

Splunk

Splunk Universal Forwarder & Splunk
Enterprise

10.0.2

Integration Guide

ESKM

8.54.0

utimaco[®]

Imprint

Copyright 2026	Utimaco IS GmbH Krefelder Straße 220 52070 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	1.0.0
Date	2026-01-08
Status	PUBLISHED
Document No.	IG-2025-0066
All rights reserved	<p>No part of this documentation may be reproduced in any form (printing, photocopy or according to any other process) without the written approval of Utimaco IS GmbH or be processed, reproduced or distributed using electronic systems.</p> <p>Utimaco IS GmbH reserves the right to modify or amend the documentation at any time without prior notice. Utimaco IS GmbH assumes no liability for typographical errors and damages incurred due to them.</p> <p>All trademarks and registered trademarks are the property of their respective owners.</p>

Table of Contents

1	Introduction	5
1.1	About This Guide	5
1.2	Target Audience	5
1.3	Purpose of the Integration	5
1.4	Abbreviations	5
1.5	Document Conventions	7
2	Product Overview	8
2.1	Overview of ESKM	8
2.2	Overview of Splunk Universal Forwarder	8
2.3	Joint Value Proposition	8
3	Integration Requirements and Prerequisites	10
3.1	Tested Versions	10
3.2	Hardware and Software Requirements	10
3.3	Prerequisites	10
4	Installation and Configuration	11
4.1	Setting Up ESKM	11
4.2	Setting Up Splunk Enterprise and Universal Forwarder	12
5	Integration Steps	16
5.1	Configuration on ESKM	16
5.2	Configuration on Syslog and Splunk Universal Forwarder	17
5.3	Configuration on Splunk Enterprise	19
6	Verification and Testing	22
6.1	Functional Testing	22
6.2	Verification of Integration with TLS Enabled	22
6.2.1	Configuration of Syslog	22
6.2.2	Upload CA and Client Certificate to ESKM	24
6.2.3	Syslog TLS and Server Setting in ESKM	26
6.2.4	Verify Logs Displayed in Splunk	28
7	Troubleshooting	30
7.1	Common Issues	30
8	Contact and Support Information	33

9 Appendices 34

9.1 Command Summary 34

9.2 References 37

1 Introduction

1.1 About This Guide

This guide provides information on how to integrate ESKM with external logging systems. In addition to the internal log, Utimaco ESKM can be configured to forward audit entries to external log management systems. This ensures that enterprise security teams have a centralized view of activity across all platforms and can verify the health of the system according to the ESKM events.

1.2 Target Audience

This guide is intended for Utimaco ESKM administrators.

1.3 Purpose of the Integration

The purpose of this manual is to integrate the Utimaco ESKM with the Splunk Universal Forwarder, which provides centralized log analytics and enhanced security. ESKM generates audit, system, and operational logs related to key management activities. Forwarding these logs to a centralized logging solution enables organizations to collect and index large volumes of data in real time, allowing fast search, filtering, and aggregation for operational monitoring and troubleshooting. This integration also supports security analysis and compliance reporting by making logs easily searchable, ensuring visibility and control over cryptographic operations and key lifecycle events across the enterprise.

1.4 Abbreviations

Abbreviations	Meaning
ESKM	Enterprise Secure Key Manager
KMIP	Key Management Interoperability Protocol
KMS	Key Management Server

Abbreviations	Meaning
CA	Certificate Authority
SSL	Secure Sockets Layer
TLS	Transport Layer Security
FIPS	Federal Information Processing Standards
UF	Universal Forwarder
IP	Internet Protocol

Table 1: Abbreviations

1.5 Document Conventions

The following conventions are used in this guide:

Convention	Use	Example
Bold	Items of the Graphical User Interface (GUI), e.g., menu options	Click Save
<code>Monospaced</code>	Code that is given for explanation or as an example, file paths	<code>chmod 750</code>
<i>Italic</i>	References and important terms	<i>ESKM_Installation and Replacement_Guide_8.54.0</i>

Table 2: Document conventions

We use special icons to highlight the most important notes and information.



Here you will find important safety information.



Here you will find additional notes or supplementary information.



This message indicates the expected result after the successful execution of an instruction.

2 Product Overview

2.1 Overview of ESKM

ESKM is a centralized key management solution that securely stores, distributes, and manages encryption keys throughout their lifecycle. It supports industry standards, including the KMIP, enabling integration with a wide range of enterprise applications and storage systems.

In the Splunk Universal Forwarder integration, ESKM operates as a centralized source of audit and system events. These logs are forwarded from ESKM to a syslog server and then ingested into Splunk Enterprises, enabling administrators to monitor key management activities, track system behavior, and analyze security-relevant events through Splunk dashboards and alerts.

2.2 Overview of Splunk Universal Forwarder

Splunk Universal Forwarder is a lightweight agent designed to collect and securely forward machine data such as logs, metrics, and application events from endpoints to Splunk Enterprise for indexing and analysis. It runs as a background service with minimal resource consumption and supports features like SSL encryption, load balancing, and centralized configuration via a Deployment Server. In a Splunk Enterprise environment, the forwarder acts as the data collection layer, streaming raw data from distributed systems to indexers, where it is parsed, stored, and made searchable for dashboards, alerts, and analytics. This architecture ensures scalable, real-time visibility across IT and security infrastructures without impacting endpoint performance.

2.3 Joint Value Proposition

Integrating Utimaco ESKM with Splunk Universal Forwarder provides a unified and secure approach to monitoring key-management operations across the enterprise. ESKM acts as the centralized key management platform, generating detailed audit, system, and security events that are forwarded reliably to Splunk through the Splunk Universal Forwarder. By ingesting ESKM logs into Splunk Universal Forwarder, organizations gain real-time visibility into key lifecycle activities, cryptographic operations, administrative actions, and system health.

This combined solution strengthens compliance with regulatory frameworks such as PCI DSS, HIPAA, and GDPR by ensuring complete auditability and traceability of key-management processes. Splunk's analytics, dashboards, and alerting capabilities enhance security operations, while ESKM enforces strong key governance and policy controls. Together, they enable

organizations to achieve operational transparency, improved security posture, and centralized monitoring without compromising performance or compliance.

3 Integration Requirements and Prerequisites

3.1 Tested Versions

Splunk Enterprise Version	Splunk Universal Forwarder Version	Utimaco ESKM Version
10.0.2	10.0.2	8.54.0

Table 3: Tested versions

3.2 Hardware and Software Requirements

Software	Software Requirements
Splunk Enterprise and Splunk Universal Forwarder	10.0.2
ESKM	8.54.0
Windows	Windows 10
Linux	RHEL/Ubuntu

Table 4: Software requirements

3.3 Prerequisites

Before you begin, please ensure that you have:

- Installed/set up the Splunk Universal Forwarder and Enterprise versions listed in [Tested Versions](#).
- Installed/set up the ESKM version listed in [Tested Versions](#).
- The required Splunk Enterprise License, if the user is using Splunk Enterprise to view the logs.

4 Installation and Configuration

The following section outlines the procedures required to configure Utimaco ESKM, Splunk Enterprise, and Splunk Universal Forwarder for log view.

4.1 Setting Up ESKM

The initial phase involves configuring ESKM before proceeding to Splunk Enterprise and Splunk Universal Forwarder. For detailed configuration steps, refer to the *"ESKM_Installation and Replacement_Guide_8.54.0"*.

After successful installation and configuration, log in to ESKM.

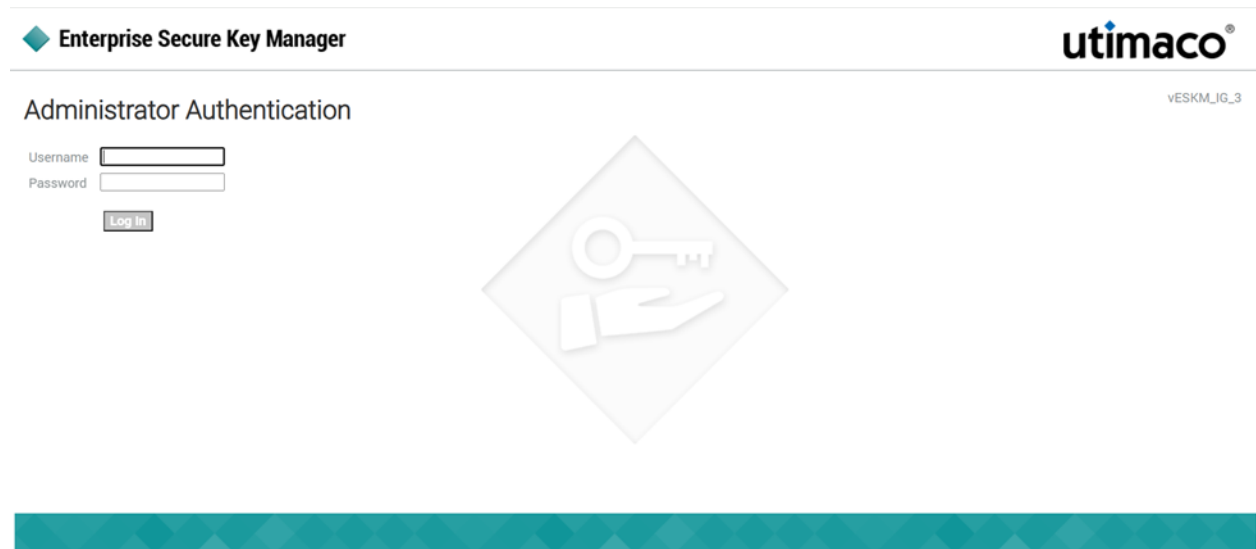
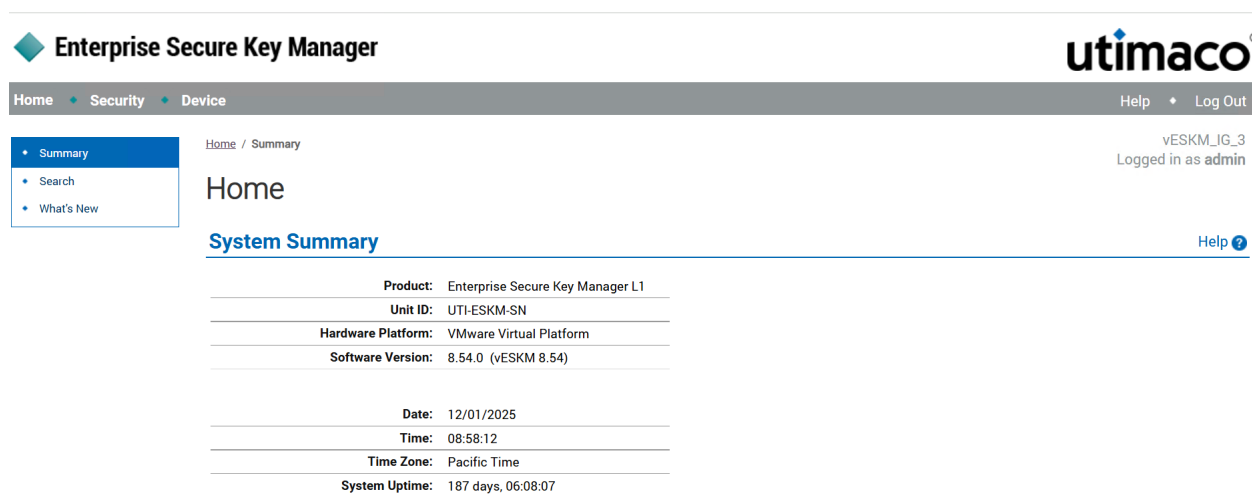


Figure 1 : ESKM login page



Enterprise Secure Key Manager

Home • Security • Device

Help • Log Out

vESKM_IG_3
Logged in as admin

Home / Summary

Home

System Summary [Help ?](#)

Product:	Enterprise Secure Key Manager L1
Unit ID:	UTI-ESKM-SN
Hardware Platform:	VMware Virtual Platform
Software Version:	8.54.0 (vESKM 8.54)
Date:	12/01/2025
Time:	08:58:12
Time Zone:	Pacific Time
System Uptime:	187 days, 06:08:07

Figure 2 : ESKM Home page

4.2 Setting Up Splunk Enterprise and Universal Forwarder

1. Download and install Splunk Enterprise in a Windows machine. Refer to the [Splunk Enterprise](#) link to register and download the latest version of Splunk Enterprise.
2. Access the Linux machine and install Syslog ng following the steps below.
3. Install the epel-release using the command:

```
dnf install -y epel-release
```

```
[root@master-node ~]# dnf install -y epel-release
Last metadata expiration check: 1:34:54 ago on Tue 18 Nov 2025 06:50:29 PM PST.
Dependencies resolved.
=====
Package                Architecture          Version               Repository            Size
=====
Installing:
epel-release            noarch                9-7.e19              extras                 19 k
Transaction Summary
=====
Install 1 Package
```

Figure 3 : Install epel-release

4. Install syslog-ng using command below:

```
dnf install -y syslog-ng
```

```
[root@master-node ~]# dnf install -y syslog-ng
Extra Packages for Enterprise Linux 9 - x86_64                6.6 MB/s | 20 MB    00:03
Extra Packages for Enterprise Linux 9 openh264 (From Cisco) - x86_64  1.3 kB/s | 2.5 kB    00:01
Last metadata expiration check: 0:00:01 ago on Tue 18 Nov 2025 08:26:54 PM PST.
Dependencies resolved.
=====
Package                       Architecture           Version                Repository             Size
=====
Installing:
  syslog-ng                    x86_64                 3.35.1-7.e19         epel                   908 k
Installing dependencies:
  ivykis                       x86_64                 0.42.4-7.e19         epel                   46 k
Transaction Summary
-----
Install 2 Packages
```

Figure 4 : Install syslog-ng

5. Get the Splunk Universal Forwarder installation file using the wget command:

```
wget -O splunkforwarder-10.0.2-e2d18b4767e9.x86_64.rpm "https://
download.splunk.com/products/universalforwarder/releases/10.0.2/linux/
splunkforwarder-10.0.2-e2d18b4767e9.x86_64.rpm"
```

```
[root@master-node ~]# wget -O splunkforwarder-10.0.2-e2d18b4767e9.x86_64.rpm "https://download.splunk.com/products/universalforwarder/releases/10.0.2/linux/splunkforwarder-10.0.2-e2d18b4767e9.x86_64.rpm"
--2025-11-19 00:47:06-- https://download.splunk.com/products/universalforwarder/releases/10.0.2/linux/splunkforwarder-10.0.2-e2d18b4767e9.x86_64.rpm
Resolving download.splunk.com (download.splunk.com)... 3.169.183.74, 3.169.183.78, 3.169.183.124, ...
Connecting to download.splunk.com (download.splunk.com)|3.169.183.74|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 112129206 (107M) [binary/octet-stream]
Saving to: 'splunkforwarder-10.0.2-e2d18b4767e9.x86_64.rpm'

splunkforwarder-10.0.2-e2d1 100%[=====>] 106.93M  54.7MB/s   in 2.0s
2025-11-19 00:47:09 (54.7 MB/s) - 'splunkforwarder-10.0.2-e2d18b4767e9.x86_64.rpm' saved [112129206/112129206]
```

Figure 5 : Get the Splunk Universal Forwarder Installation Universal Forwarder installation file

6. Install Splunk Universal Forwarder.

```
sudo rpm -i splunkforwarder-10.0.2-e2d18b4767e9.x86_64.rpm
```

```
[root@master-node ~]# sudo rpm -i splunkforwarder-10.0.2-e2d18b4767e9.x86_64.rpm
warning: splunkforwarder-10.0.2-e2d18b4767e9.x86_64.rpm: Header V4 RSA/SHA256 Signature, key ID b3cd4420: NOKEY
verify that this system has all the commands we will require to perform the preflight step
no need to run the splunk-preinstall upgrade check
find: '/opt/splunkforwarder/lib/python3.7/site-packages': No such file or directory
find: '/opt/splunkforwarder/lib/python3.9/site-packages': No such file or directory
complete
```

Figure 6 : Splunk Universal Forwarder installation

7. Create a user account for the Splunk Universal Forwarder by running the following command. When prompted, enter a username and password to complete the setup.

```
sudo /opt/splunkforwarder/bin/splunk start --accept-license
```

```
[root@master-node ~]# sudo /opt/splunkforwarder/bin/splunk start --accept-license
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: admin
Password must contain at least:
  * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
Important: splunk will start under systemd as user: splunkfwd
The unit file has been created.

Splunk> Needle. Haystack. Found.

Checking prerequisites...
  Checking mgmt port [8089]: open
  Creating: /opt/splunkforwarder/var/lib/splunk
  Creating: /opt/splunkforwarder/var/run/splunk
  Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
  Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
  Creating: /opt/splunkforwarder/var/run/splunk/upload
  Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry
  Creating: /opt/splunkforwarder/var/run/splunk/search_log
```

Figure 7 : Create Splunk Universal Forwarder user

8. The following command configures the Splunk Universal Forwarder to start automatically every time the system boots. This ensures that log forwarding from the ESKM syslog server to Splunk Enterprise continues without requiring manual intervention after reboots or maintenance activities.

```
/opt/splunkforwarder/bin/splunk enable boot-start
```

```
[root@master-node ~]# sudo /opt/splunkforwarder/bin/splunk enable boot-start  
splunk is currently running, please stop it before running enable/disable boot-start
```

Figure 8 : Enable Splunk Universal Forwarder

5 Integration Steps

5.1 Configuration on ESKM

1. Log in to ESKM.
2. Click the **Device** tab and click the **Log Configuration** link under the **Logs & Statistics** section.
3. Click the **Edit** button under the **Syslog Settings** table.
4. Select the checkboxes under the **Enable Syslog** column for the logs that need to be displayed in Splunk.
5. Enter the machine IP where Syslog and Splunk Universal Forwarder are installed under the **Syslog Server #1 IP** column, and enter the port number (default – 514) in the **Syslog Server #1 Port** column.
6. Click the **Save** button.

Syslog Settings

Log Name	Enable Syslog	Syslog Server #1 IP	Syslog Server #1 Port	Syslog Server #2 IP
<input checked="" type="radio"/> System	<input checked="" type="checkbox"/>	172.31.1.72	514	[None]
<input type="radio"/> Audit	<input checked="" type="checkbox"/>	172.31.1.72	514	[None]
<input type="radio"/> Activity	<input checked="" type="checkbox"/>	172.31.1.72	514	[None]
<input type="radio"/> Client Event	<input type="checkbox"/>	[None]	514	[None]
<input type="radio"/> KMIP	<input type="checkbox"/>	[None]	514	[None]
<input type="radio"/> REST	<input type="checkbox"/>	[None]	514	[None]

Figure 9 : Syslog Settings

5.2 Configuration on Syslog and Splunk Universal Forwarder

1. Login to the Linux machine where Splunk Universal Forwarder is installed.
2. Create a folder `eskm` under `/var/log` and give permission.

```
mkdir -p /var/log/eskm
chown root:root /var/log/eskm
chmod 750 /var/log/eskm
```

3. Create an `eskm.conf` file under `/etc/syslog-ng/conf.d` with the following configurations.

```
@version: 3.29

# Network source - accept TCP & UDP from ESKM
source s_eskm_net {
    network(
        ip("0.0.0.0")
        port(514)
        transport("tcp")
    );
    network(
        ip("0.0.0.0")
        port(514)
        transport("udp")
    );
};

# Destination file for ESKM logs
destination d_eskm {
    file("/var/log/eskm/eskm.log"
        create_dirs(yes)
        perm(0640)
    );
};

# Log path
log {
    source(s_eskm_net);
    destination(d_eskm);
};
```

4. After creating the `eskm.conf` file under `/etc/syslog-ng/conf.d`, restart the `syslog-ng` service to apply the new configuration. Enabling the service ensures it automatically starts

on system boot, and checking its status verifies that syslog-ng is running correctly and ready to receive ESKM log events.

```
systemctl restart syslog-ng
systemctl enable syslog-ng
systemctl status syslog-ng
```

- The systemctl status output should display the service as active (running), confirming that syslog-ng has successfully loaded the new configuration and is operational.

```
[root@master-node ~]# vim /etc/syslog-ng/conf.d/eskm.conf
[root@master-node ~]# systemctl restart syslog-ng
[root@master-node ~]# systemctl enable syslog-ng
[root@master-node ~]# systemctl status syslog-ng
● syslog-ng.service - System Logger Daemon
   Loaded: loaded (/usr/lib/systemd/system/syslog-ng.service; enabled; preset: enabled)
   Active: active (running) since Tue 2025-11-18 21:01:02 PST; 29s ago
     Docs: man:syslog-ng(8)
  Main PID: 297527 (syslog-ng)
    Tasks: 2 (limit: 23154)
   Memory: 6.3M
      CPU: 10.230s
   CGroup: /system.slice/syslog-ng.service
           └─297527 /usr/sbin/syslog-ng -F -p /var/run/syslogd.pid

Nov 18 21:01:02 master-node systemd[1]: Starting System Logger Daemon...
Nov 18 21:01:02 master-node syslog-ng[297527]: [2025-11-18T21:01:02.948144] WARNING: you have multiple @ver
Nov 18 21:01:02 master-node syslog-ng[297527]: [2025-11-18T21:01:02.957108] WARNING: With use-dns(no), dns-
Nov 18 21:01:02 master-node systemd[1]: Started System Logger Daemon.
```

Figure 10 : Syslog-ng started running

- Create an `inputs.conf` file under `/opt/splunkforwarder/etc/system/local/` with the following configurations.

```
[monitor:///var/log/eskm/eskm.log]
index = eskm_index
sourcetype = utimaco:eskm
crcSalt = <SOURCE>
```

- Create an `outputs.conf` file under `/opt/splunkforwarder/etc/system/local/` with the following configurations.

```
[tcpout]
defaultGroup = default-indexer-group

[tcpout:default-indexer-group]
```

```
server = <SPLUNK_ENTERPRISE_IP>:9997
```



Replace <SPLUNK_ENTERPRISE_IP> with the IP address of the server where Splunk Enterprise is installed and listening on port 9997 for Universal Forwarder connections.

8. After creating or updating both the `inputs.conf` and `outputs.conf` files, the Splunk Universal Forwarder must be restarted for the new configurations to take effect.

```
/opt/splunkforwarder/bin/splunk restart
```

5.3 Configuration on Splunk Enterprise

1. Log in to the machine where Splunk Enterprise has been installed.
2. Open and log in to the Splunk Enterprise application.
3. Click **Settings** and **Indexes**, then click **New Index**.
 - a. Enter the same index name given in the `inputs.conf` file in the **Index Name** field and select Search & Reporting from the **App** dropdown.

New Index [Close]

General Settings

Index Name:
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: Events Metrics
The type of data to store (event-based or metrics).

Home Path:
Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

Cold Path:
Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path:
Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check: Enable Disable

[Save] [Cancel]

Figure 11 : Index name configuration

New Index [Close]

Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket: GB ▾
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path:
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App:

Storage Optimization

Tsidx Retention Policy: Enable Reduction Disable Reduction
Warning: Do not enable reduction without understanding the full implications. It is extremely difficult to rebuild reduced buckets. [Learn More](#)

Reduce tsidx files older than: Days ▾
Age is determined by the latest event in a bucket.

[Save] [Cancel]

Figure 12 : App configuration

4. Click the **Save** button.
5. Click **Settings** and **Forwarding & Receiving**, then click the **+Add new** button under the **Receive data** section.
6. Type 9997 in the **Listen on this port** field and click the **Save** button.

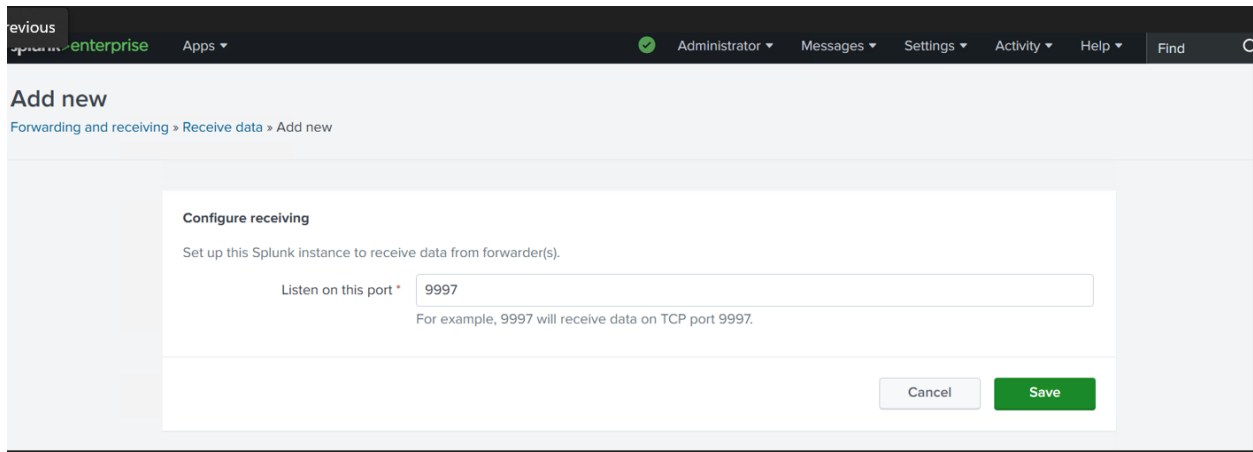
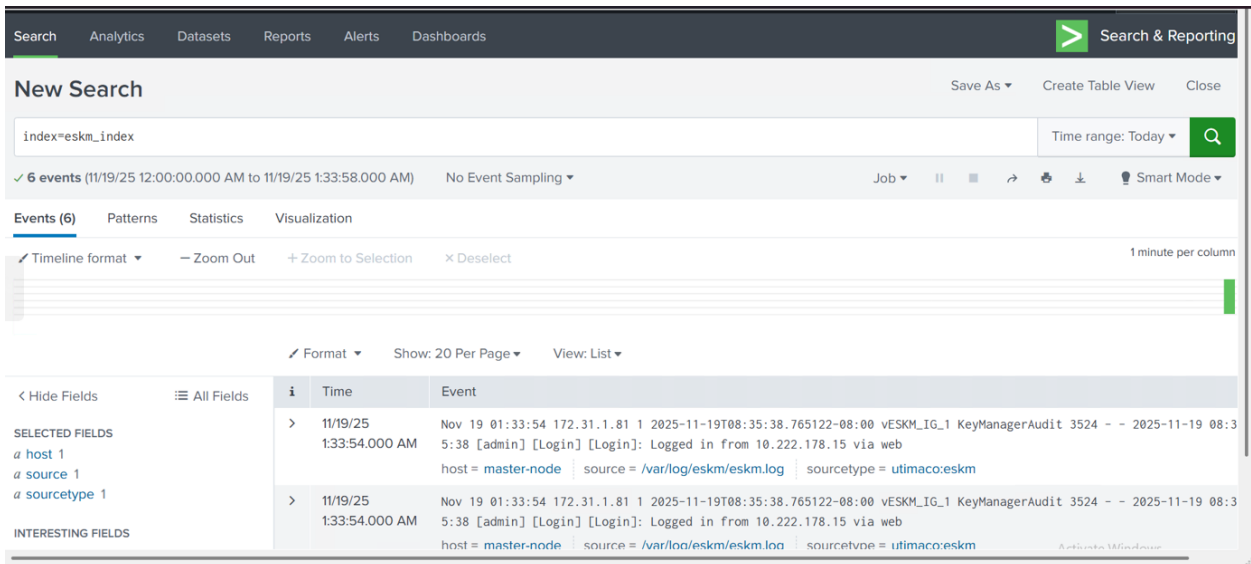


Figure 13 : Configure the receiving port

6 Verification and Testing

6.1 Functional Testing

1. Log in to the Windows machine where Splunk Enterprise is configured and log in to it.
2. Click the **Apps** menu and select **Search & Reporting**. The same link is also available in the Splunk Enterprise dashboard.
3. Enter `index=<created_index>` in the search bar and verify that the corresponding ESKM logs are displayed.



The screenshot displays the Splunk Search & Reporting interface. At the top, the navigation bar includes 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The 'Search & Reporting' section is active. Below the navigation bar, the 'New Search' header is visible, along with options to 'Save As', 'Create Table View', and 'Close'. The search bar contains the query 'index=eskm_index' and the time range is set to 'Today'. Below the search bar, it indicates '6 events' and 'No Event Sampling'. The main content area shows a table of search results with columns for 'Time' and 'Event'. Two events are displayed, both from 11/19/25 at 1:33:54.000 AM. The event details include the date, time, IP address, and a login message: 'Nov 19 01:33:54 172.31.1.81 1 2025-11-19T08:35:38.765122-08:00 vESKM_IG_1 KeyManagerAudit 3524 - - 2025-11-19 08:31:33:54.000 AM 5:38 [admin] [Login] [Login]: Logged in from 10.222.178.15 via web'. The host is identified as 'master-node' and the source is '/var/log/eskm/eskm.log' with a sourcetype of 'utimaco:eskm'.

Figure 14 : ESKM logs displayed in Splunk



After Splunk UF is configured, perform actions on the ESKM server, such as login, logout, or any administrative operation, to ensure new events are captured.

6.2 Verification of Integration with TLS Enabled

6.2.1 Configuration of Syslog

1. Log in to the Linux machine where Splunk UF is installed.

2. Create a Certificate Authority (CA).

```
openssl genrsa -out ca.key 4096
openssl req -x509 -new -nodes -key ca.key -sha256 -days 3650 -out ca.crt -subj "/
C=US/ST=TX/L=AU/O=Utimaco/OU=Security/CN=ESKM-CA"
```

3. Create a server certificate for syslog-ng.

```
openssl genrsa -out syslog.key 4096
openssl req -new -key syslog.key -out syslog.csr -subj "/C=US/ST=TX/L=AU/
O=Utimaco/OU=Security/CN=<SYSLOG_SERVER_IP>"
```



Replace `<SYSLOG_SERVER_IP>` with the IP address that ESKM uses to reach syslog-ng.

4. Sign the server certificate with the CA.

```
openssl x509 -req -in syslog.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out
syslog.crt -days 3650 -sha256
```

5. Create a folder `certs` in `/etc/syslog-ng` and copy the certificate and key files to it.

```
mkdir -p /etc/syslog-ng/certs
cp syslog.crt syslog.key ca.crt /etc/syslog-ng/certs/
chmod 600 /etc/syslog-ng/certs/*
```

6. Update `eskm.conf` in `etc/syslog-ng/conf.d` directory with the following set of configurations.

```
# TLS options
source s_eskm_tls {
    network(
        ip("0.0.0.0")
        port(6514)
        transport("tls")
        tls(
            key-file("/etc/syslog-ng/certs/syslog.key")
            cert-file("/etc/syslog-ng/certs/syslog.crt")
        )
    )
}
```

```
        ca-file("/etc/syslog-ng/certs/ca.crt")
        peer-verify(optional-untrusted)
    )
);
};
destination d_eskm {
    file("/var/log/eskm/eskm.log" create_dirs(yes) perm(0640));
};
log {
    source(s_eskm_tls);
    destination(d_eskm);
};
```

7. Create a client certificate and copy the certificate to the machine where the user accesses the ESKM application (WinSCP or any other means).

```
openssl pkcs12 -export -in server.crt -inkey server.key -certfile ca.crt -out
eskm-syslog-client.p12
```

8. Restart syslog-ng and check for no errors.

```
systemctl restart syslog-ng
systemctl status syslog-ng
```

6.2.2 Upload CA and Client Certificate to ESKM

1. Log in to the machine to which the CA and Client certificates have been copied.
2. Save both certificates as .pem files.
3. Log in to the ESKM Web UI.
4. Click the **Security** tab and click the **Known CA** link under the **Certificates & CA** section.
5. Under the **Install CA Certificate** Section, enter the CA name in the **Certificate Name** field and copy the content of the CA certificate to the **Certificate** textbox.

Install CA Certificate

Certificate Name:

Certificate:

```

R5ISQJ0J+3BNV+0BFNLZATmoaEHUOVYTXouaTWCWIMEI2j+qvUVUnaxnTPVaJIZ8
7m0Lno+JJm30oASo0tmbvQCRZa2IJ387m18YHv6t1zStsT1BP5UDD7QyZRm10FDA
uFAVAgMBAAGjUzBRMB0GA1UdDgQWBBSZDYBYaGQ05iB+aV+47teduyV8IzAFBgNV
HSMEGDAWgBSZDYBYaGQ05iB+aV+47teduyV8IzAPBgNVHRMBAf8EBTADAQH/MA0G
CSqGSIb3DQEBCwUAA4ICAQAdn+B76Vk9ubQFZKjK1ocCf16a7R9ZehCycwuE2yw1
/3ZPQJ47HYo1BTFdGLa30t2U0q/vp4sfUUm7/ompPsw0h1tmh5wYTAyosZCzwC9d
ocAcP8K+60oHBmKk2Hx19zExmg9ho+xs000b4cJor3M0SqnAqYOLy12ogAqMNuxs
VhgQVIt+xu5hbXIH1JzEdXaqxd/uB3rWneBahTzvGKg2W+VHqdESpdks8IYhxua
0IAME555JRZw4zFBjZVE9s3SD0OCib4+CgVIohIpmtI+83skzKCUDuqA/d8BgpkD
LNw161e5x16kMDTbMU6A28RUSMSLQ8Bnix51FGPV+VcdfS/uEUp8TuNTf1JoP7gn
ZK3k/NX1VwZ7SBMDOKF1lkgaYSxPzV5PSIKiwjTzV0WFqC6duVBVza+o2p12KMMe
uL98k3wUVRfbcsvUAV1FrpjmddekoXh7oPLqZ0zzrfYNNaUY1DEsfwmbHOvPtWvM
QlsDLDiDIIsYwkdiqyR6qSrNh5iXSpm08SAABZsW0XOI4rirFFtcaJmaoOC24Z00
eEPv6LF3EsvQBhIyhsh6W+0LEVjqQNsWzQ5W/vkDBkv34Et9hNNuCPg+Jxiz6Iir
SxbgL0D0/xG0+A0kAJDpEwOWIZCmt7QGwgJjAjTzB1VS2Z0XJ1jq8iWZCQsjMzmr
    
```

Install

Figure 15 : Install CA Certificate

- Click the **Install** button. The newly installed CA is listed under the CA Certificate List section.

CA Certificate List

Filtered by where value

Items per page:

Certificate Name	Certificate Information	Certificate Status
<input checked="" type="radio"/> CA	Issuer: Utimaco Expires: Nov 30 09:21:07 2035 GMT	Certificate Active

1 - 1 of 1

Figure 16 : CA Certificate List

- Click on the **Certificates** link under the **Certificates & CA** section.
- Select the **Upload from browser** radio button under **Import Certificate** section.

9. Select the client certificate by clicking on the **Choose File** button.
10. Enter a name in the **Certificate Name** field.
11. Enter the **Private Key Password** if any password was set; otherwise, leave it blank.

Import Certificate

Source:

Upload from browser File: eskm-syslog-client.p12

SCP

Host:

Filename:

Username:

Password:

Certificate Name:

Private Key Password:

Figure 17 : Import client certificate to ESKM

12. Click on the **Import Certificate** button.
13. The newly imported certificate is listed under the **Certificate List** section.

Certificate List

Certificate Name	Certificate Information	Certificate Purpose	Certificate Status
<input checked="" type="radio"/> client	Common: 172.31.1.72 Issuer: Utimaco Expires: Nov 30 09:24:18 2035 GMT	Server/Client	Active

Figure 18 : Client certificate listed in the Certificate List

6.2.3 Syslog TLS and Server Setting in ESKM

1. Click the **Device** tab and click the **Log Configuration** link under the **Logs & Statistics** section.
2. Click the **Edit** button under the **Syslog Settings** table.

3. Select the checkboxes under the **Enable Syslog** column for the logs that need to be displayed in Splunk.
4. Enter the machine IP where Syslog and Splunk UF are installed in the **Syslog Server #1 IP** column, and enter port number 6514 in the **Syslog Server #1 Port** column.
5. Click the **Save** button.

Syslog Settings

Log Name	Enable Syslog	Syslog Server #1 IP	Syslog Server #1 Port	Syslog Server #2 IP	Syslog Server #2 Port
<input checked="" type="radio"/> System	<input checked="" type="checkbox"/>	172.31.1.72	6514	[None]	514
<input type="radio"/> Audit	<input checked="" type="checkbox"/>	172.31.1.72	6514	[None]	514
<input type="radio"/> Activity	<input checked="" type="checkbox"/>	172.31.1.72	6514	[None]	514
<input type="radio"/> Client Event	<input type="checkbox"/>	[None]	514	[None]	514
<input type="radio"/> KMIP	<input type="checkbox"/>	[None]	514	[None]	514
<input type="radio"/> REST	<input type="checkbox"/>	[None]	514	[None]	514

Figure 19 : Syslog Settings

6. Click the **Edit** button in the **Syslog TLS Settings** section.
7. Enable the **Enable TLS** checkbox.
8. Select the uploaded client certificate name from the **Certificate** dropdown list.
9. Select the uploaded CA from the **Trusted Certificate Authority** dropdown list.
10. Click the **Save** button.

Syslog TLS Settings

Enable TLS:

Certificate: client

Trusted Certificate Authority: Known: CA

Figure 20 : Syslog TLS Settings

11. Click on the **Syslog Test** button in the **Syslog Settings** section.

Syslog Settings

Log Name	Enable Syslog	Syslog Server #1 IP	Syslog Server #1 Port
<input checked="" type="radio"/> System	<input checked="" type="checkbox"/>	172.31.1.72	6514
<input type="radio"/> Audit	<input checked="" type="checkbox"/>	172.31.1.72	6514
<input type="radio"/> Activity	<input checked="" type="checkbox"/>	172.31.1.72	6514
<input type="radio"/> Client Event	<input type="checkbox"/>	[None]	514
<input type="radio"/> KMIP	<input type="checkbox"/>	[None]	514
<input type="radio"/> REST	<input type="checkbox"/>	[None]	514

Note: Successfully connected to syslog server #1.

[Edit](#) [Syslog Test](#)

Figure 21 : Syslog server connection confirmation message

12. Log out from the ESKM Web UI and log in again.
13. Click the **Device** tab and click the **Log Viewer** link under the **Logs & Statistics** section.
14. Click on the **Audit** link under the Log Viewer section and note down the latest logs displayed under **Log File: Current**.

The screenshot shows the 'Log File: Current (Showing Last 10 Lines)' section of the Log Viewer. A 'Download Entire Log' button is visible at the top. The log entries are as follows:

```

Audit Log:
2025-12-03 09:48:26 [admin] [Login] [Login]: Logged in from 10.222.178.15 via web
2025-12-03 09:56:18 [admin] [Login] [Login]: User admin login has expired.
2025-12-03 09:56:27 [admin] [Login] [Login]: Logged in from 172.31.1.54 via web
2025-12-03 10:02:05 [admin] [Login] [Login]: Logged out from 172.31.1.54 via web
2025-12-03 10:02:15 [admin] [Login] [Login]: Logged in from 172.31.1.54 via web
2025-12-03 10:12:38 [admin] [Login] [Login]: User admin login has expired.
2025-12-03 10:12:48 [admin] [Login] [Login]: Web login failure in login attempt for administrator "admin" from 10.222.178.15
2025-12-03 10:13:00 [admin] [Login] [Login]: Logged in from 10.222.178.15 via web
2025-12-03 10:20:46 [admin] [Login] [Login]: Login attempted with invalid pending session ID.
2025-12-03 10:21:00 [admin] [Login] [Login]: Logged in from 10.222.178.15 via web
    
```

Figure 22 : Audit log details

6.2.4 Verify Logs Displayed in Splunk

1. Log in to the Windows machine where Splunk Enterprise is configured and log in to Splunk Enterprise.
2. Click the **Apps** menu and select **Search & Reporting**. The same link is also available in the Splunk Enterprise dashboard.

3. Enter index=<created_index> in the search bar and verify that the corresponding ESKM logs are displayed in the results.

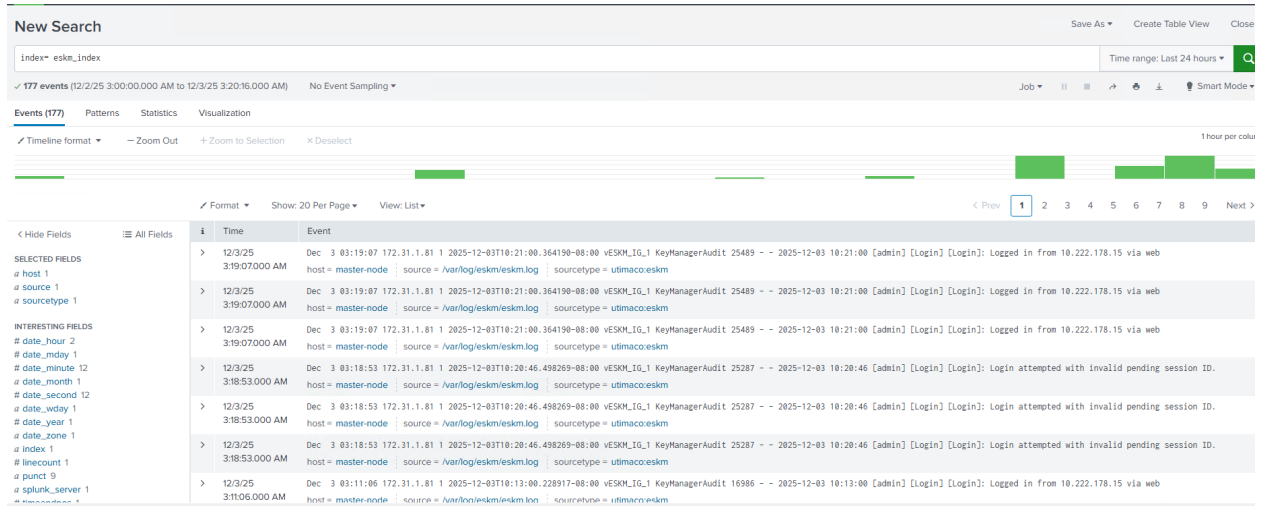


Figure 23 : ESKM logs displayed in Splunk

7 Troubleshooting

7.1 Common Issues

1. Verifying ESKM Logs on the Linux syslog-ng Server

- After configuring `eskm.conf`, verify logs are received by checking:

```
#tail -f /var/log/eskm/eskm.log
```

- Ensure syslog-ng is listening on port 514 (TCP/UDP):

```
#ss -tulpn | grep 514
```

2. Verifying Ports and Connectivity from Splunk Enterprise

- Ensure Splunk Enterprise is listening on port 9997 on your Windows machine:

```
#netstat -ano | findstr 9997
```

- Check that the receiving port is enabled in Splunk Enterprise at **Settings** → **Forwarding & Receiving** → **Receive Data** → **Port 9997**.

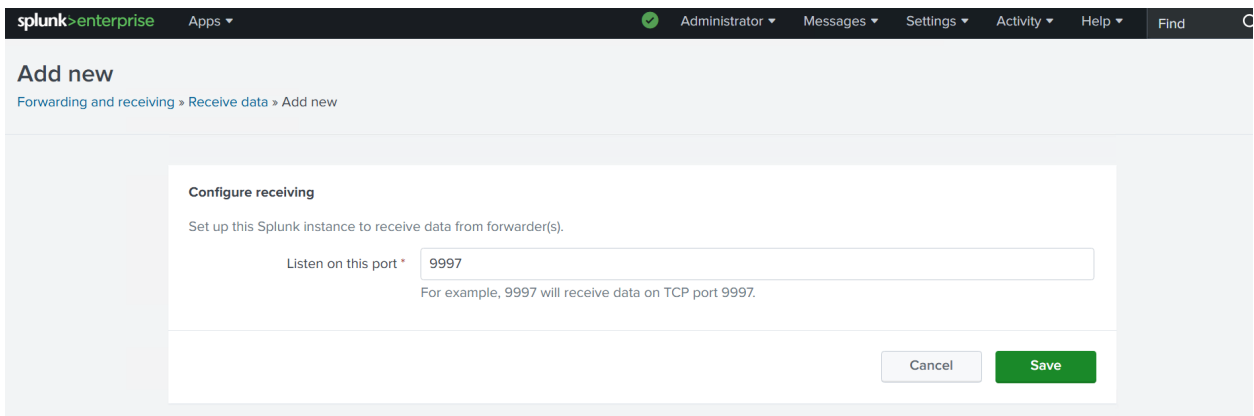


Figure 24 : Verify receiving port

3. Verifying Universal Forwarder Connectivity

- Confirm the UF service is running:

```
#/opt/splunkforwarder/bin/splunk status
```

- Verify the UF is monitoring the correct log file:

```
#/opt/splunkforwarder/bin/splunk list monitor
```

- Test connectivity from UF to Splunk Enterprise:

```
#nc -vz <SPLUNK_ENTERPRISE_IP> 9997
```

4. Verifying Logs Arrive in Splunk Enterprise

- Confirm the index exists under **Settings** → **Indexes** → **eskm_index**

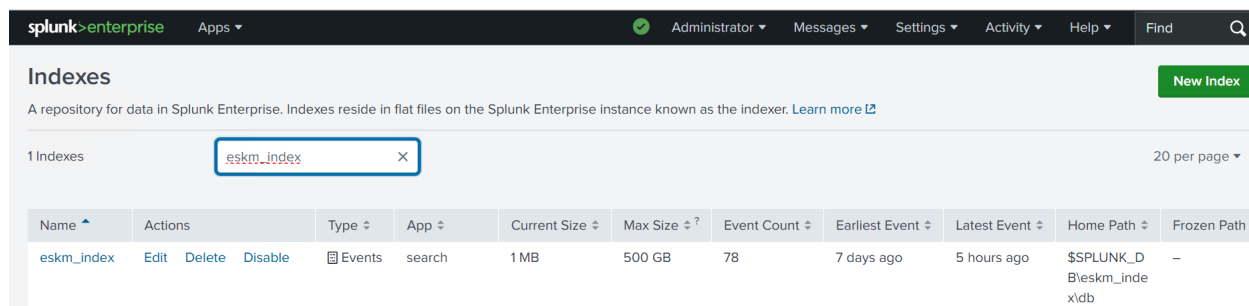


Figure 25 : Verify index

- Check if the UF has connected to Splunk by searching "index=_internal sourcetype=splunkd component=Metrics group=tcpin_connections".

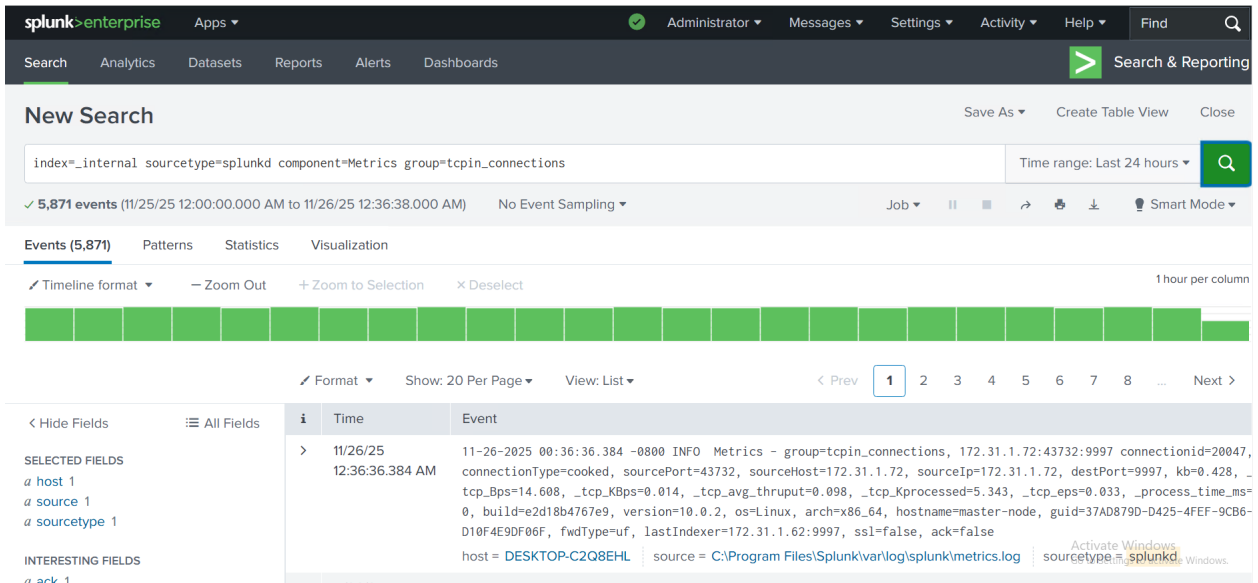


Figure 26 : Verify UF connection

5. Verifying Log Flow End-to-End

- Trigger an event on ESKM (login/logout, config change).
- Confirm the event appears in:
 - Linux syslog file (`/var/log/eskm/eskm.log`)
 - Splunk UF monitored file list
 - Splunk Enterprise search (`index=eskm_index`)

8 Contact and Support Information

You can reach us from Monday to Friday, 09.00 a.m. to 05.00 p.m., Central European Time (CET).

Utimaco IS GmbH
Krefelder Straße 220
52070 Aachen
Germany

RMA Query

If you need to send the device back to Utimaco IS GmbH, please open a new RMA case (Return Merchandise Authorization). We request that you use the following web address. RMA cases cannot be opened by email or phone.

<https://support.hsm.utimaco.com/support/rma/new>

Other Support Queries

- Mail (preferred contact method)
support@utimaco.com
Attach the diagnostic information to your email.
- Web portal
<https://support.hsm.utimaco.com/support/cases/new/>
The diagnostic information will be requested in our response if necessary.
- By phone
AMERICAS +1-844-UTIMACO (+1 844-884-6226)
EMEA +49 800-627-3081
APAC +81 800-919-1301
The diagnostic information will be requested in our response if necessary.

9 Appendices

9.1 Command Summary

Command	Purpose
<code>dnf install -y epel-release</code>	Enables the EPEL repository to access additional packages required for syslog-ng installation.
<code>dnf install -y syslog-ng</code>	Installs the syslog-ng service on Rocky Linux, which will receive syslog data from ESKM.
<code>wget -O splunkforwarder-10.0.2-e2d18b4767e9.x86_64.rpm "<Splunk_UF_Download_URL>"</code>	Downloads the Splunk Universal Forwarder installation package from Splunk's official repository.
<code>sudo rpm -i splunkforwarder-10.0.2-e2d18b4767e9.x86_64.rpm</code>	Installs the Splunk Universal Forwarder on the Rocky Linux syslog server.
<code>sudo /opt/splunkforwarder/bin/splunk start --accept-license</code>	Starts the Splunk Universal Forwarder for the first time and prompts for creating admin credentials.
<code>/opt/splunkforwarder/bin/splunk enable boot-start</code>	Configures the Universal Forwarder to automatically start on system boot.
<code>mkdir -p /var/log/eskm</code>	Creates a dedicated directory to store incoming ESKM syslog logs.

Command	Purpose
<code>chown root:root /var/log/eskm</code>	Sets correct ownership for the ESKM log directory so syslog-ng and Splunk UF can access it.
<code>chmod 750 /var/log/eskm</code>	Applies secure permissions to the ESKM log directory.
<code>tail -f /var/log/eskm/eskm.log</code>	Monitors ESKM logs in real time to verify syslog-ng is receiving events.
<code>/opt/splunkforwarder/bin/splunk status</code>	Checks the running status of the Splunk Universal Forwarder service.
<code>/opt/splunkforwarder/bin/splunk list monitor</code>	Displays the list of log files currently monitored by the Universal Forwarder.
<code>dnf install -y epel-release</code>	Enables the EPEL repository to access additional packages required for syslog-ng installation.
<code>dnf install -y syslog-ng</code>	Installs the syslog-ng service on Rocky Linux, which will receive syslog data from ESKM.
<code>wget -O splunkforwarder-10.0.2-e2d18b4767e9.x86_64.rpm "<Splunk_UF_Download_URL>"</code>	Downloads the Splunk Universal Forwarder installation package from Splunk's official repository.
<code>sudo rpm -i splunkforwarder-10.0.2-e2d18b4767e9.x86_64.rpm</code>	Installs the Splunk Universal Forwarder on the Rocky Linux syslog server.

Command	Purpose
<code>sudo /opt/splunkforwarder/bin/splunk start --accept-license</code>	Starts the Splunk Universal Forwarder for the first time and prompts for creating admin credentials.
<code>/opt/splunkforwarder/bin/splunk enable boot-start</code>	Configures the Universal Forwarder to automatically start on system boot.
<code>mkdir -p /var/log/eskm</code>	Creates a dedicated directory to store incoming ESKM syslog logs.
<code>chown root:root /var/log/eskm</code>	Sets correct ownership for the ESKM log directory so syslog-ng and Splunk UF can access it.
<code>chmod 750 /var/log/eskm</code>	Applies secure permissions to the ESKM log directory.
<code>tail -f /var/log/eskm/eskm.log</code>	Monitors ESKM logs in real time to verify syslog-ng is receiving events.
<code>/opt/splunkforwarder/bin/splunk status</code>	Checks the running status of the Splunk Universal Forwarder service.
<code>/opt/splunkforwarder/bin/splunk list monitor</code>	Displays the list of log files currently monitored by the Universal Forwarder.

Table 5: Splunk CLI commands

9.2 References

Title	Description	Document/Link
ESKM Installation Guide	Step-by-step guide for installing and configuring ESKM	<i>2021-0047 Installation and Replacement Guide</i>
Splunk Enterprise Windows Installation	Installation guide for Splunk Enterprise in Windows	<i>Install on Windows Splunk Docs</i>

Table 6: References