk | 8.2.x | RHEL 8 |

**Luna HSM:** Luna HSM appliances are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing. Luna HSM on premise offerings include the Luna Network HSM, Luna PCIe HSM, and Luna USB HSMs. Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic.

# Configuring Splunk to monitor Luna HSM

Install and set up the Splunk Luna HSM App, using the following steps:

> Add custom MIBs to Splunk Modular Input

> Start using Luna HSM App

## Install Luna HSM App

To install Luna HSM App, complete the following activities:

> Luna HSM App installation prerequisites

> Post-installation requirements

> Install Luna HSM App in Splunk

### Luna HSM App installation prerequisites

Before installing the Luna HSM App, ensure that you have completed the following tasks on the host system:

1. Download and install Splunk Enterprise Server.

   **NOTE:** The Luna HSM App is supported by Splunk Enterprise on RHEL Linux and Cent OS platforms.

2. Ensure that the Luna HSM appliances you intend to monitor each have a unique hostname. The hostname is used to identify the appliance in the application logs.
3. Deploy Splunk SNMP modular input version 1.7.8 on the Splunk server.

   **NOTE:** The steps for deployment of SNMP are available at the following URL: https://splunkbase.splunk.com/app/1537/#/details

4. Configure Syslog and SNMP poll/trap on the Luna HSM Appliance.
   - To configure syslog on splunk server, run the following command on your Luna Network appliance.
     ```
     syslog re add -h < Splunk_server_IP > -pr tcp -po 7171
     ```
   - To configure and enable SNMP traps/poll on Luna appliance, run the following steps. Each step corresponds to an administrative command via the Luna shell.

   a. Add an SNMP user to the system:

      ```
      sysconf snmp user add -s <Security_Username > -authPassword < PASSWORD > -
      authProtocol < Auth_protocol > -privPassword < PASSWORD > -privProtocol <
      Priviledge_protocol >
      ```

   b. Enable SNMP:

      ```
      sysconf snmp enable
      ```

   c. Set the SNMP trap parameters for the SNMP user:

      ```
      sysconf snmp trap set -h < Splunk_server_IP > -s <Security_Username > -e <
      engineID > -authpr SHA -authpw < PASSWORD > -privPr AES -privPwd <PASSWORD>
      ```

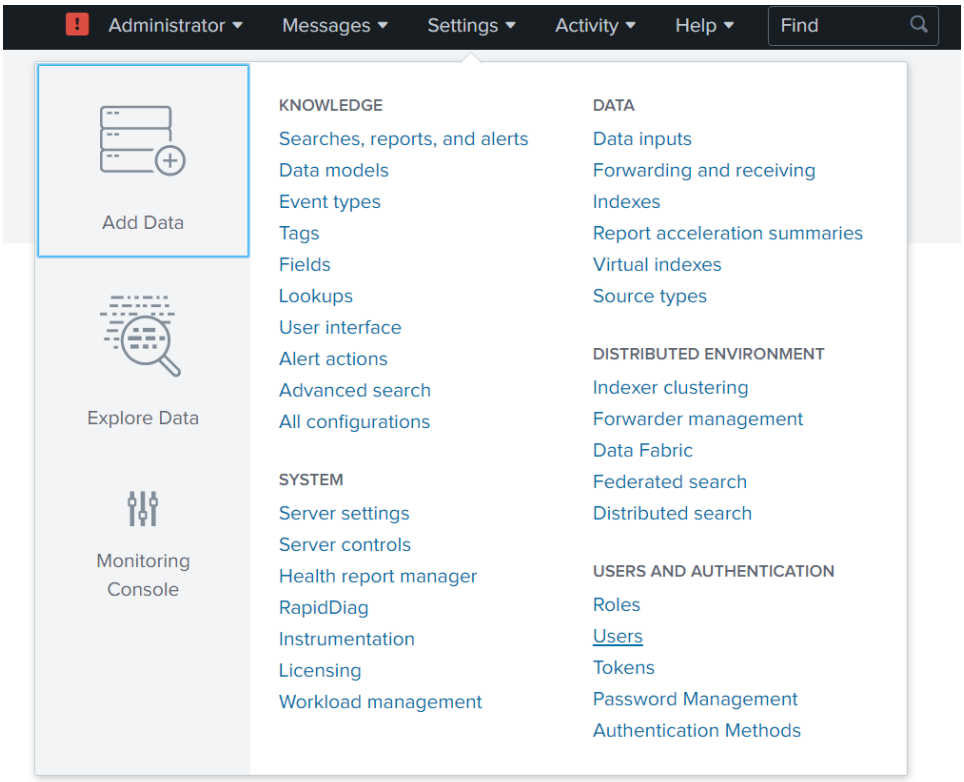
   d. Enable SNMP traps:

      ```
      sysconf snmp trap enable
      ```

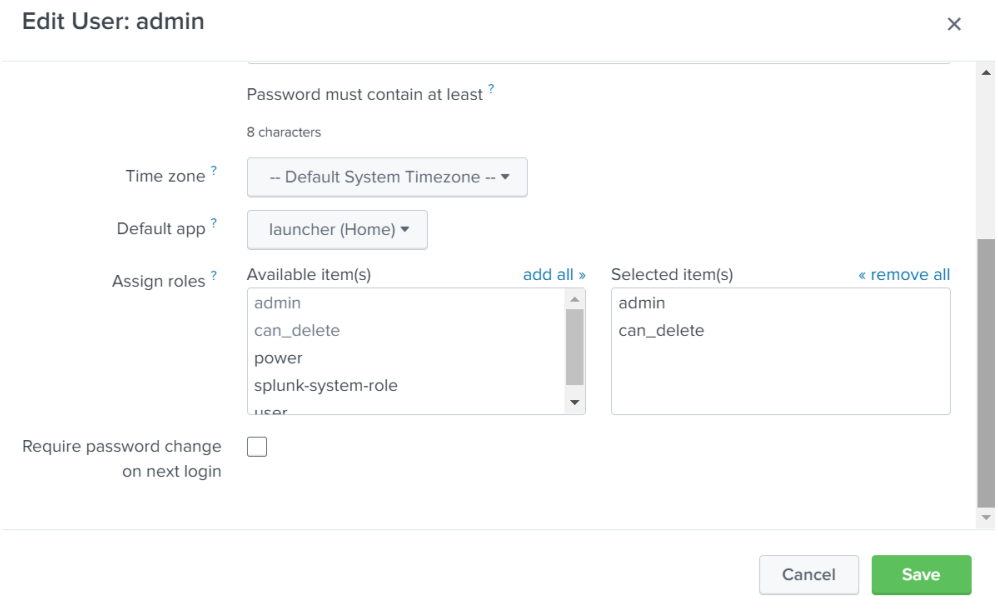
### Post-installation requirements

Ensure you configure the following settings on the Splunk Web interface after downloading and installing the Luna HSM App.

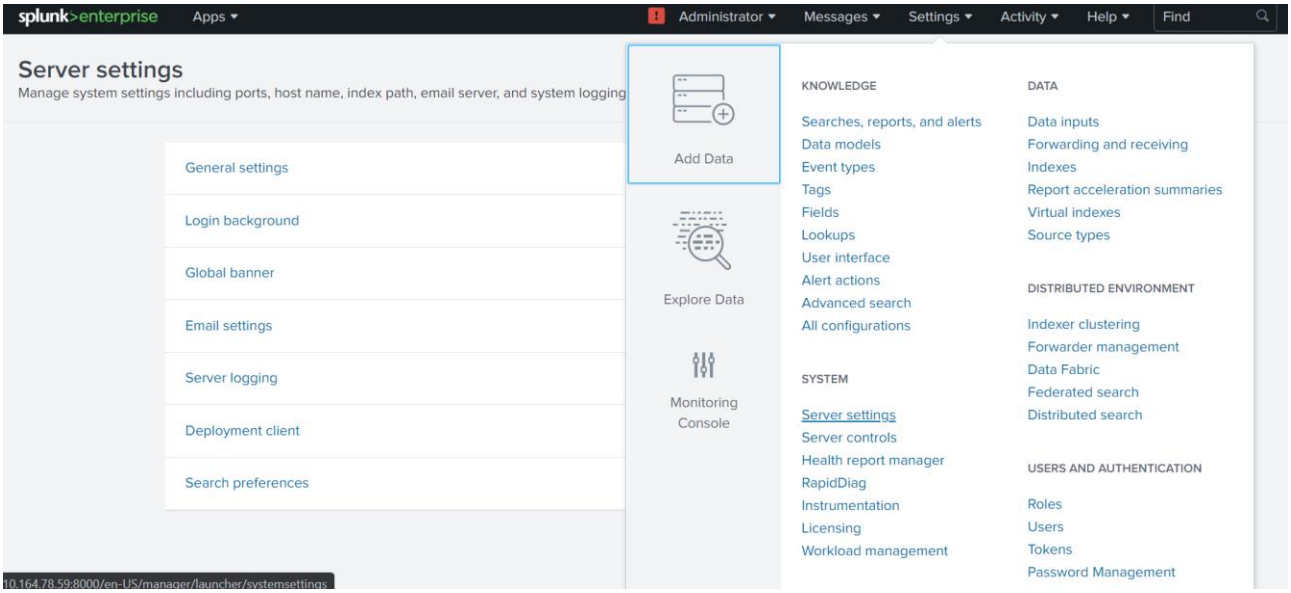
1. Open Splunk web page, click **Settings** and then click **Add Data** from the left pane.
2. Select Users under USERS AND AUTHENTICATION.




3. Click on administrator user that you have created and under **Assign Roles,** select **can_delete**.



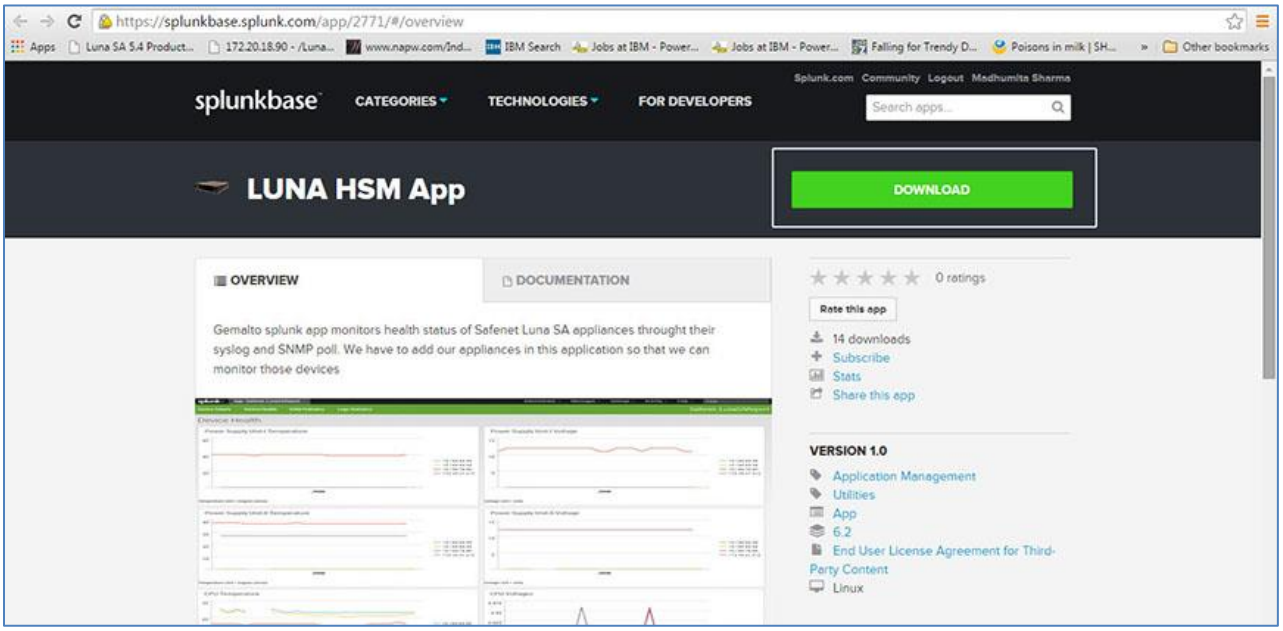
4. Click **Save.**
5. Make sure that you configure the email settings to send alerts on sensitive operations to users by clicking **Settings** – **Server settings** under **Server settings** – **Email settings** on the Splunk Web interface.




### Install Luna HSM App in Splunk

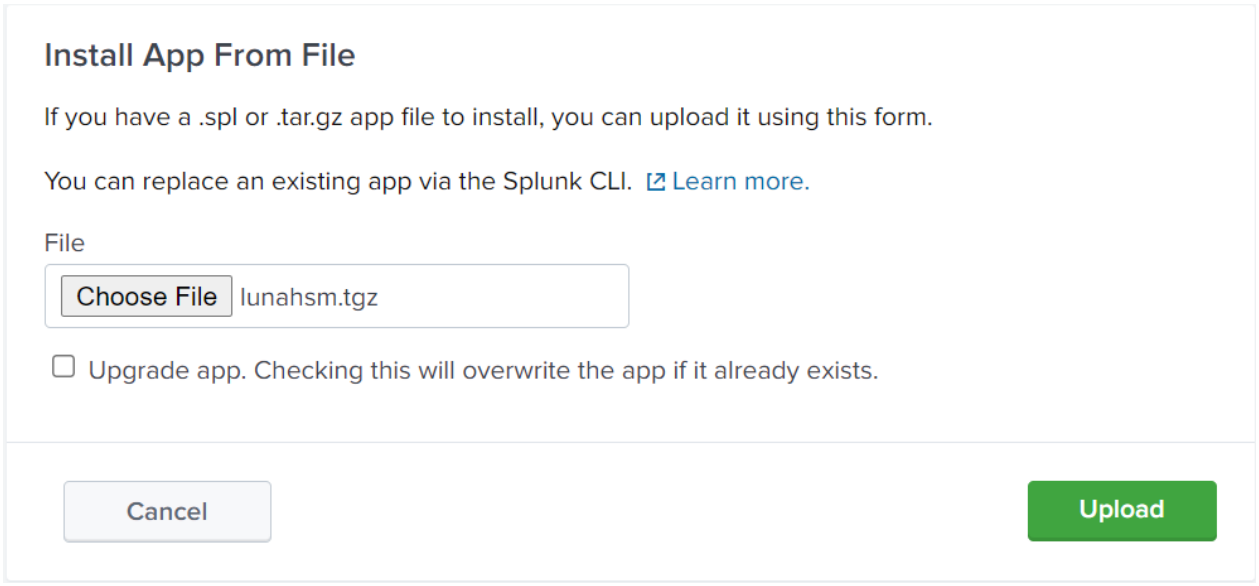
This section details the instructions on downloading the Luna HSM App.

1. Download the **Luna HSM App** application from the Splunk App Page. Accept the license agreements and download the **lunahsm.tgz** file.

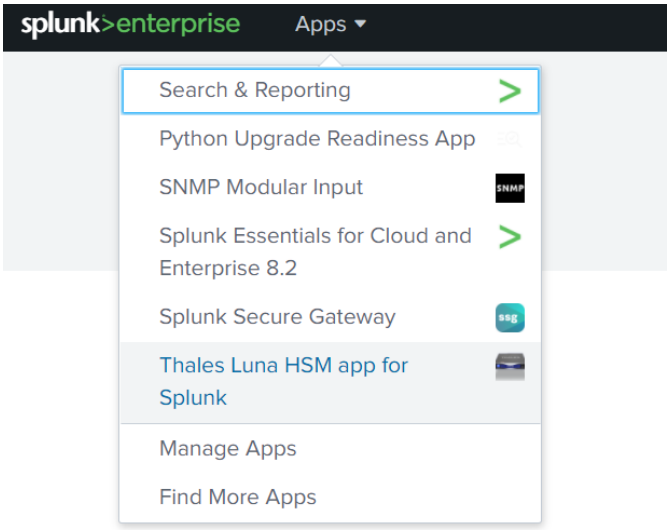



2. Log in to the Splunk web interface and click on **App – Manage Apps** to open the Apps Management page in Manager.

3. Click the **Install app from file** button, locate the downloaded **lunahsm.tgz** file, and then click **Upload**.




4. Restart the Splunk server after the file gets uploaded.
5. Verify the application installation. It should be included in the list of apps installed within the Splunk Web Interface. For example: http://IP address:8000.

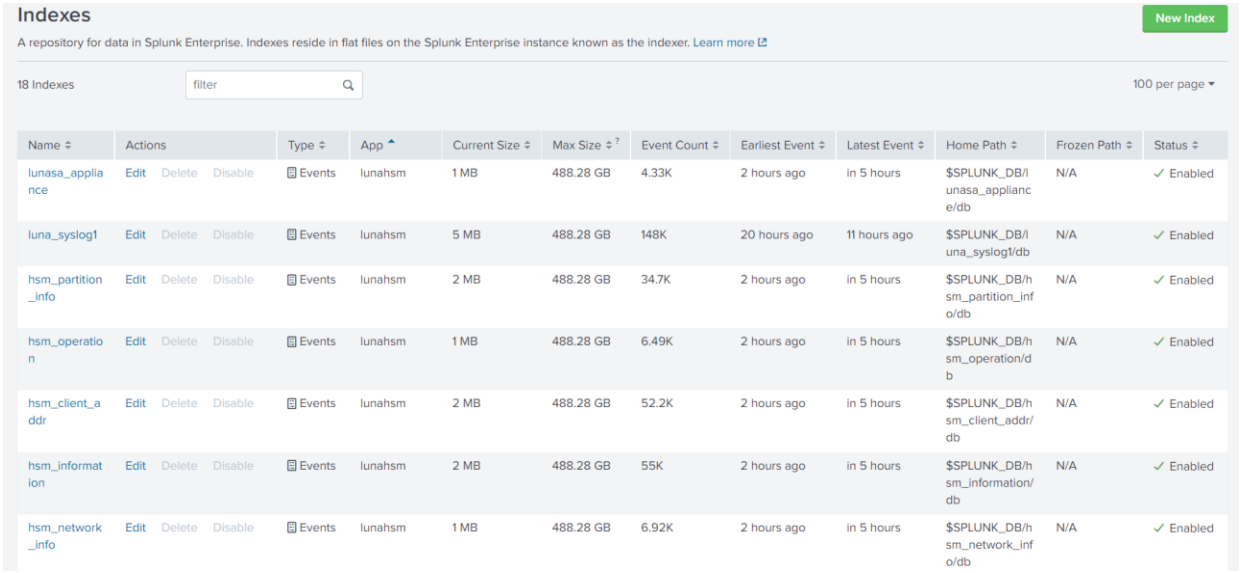


## Verify Luna HSM App installation

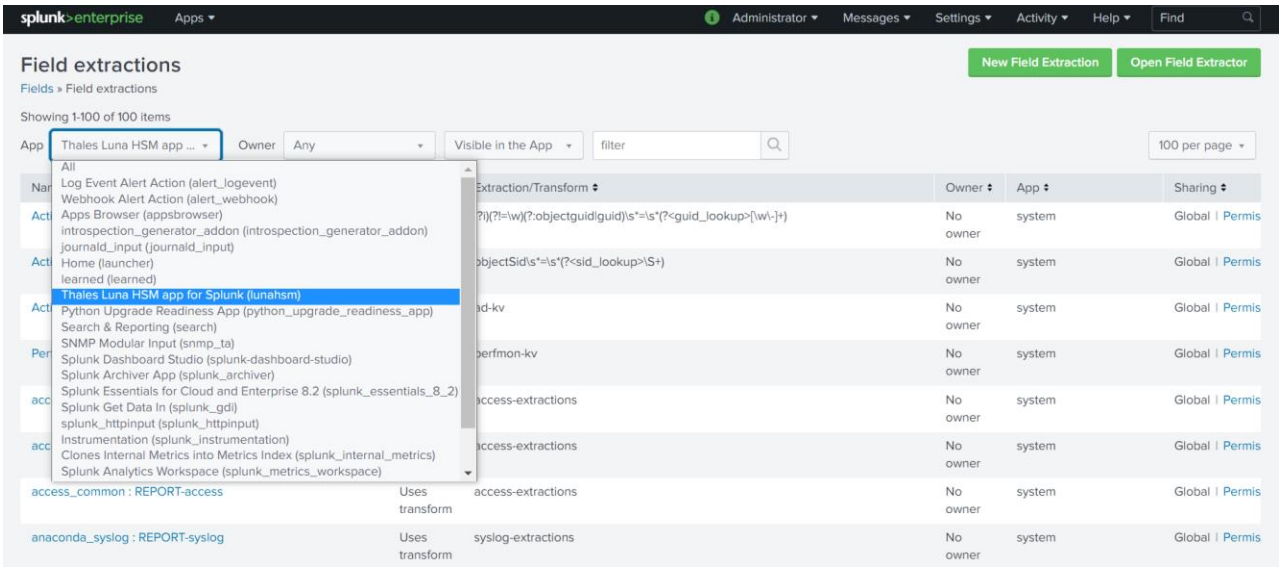
To install Luna HSM App correctly, ensure that the following conditions are met:

> A new application, Thales Luna HSM App for Splunk, exists in the applications list.

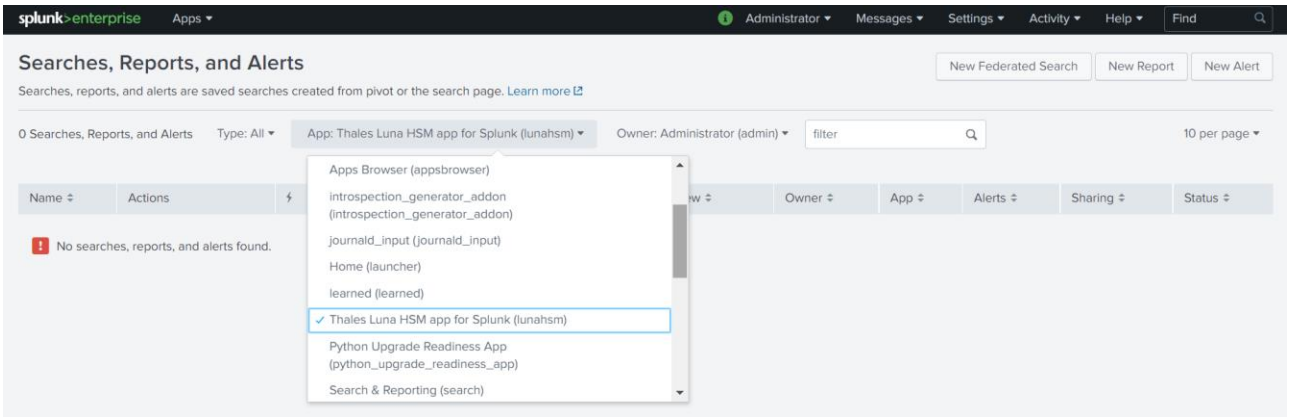
> New indexes named lunasa_appliance, luna_syslog1, hsm_partition_info, hsm_operation, hsm_client_addr, hsm_information and hsm_network_info exist in the index list section.



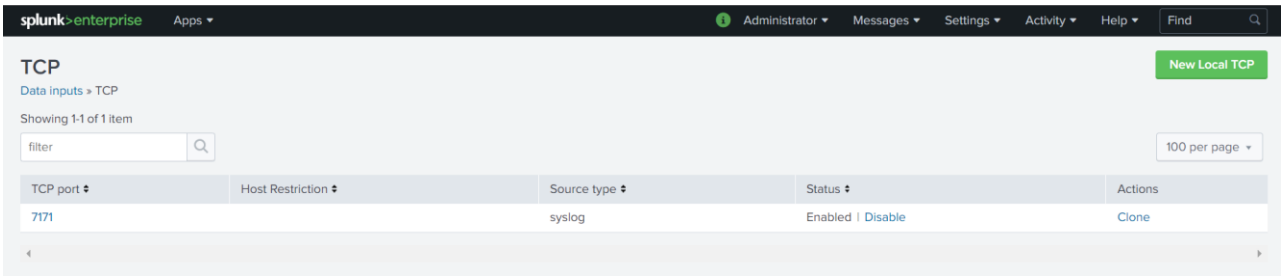

> The Splunk **Setting > Fields > Fields extractions** section displays a section for the Thales Luna HSM app for Splunk.



> New alerts are displayed in **Setting > Search, Reports and Alert** section for the Thales Luna HSM app for Splunk.




> The **Setting > Data Inputs > TCP** Section displays a TCP input type. The TCP port should be 7171.




Refer to Splunk Documentation for more information about verifying these values.

## Add Custom MIBs to Splunk Modular Input

Deploy the PyCrytpo package (pip install pycryptodomex) before adding custom MIBs to the Splunk Modular Input. Refer to https://www.baboonbones.com/php/markdown.php?document=snmp/README.md for more information about adding custom MIBs to SNMP Modular Input. Luna HSM App requires the following custom MIBs in python (.py) format:

> SAFENET-HSM-MIB

> LM-SENSORS-MIB

> CHRYSALIS-UTSP-MIB

> SAFENET-APPLIANCE-MIB

> SAFENET-GLOBAL-MIB

> SNMPv2-SMI

**NOTE:** Ensure that Thales provides these custom MIBs files in python (.py) as well as in the .txt format with this application.

Copy the mibs.py files from the location MIBs present in the downloaded Luna App for Splunk zip file and paste them at "$SPLUNK_HOME/etc/apps/snmp_ta/bin/mibs/user_python_mibs" or regenerate python files out of the

custom MIB txt files using the `SPLUNK_HOME/etc/apps/snmp_ta/bin/mibdump.py` script available with Splunk Modular Input (click the link here to refer to the process as defined under the section **`Adding Custom MIBs`** in Splunk Modular Input documentation).

## Start using Luna HSM App

After the successful installation of the Thales Luna HSM app for Splunk, you can configure, run, or maintain the application as a service. Luna HSM App usage operations include the following:

- **Adding a New Luna Device**: Configure a Luna HSM Appliance with the Splunk Luna HSM App. The **Add Luna Appliance** page on the Splunk web interface allows you to add a Luna HSM appliance in an easy way.
- **Monitoring Luna HSM Appliances**: Monitor a Luna HSM appliance for usage, availability and health status, etc. enabling you to gain end-to-end visibility across all the components of your appliance.
- **Configuring Settings for Server and Authentication**: Configure user roles and email settings for setting alerts on sensitive operations.

# Adding and removing Luna HSM

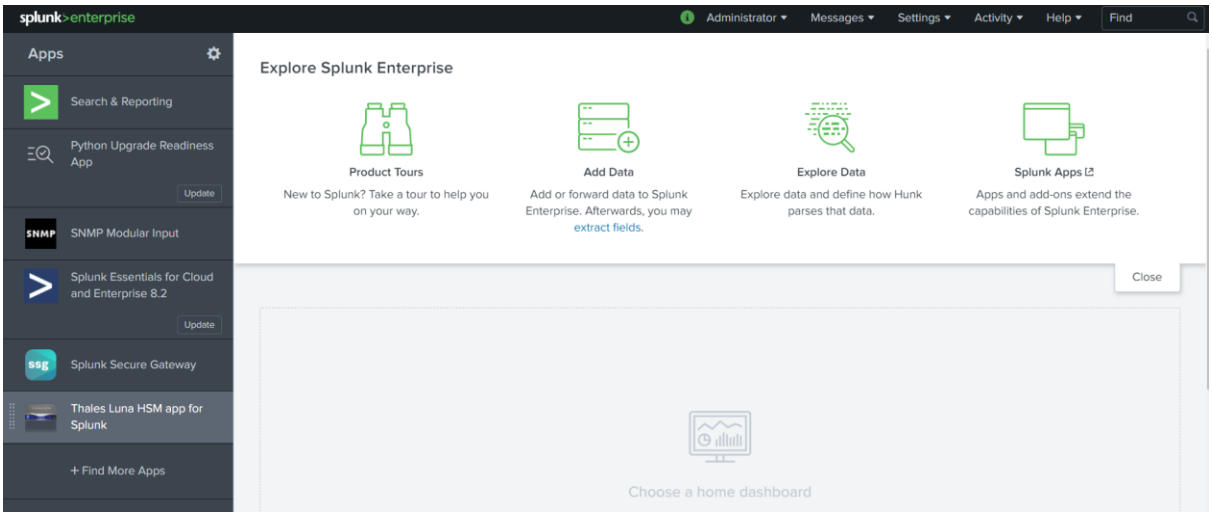
To monitor a Luna HSM using the Splunk application, you must provide Splunk access to the Luna HSM. If you would like to stop monitoring a Luna HSM, you can remove the device from the Splunk application. This section contains the following topics:



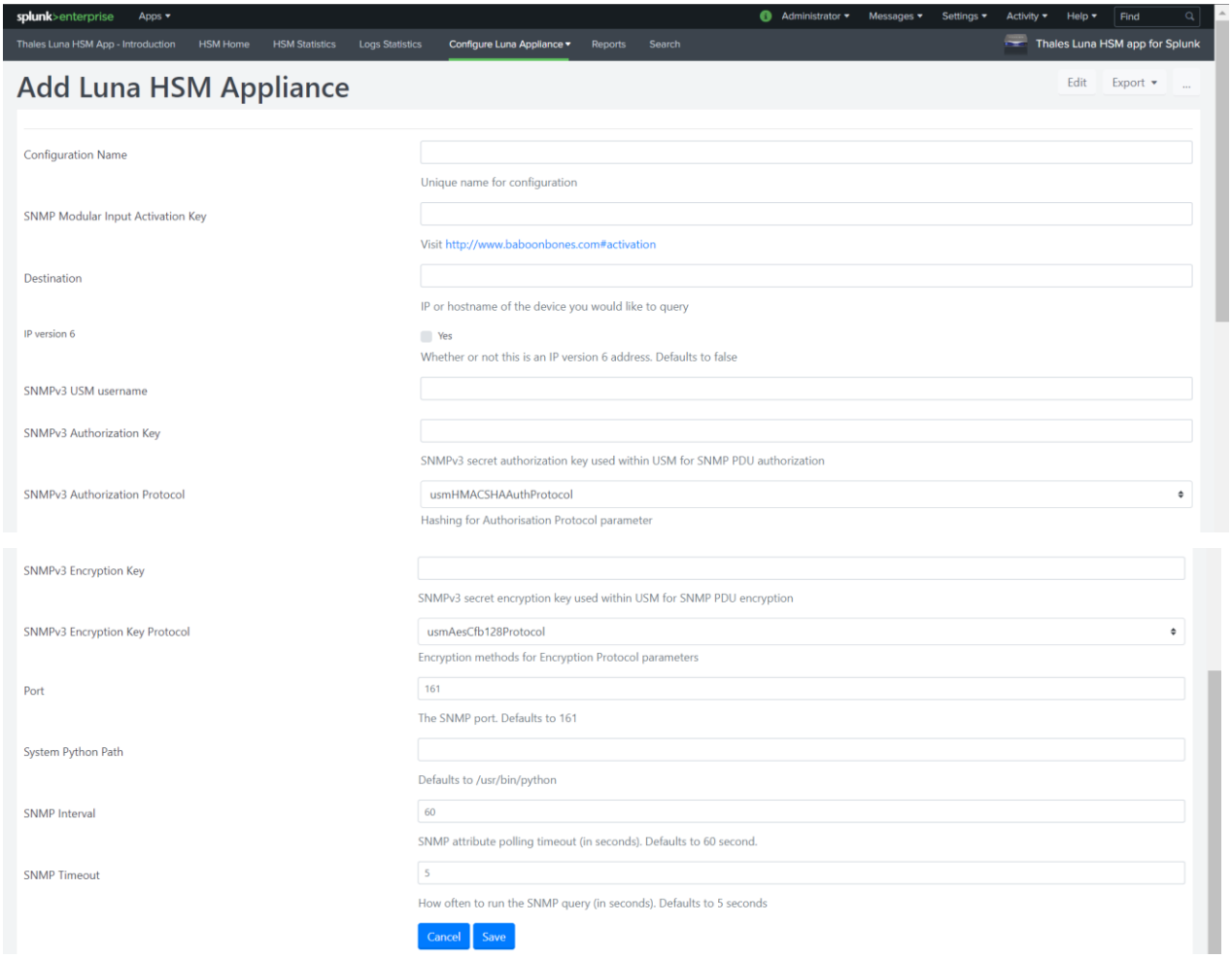
## Add a Luna HSM device

To add a Luna HSM device

1. Log in to the Splunk web interface as an Administrator user.
2. Click **Thales Luna HSM app for Splunk**.



3. Click **Configure Luna Appliance** and select **Add Luna HSM Appliance**.




4. Enter your information on the **Add Luna HSM Appliance** page, as explained below:

   a. **Configuration Name** : Enter the name of your SNMP input for the Luna device. You can select a random name that is unique for each appliance.

   b. **SNMP Modular Input Activation Key :** Get activation key for SNMP Modular from https://www.baboonbones.com/#activation

   c. **IP Version 6**: Mark this checkbox, if your device support IPv6.

   d. **Destination**: IP or hostname of the HSM device you would like to query.

   e. **SNMPv3 USM username**: Enter the username you created on your Luna appliance while configuring SNMP.

   f. **SNMPv3 Authorization Key**: Enter the SNMPv3 secret authorization key you used during SNMP user creation on the Luna device.

   g. **SNMPv3 Encryption Key**: Enter the SNMPv3 secret encryption key you used during SNMP user creation on the Luna device.

   h. **SNMPv3 Authorization Protocol**: Select the Authorization protocol name corresponding to the key you used during SNMP user creation on Luna Box.

   i. **SNMPv3 Encryption Key Protocol**: Select the Encryption protocol name corresponding to the key you used during SNMP user creation on Luna Box.

j. **System Python Path :** Defaults to /usr/bin/python**.** Change path if you have python installed at different location.

k. **Port**: Enter the SNMP polling port available on Luna appliance. The default port is **161**.

l. **SNMP Interval**: Enter the time interval (in seconds) to determine the frequency of SNMP queries. It is recommended to set it at 300 seconds. The default value is **60** seconds.

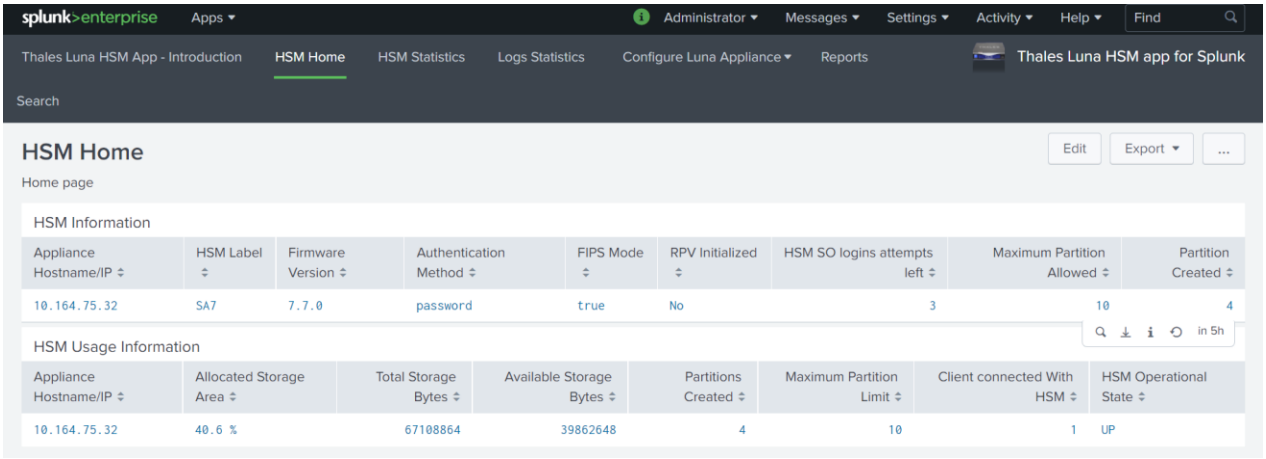
m. **SNMP Timeout :** Enter how often to run the SNMP query (in seconds). Defaults to 5 seconds.

5. Click **Save** to continue.

6. Restart Splunk service

```
# /opt/splunk/bin/splunk restart
```

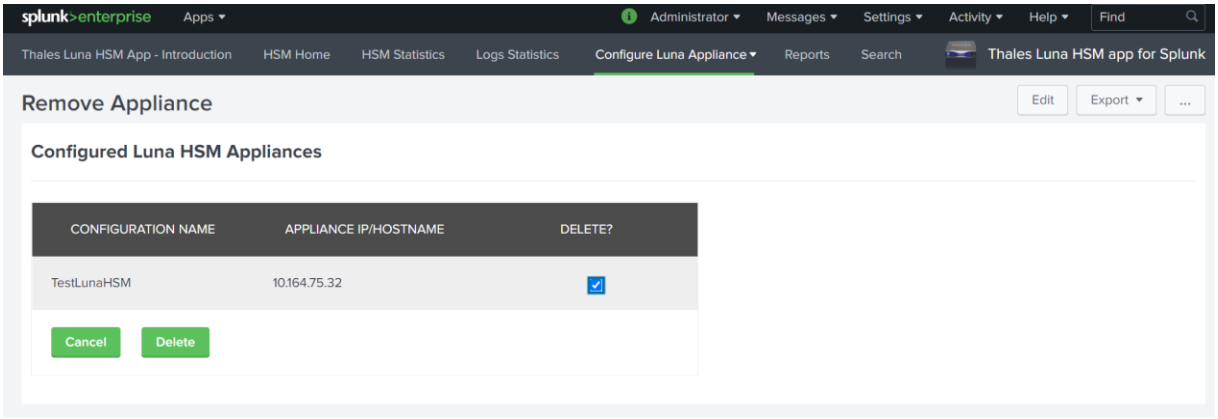
The Luna Network HSM appliance is now configured with Luna HSM App on the Splunk web interface. Verify the Luna Network HSM is available in the **HSM Home** tab.




## Remove a Luna HSM device

Remove Luna HSM appliances that you do not want Splunk to monitor. To remove a Luna device:

7. On the Splunk interface for Luna HSM App click Click **Configure Luna Appliance** and select **Remove Luna Device.** The **Remove Appliance** screen displays.




8. Select the Luna Network HSM appliance that you want to remove from the list of configured devices, then click **Delete.**

9. Restart Splunk service

```
# /opt/splunk/bin/splunk restart
```

> **NOTE:** It can take some time to remove the HSM information after deleting it.

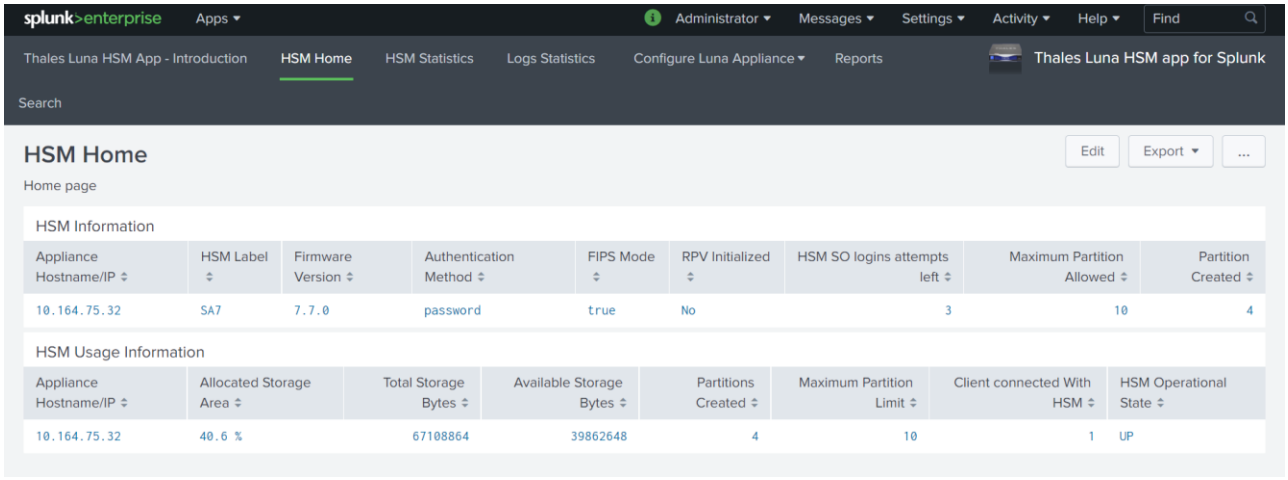
# Monitoring Luna HSM devices

You can use the Luna HSM App for monitoring the health status, logs, availability, appliances operations and status of Luna HSM devices. Using the syslog and SNMP poll request, you can monitor the Luna HSM for the following purposes:

- HSM Inventory
- HSM Health
- HSM Statistics
- Log Statistics

## HSM Inventory

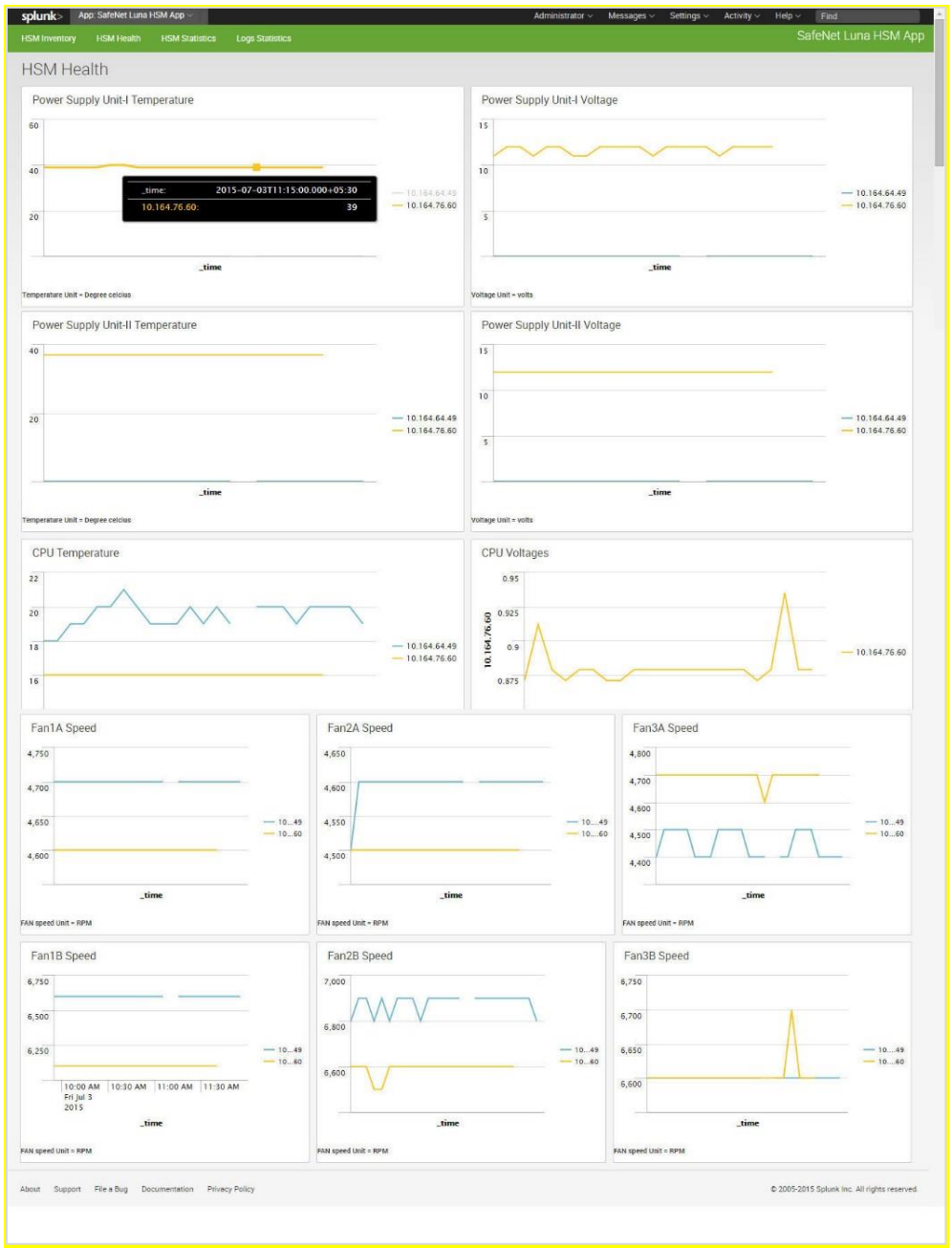
The HSM Inventory tab on Luna HSM app provides information on the Luna HSM appliances configured with the application. Click the **HSM Home** for inventory which displays **HSM Information** panel and **HSM Usage Information** panel.




- **HSM Information:** This panel provides appliance details, including IP Address, HSM Label, Firmware Version, Authentication Method, FIPS Mode, RPV Initialized, HSM SO logins attempts left, Maximum Partition Allowed, and Partition Created.
- **HSM Usage Information:** This panel provides information regarding storage space and partition, including Appliance Hostname/IP, Allocated Storage Area, Total Storage Bytes, Available Storage Bytes, Partitions Created, Maximum Partition Limit, Client connected With HSM, and HSM Operational State.

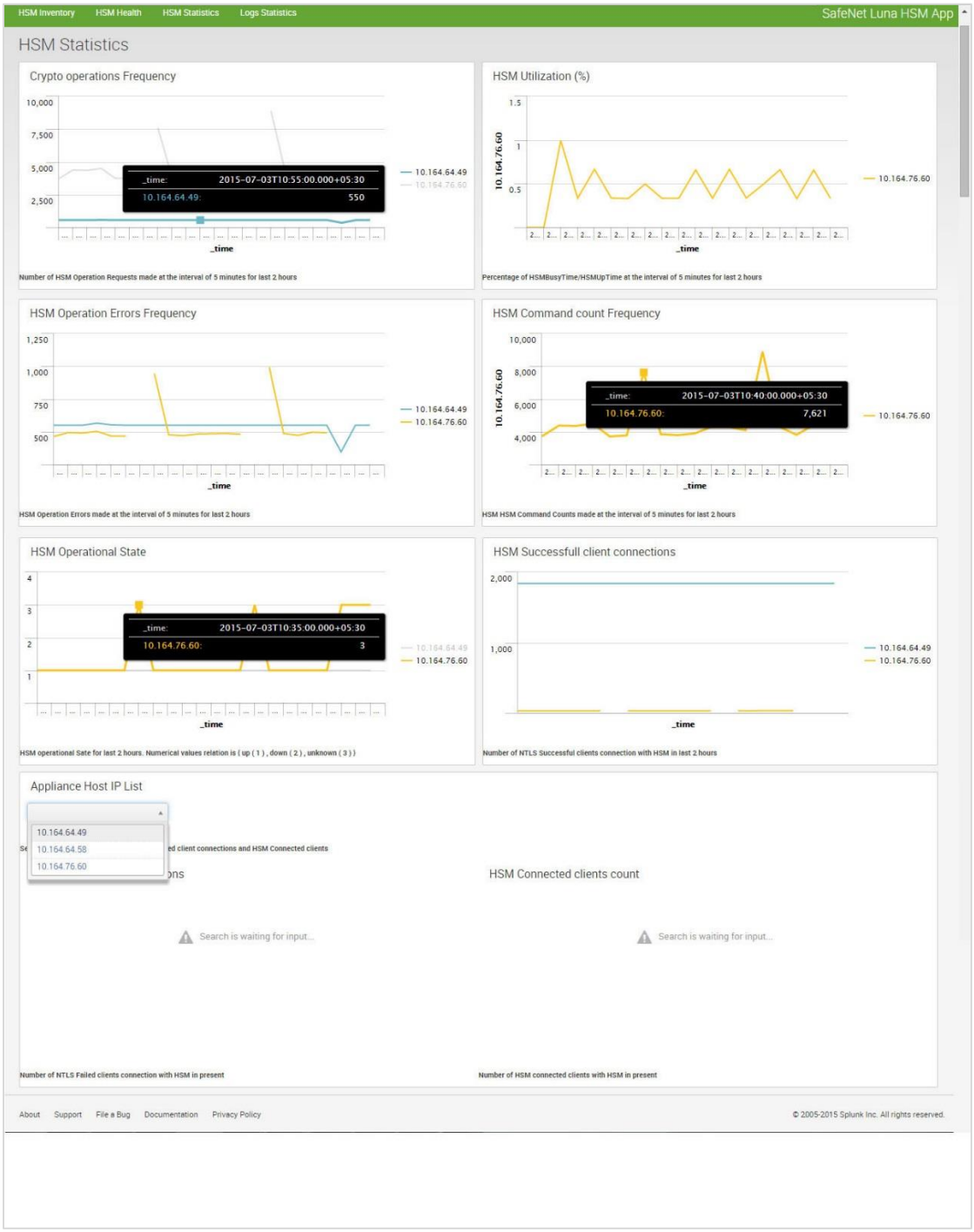
## HSM Health

Click the **HSM Health** tab to view statistical information on your appliance at various hours of a particular date, including **Power Supply (CPU Temperature, Voltage)** and **Fan Speed**.



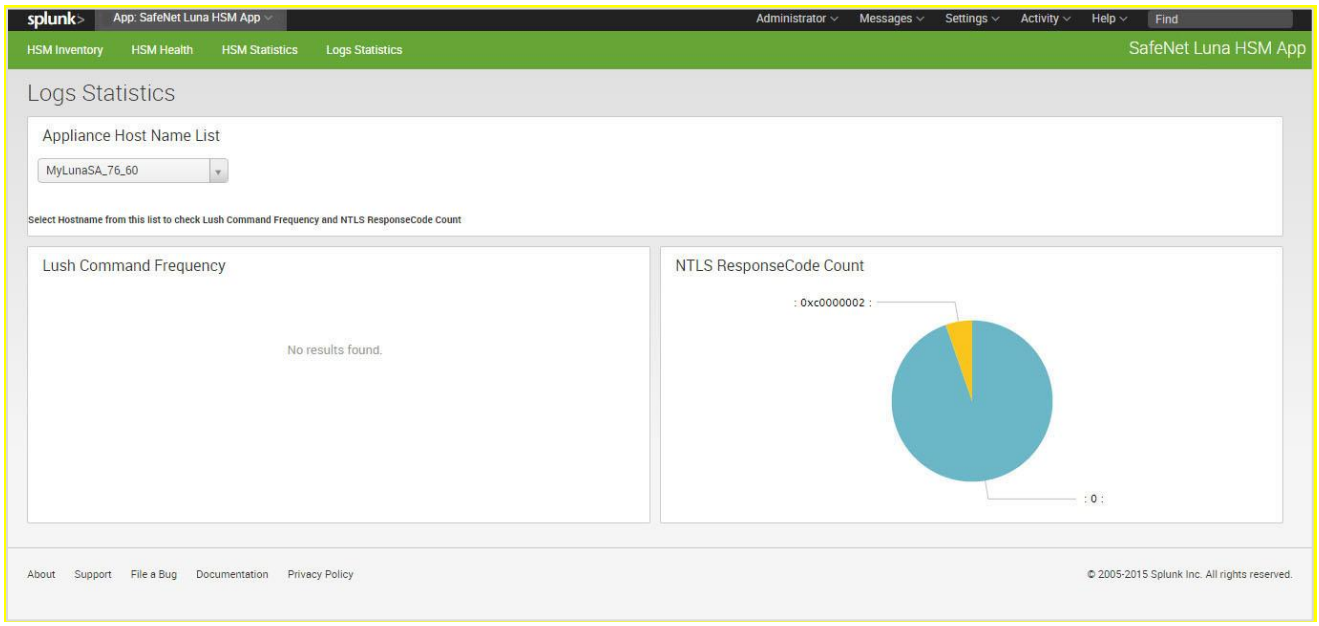
## HSM Statistics

Click the **HSM Statistics** tab to view details such as **Crypto operations frequency**, **HSM Utilization**, **HSM Operations Error Frequency**, **HSM Command count frequency**, **HSM Operational state**, **HSM Successful client connections, HSM Failed Client Connections** and **HSM Connected Clients**. Select the desired IP from the **Select Appliance** drop-down to view the statistics of a particular appliance.



## Log Statistics

Click the **Log Statistics** tab to monitor the **Lush Command Frequency** and **NTLS ResponseCode Count** of your appliance.



# Contacting customer support

If you encounter a problem during this integration, contact your supplier or Thales Customer Support. Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

## Customer support portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is a database where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable repository of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

## Telephone support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

## Email support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.