Splunk

Integration Guide

gemalto
security to be free

Document Part Number: 007-013239-001, Rev. B

Release Date: January 2019

Contents

Preface

Scope

This document guides administrators through the steps for setting up Splunk to monitor a SafeNet Luna HSM appliance. Splunk monitors the SafeNet Luna HSM using syslog and SNMP poll requests, allowing the user to monitor the appliances status and availability.

Document Conventions

This section provides information on the conventions used in this template.

Notes

Notes are used to alert you to important or helpful information. These elements use the following format:

NOTE: Take note. Contains important or helpful information.

Cautions

Cautions are used to alert you to important information that may help prevent unexpected results or data loss. These elements use the following format:

CAUTION: Exercise caution. Caution alerts contain important information that may help prevent unexpected results or data loss.

Warnings

Warnings are used to alert you to the potential for catastrophic data loss or personal injury. These elements use the following format:

WARNING: Be extremely careful and obey all safety and security measures. In this situation you might do something that could result in catastrophic data loss or personal injury.

Command Syntax and Typeface Conventions

Convention	Description
bold	The bold attribute is used to indicate the following: • Command-line commands and options (Type dir /p.) • Button names (Click Save As.) • Check box and radio button names (Select the Print Duplex check box.) • Window titles (On the Protect Document window, click Yes.)

Convention	Description
	• Field names (User Name: Enter the name of the user.) • Menu names (On the File menu, click Save.) (Click Menu > Go To > Folders.) • User input (In the Date box, type April 1.)
italic	The italic attribute is used for emphasis or to indicate a related document. (See the *Installation Guide* for more information.)
`Consolas`	Denotes syntax, prompts, and code examples.

Support Contacts

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.	

1
Introduction

Overview

This document guides administrators through the steps for setting up Splunk to monitor a SafeNet Luna HSM appliance. Splunk monitors the SafeNet Network Luna HSM using syslog and SNMP poll requests, allowing the user to monitor the appliances status and availability.

Integrating the SafeNet 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 SafeNet Network Luna HSM appliances. This provides administrators and users insights into the appliances operational performance and business results.

The benefits of using the Splunk application to monitor the status of the SafeNet Luna HSM include the following:

- Efficiently monitor the health status and availability of SafeNet Luna Network HSM appliances.
- Collect and monitor graphical and statistical information about SafeNet 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 document comprises the following chapters:

- Configuring Splunk to Monitor SafeNet HSM
- Adding and Removing SafeNet Luna HSM
- Monitoring SafeNet Luna HSM Appliances

Third Party Application Details

This integration uses the following third party application:

- Splunk

Supported Platforms

List of the platforms which are tested with the following HSMs:

SafeNet Luna HSM: is a standalone network-attached appliances that physically and logically secure cryptographic keys and cryptographic processing. The purpose of an HSM is to protect sensitive data from being stolen by providing a highly secure operation structure. HSMs are fully contained and complete solutions for cryptographic processing, key generation, and key storage.

This integration is supported with SafeNet Luna HSM on the following operating systems:

Luna HSM App	Platforms
SafeNet Splunk App for LUNA SA	RHEL

2
Configuring Splunk to Monitor SafeNet HSM

To configure Splunk to monitor a SafeNet Luna HSM device, install and setup the Splunk Luna HSM App. Complete the following steps:

- Installing Luna HSM App
- Adding Custom MIBs to Splunk Modular Input
- Getting Started Using Luna HSM App

Installing Luna HSM App

The following section details the necessary prerequisites and procedures for installing the SafeNet Luna HSM App. It contains the following sections:

- Luna HSM App Installation Prerequisites
- Post-Installation Requirements
- Installing the 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 SafeNet 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 1.2.7 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 SafeNet Luna HSM Appliance.
   - To configure syslog on splunk server, run the command below 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 set of 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. Grant the **can_delete** role to the Splunk Admin User. Open the Splunk Web Interface and select **Access Controls > Users**. Set **can_delete** in the **Settings** section.
2. This can be assigned on the splunk web interface in the **Settings** section under **Access controls » Users**.
3. Make sure that you configure the Email settings to send alerts on sensitive operations to users. You can configure the Email Settings in the **Settings** section under **Server settings » Email settings** on the Splunk Web interface.

Installing the 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 **luna-hsm-app.tgz** file.

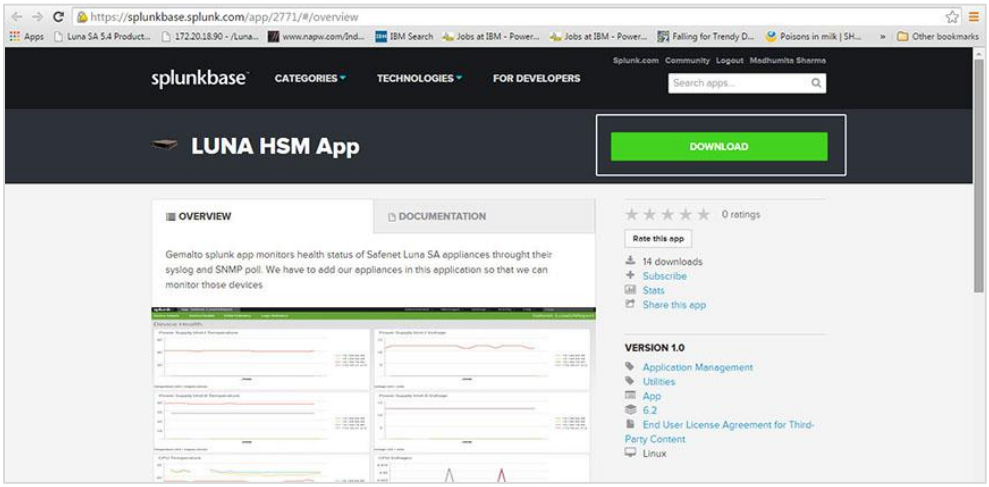

Figure 1: Luna HSM App Download

2. Login to the Splunk web interface, click on **App -> Manage Apps** to open the Apps Management page in Manager.

3. Click the **Install app from file** button, locate the downloaded file (**deviceinformation.spl** available in the **luna-hsm-app.tgz** file) and click **Upload**.
4. Restart the splunk server after the file upload. The application deploys.
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

Verifying the Luna HSM App installation

If the following conditions are met, the **Luna HSM App** is installed correctly:

- A new application, Luna HSM App, exists in the applications list.
- New indexes named lunasa_appliance, hsm_operation, hsm_client_addr, hsm_partition_info and luna_syslog1 exist in the index list section.
- The Splunk Setting > Fields > Fields extraction section displays a section for the Luna HSM App.
- New alerts display in Setting > Search, Reports and Alert section for the Luna HSM App.
- The Setting > Data Inputs > TCP Section displays a TCP input type. The TCP port should be 7171.

Refer Splunk Documentation for more information about verifying these values.

Adding Custom MIBs to Splunk Modular Input

Ensure you deploy the PyCrytpo package before you begin adding custom MIBs to the Splunk Modular Input. Refer to the section “Building and Installing PyCrypto” in the SNMP Modular Input documentation at https://splunkbase.splunk.com/app/1537/#/documentation for more information.

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
- RFC1213-MIB*
- LM-SENSORS-MIB*

*These are the open source MIB files and required to be downloaded from internet.

NOTE: Ensure SafeNet 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 "$SPLUNK_HOME$/etc/apps/deviceinformation/bin" and paste them at "$SPLUNK_HOME/etc/apps/snmp_ta/bin/mibs " or regenerate python files out of the custom MIB txt files using the **`build-pysnmp-mib`** method 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).

Getting Started Using Luna HSM App

After the successful installation of the Luna HSM App, 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 SafeNet Luna HSM Appliance with the Splunk Luna HSM App. The **Add a New 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 SafeNet 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.

3
Adding and Removing SafeNet Luna HSM

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

Adding a Luna Device

To monitor a SafeNet Luna HSM using Splunk you must provide Splunk access to the SafeNet Lune HSM.

To add a Luna HSM device

1. Login to the Splunk web interface as an Administrator user.
2. Click **SafeNet Luna HSM App**.

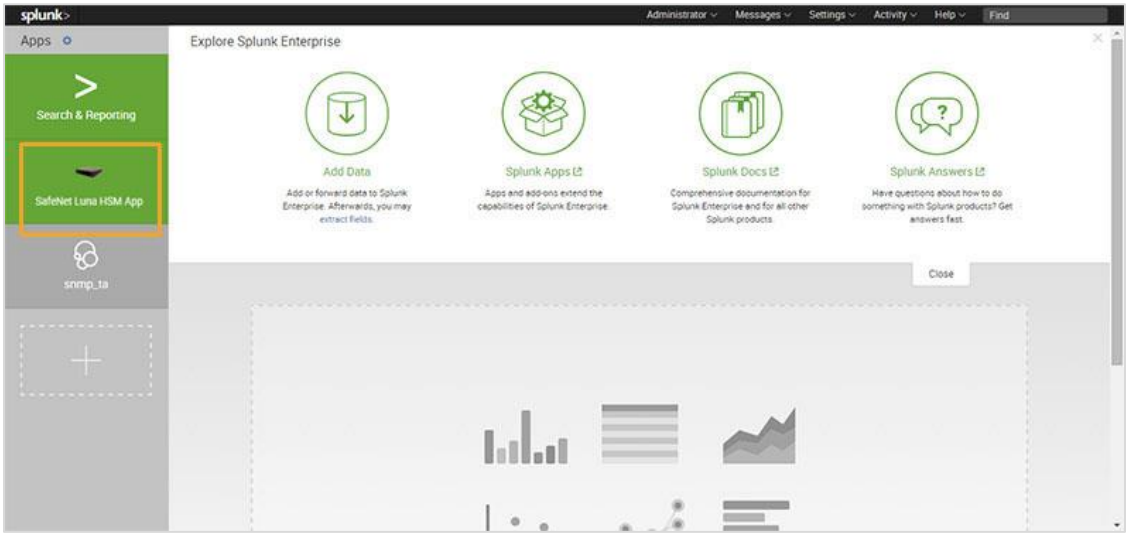

Figure 2: Luna HSM App on Splunk Web Interface

The Splunk interface for Luna HSM App displays.

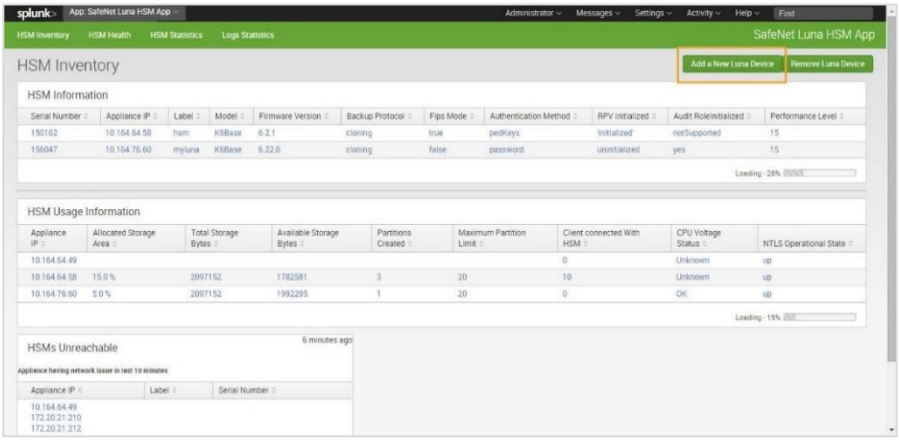

Figure 3: Add a New Luna Device on Luna HSM App

3. Click **Add a New Luna Device.** The **Add a new Luna Appliance** screen displays.

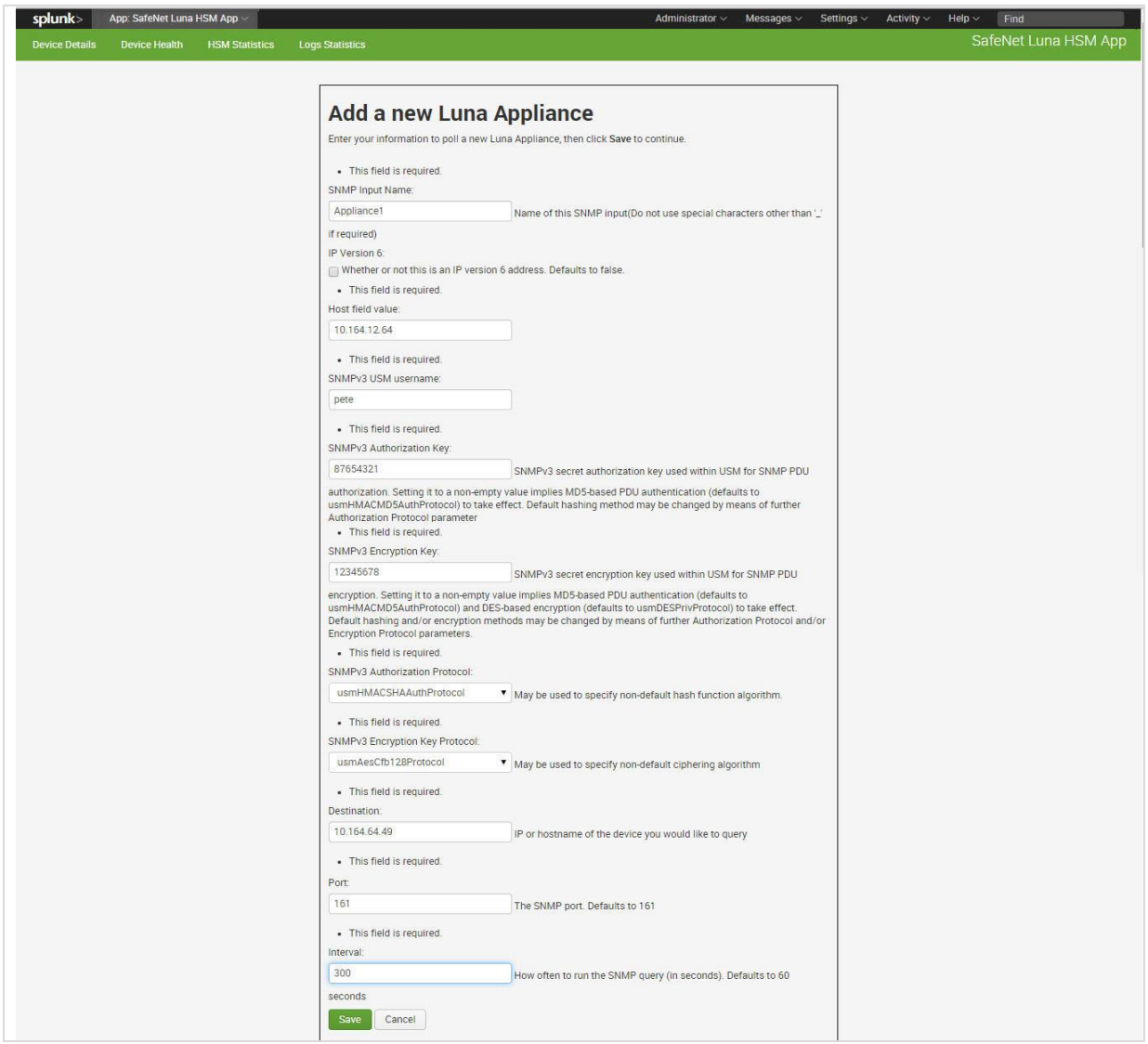

Figure 4: Add a New Luna Appliance Interface

4. Enter your information in the fields as explained below:
   a. **SNMP Input 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. **IP Version 6**: Mark this checkbox, if your device support IPv6.
   c. **Host Field Value**: Enter the I.P Address where Luna HSM App is hosted.
   d. **SNMPv3 USM username**: Enter the username you created on your Luna appliance while configuring SNMP.
   e. **SNMPv3 Authorization Key**: Enter the SNMPv3 secret authorization key you used during SNMP user creation on the Luna device.
   f. **SNMPv3 Encryption Key**: Enter the SNMPv3 secret encryption key you used during SNMP user creation on the Luna device.
   g. **SNMPv3 Authorization Protocol**: Select the Authorization protocol name corresponding to the key you used during SNMP user creation on Luna Box.
   h. **SNMPv3 Encryption Key Protocol**: Select the Encryption protocol name corresponding to the key you used during SNMP user creation on Luna Box.
   i. **Destination**: Enter the I.P of the device that will be queried for data.
   j. **Port**: Enter the SNMP polling port available on Luna appliance. The default port is **161**.
   k. **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.
5. Click **Save** to continue.

   The SafeNet Luna Network HSM appliance is now configured with Luna HSM App on the Splunk web interface. Verify the SafeNet Luna Network HSM is available in the **HSM Information** section under the **HSM Inventory** tab.

Removing a Luna Device

Remove SafeNet Luna HSM appliances that you do not want Splunk to monitor.

To remove a Luna device

1. On the Splunk interface for Luna HSM App click **Remove Luna Device.** The **Remove Luna Appliance** screen displays.

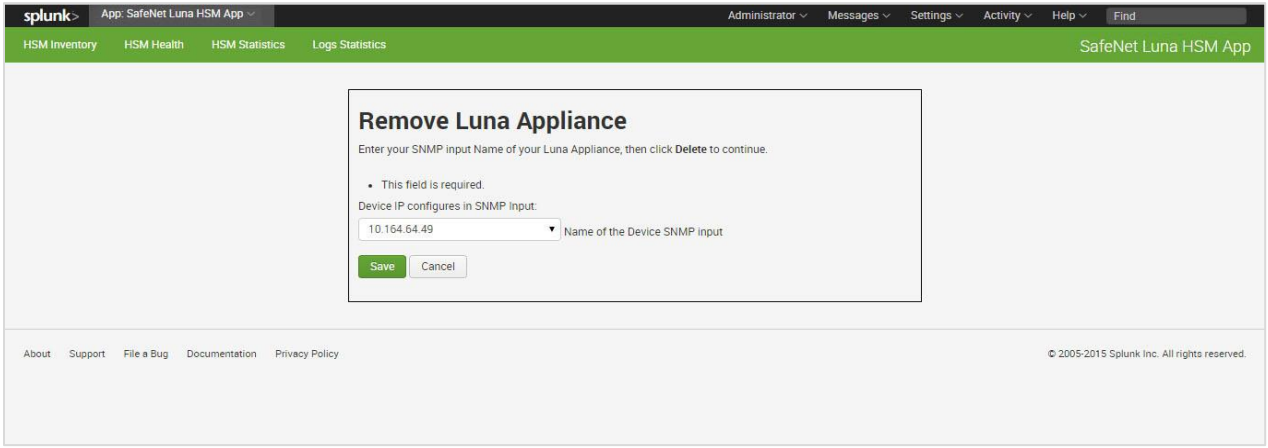

Figure 5: Remove Luna Appliance

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

   The Luna Network HSM appliance is removed from the HSM Inventory List.

4

Monitoring SafeNet Luna HSM Appliances

Use the Luna HSM App to monitor SafeNet Luna HSM appliances for health status, logs, and availability, providing visibility of the appliances operations and status. Using the syslog and SNMP poll request you can monitor the SafeNet Luna HSM for the following:

- 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 Inventory** tab view the **HSM Information**, **HSM Usage Information** and **HSMs Unreachable** categories.

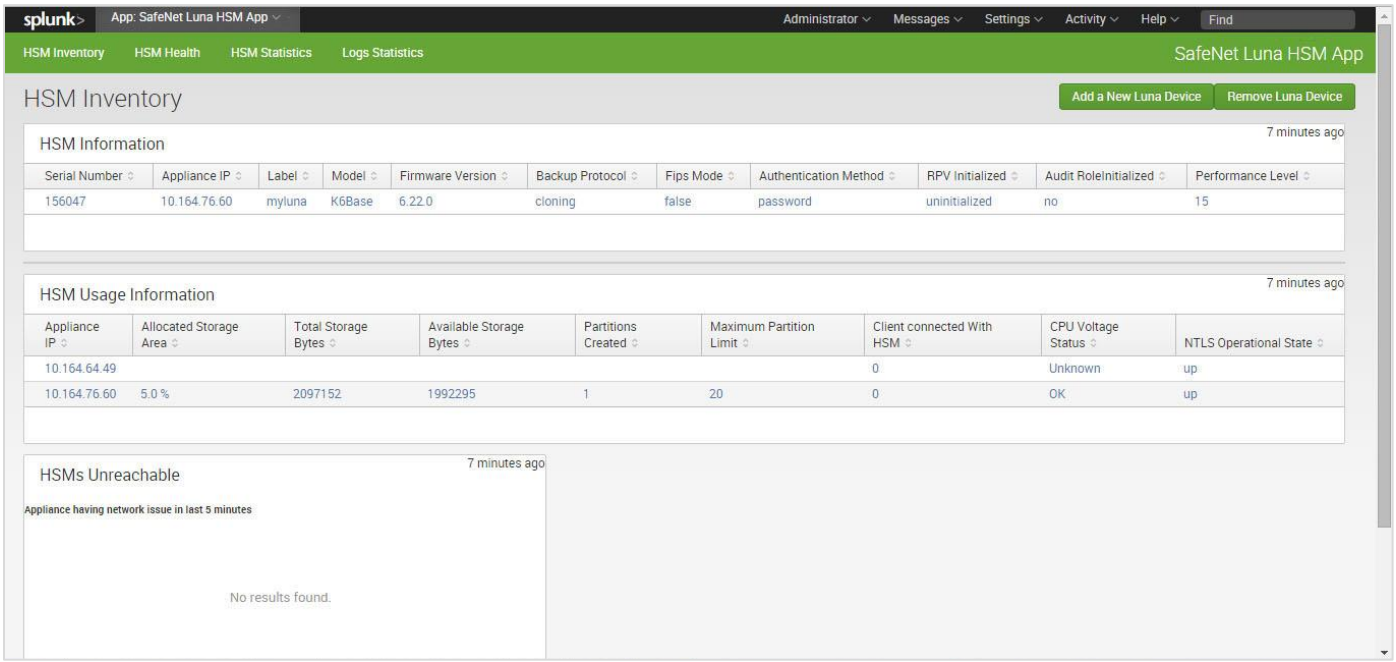

Figure 6: HSM Inventory

- **HSM Information:** The HSM Information panel provides appliance details like **IP Address**, **Box label**, **Version** and the **Performance levels**.

- **HSM Usage Information:** This panel provides information regarding storage space and partition. It also provides information about **CPU voltage** and **NTLS Operational state**.

HSM Health

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

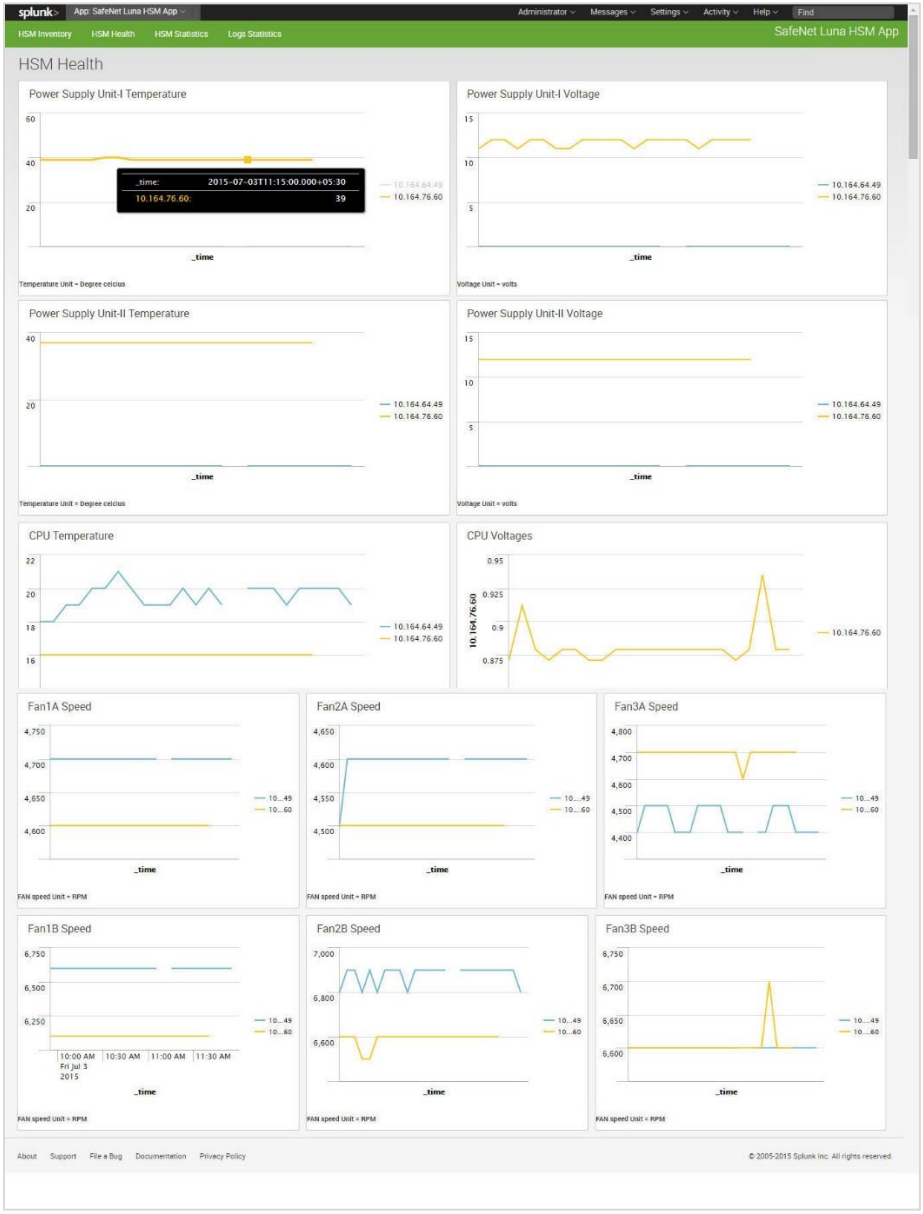

Figure 7: HSM Health

HSM Statistics

Click the **HSM Statistics** tab to view the **Crypto operations frequency**, **HSM Utilization**, **Operations Error Frequency**, **Command count frequency**, **Operational state**, and **HSM Successful client connections**. Select the desired IP from the **Appliance Host IP List** drop-down to view the HSM Statistics of a particular appliance.

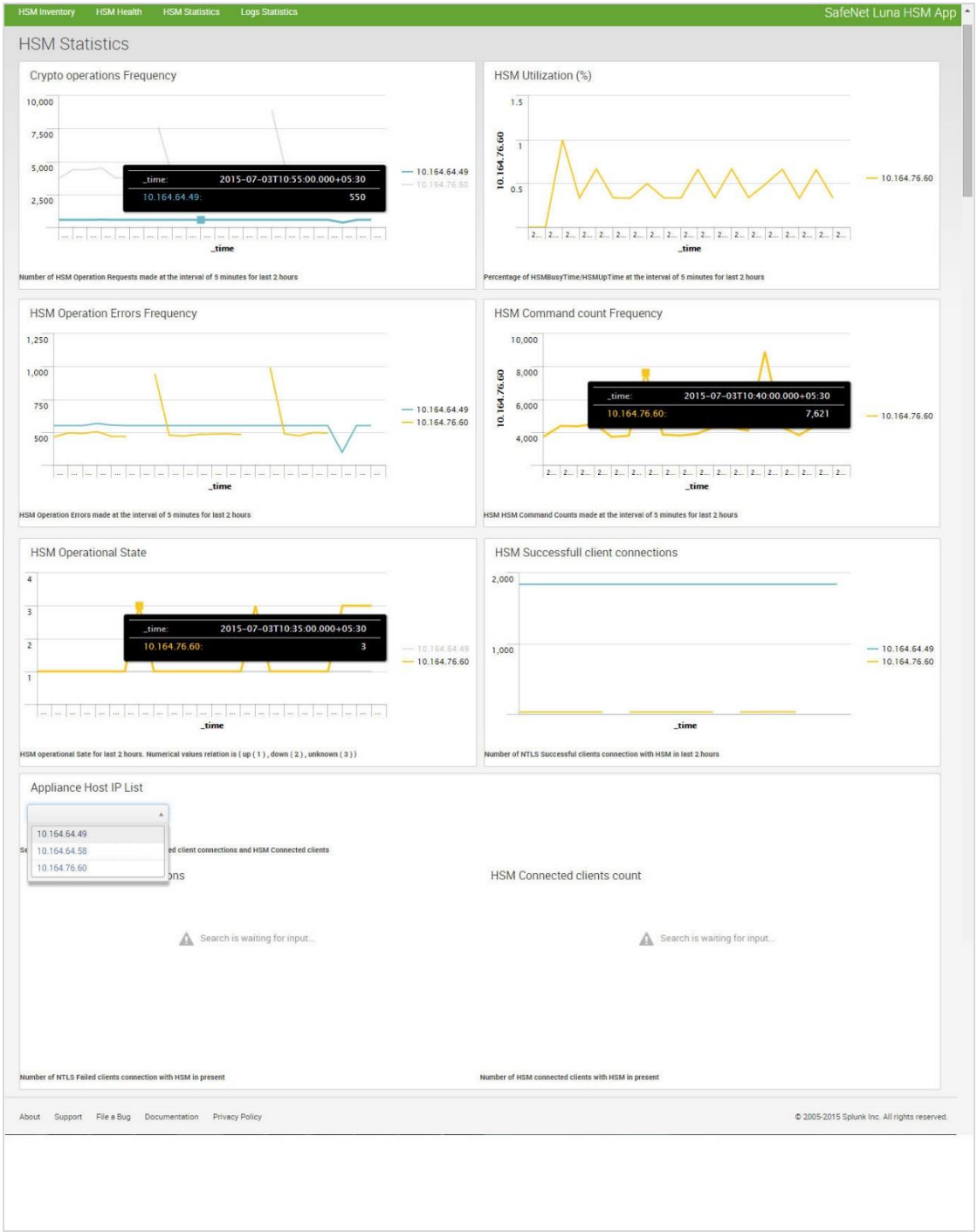

Figure 8: HSM Statistics

Log Statistics

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

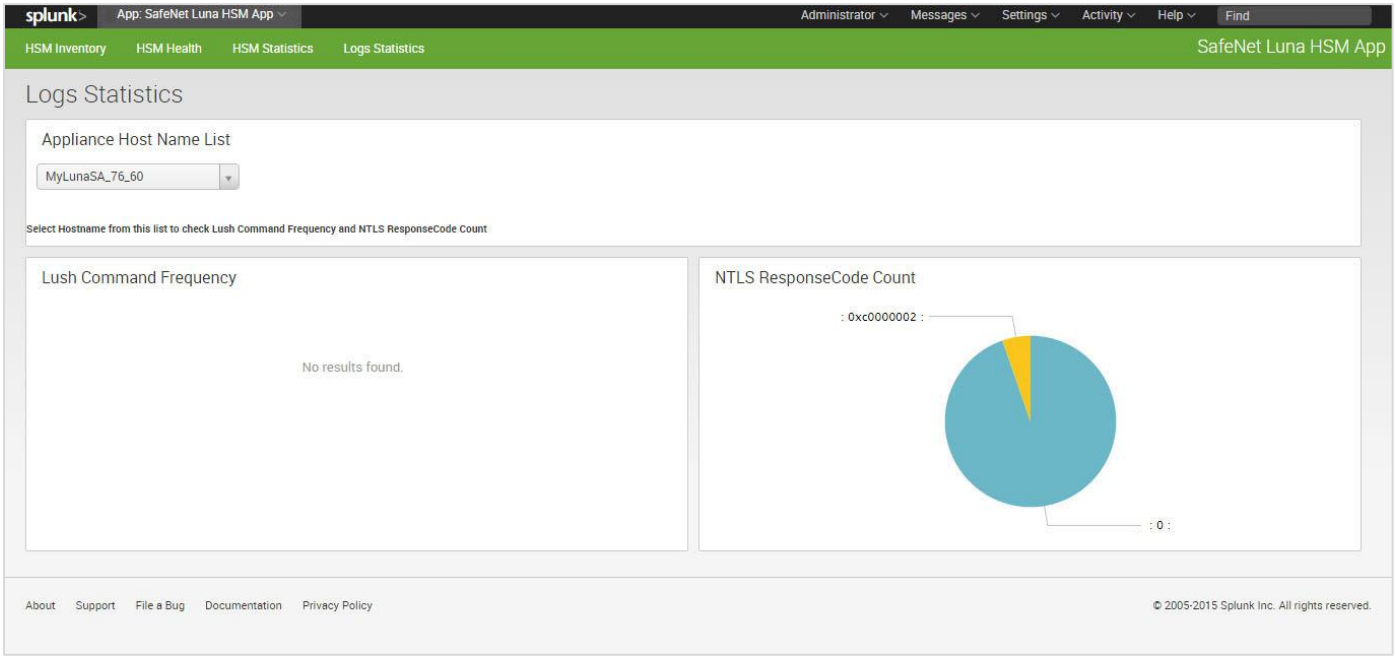

Figure 9: Log Statistics