Jan 2024

Splunk4Ninjas - Data Onboarding

Lab Guide

Overview

This lab guide contains the step by step instructions for hands-on exercises done in the Splunk4Ninjas - Data Onboarding workshop. This workshop simulates the following:

- Monitoring a location on either your local Splunk instance or from a Splunk Universal/Heavy Forwarder
- Getting data in from a data source that may not have a Splunk app or add-on currently available

Please ensure that you have a copy of the workshop slide deck: https://splk.it/S4N-DataOnboarding

Prerequisites

Splunk Instance

In order to take part in the workshop exercises, you will need your own Splunk instance. You will either be provided an instance by your workshop host or you will need to enroll in the workshop to have an instance provisioned. Your host will let you know.

If you are instructed to enroll in today's workshop, you will need to have a Splunk.com account prior to enrolling. If you don't already have a Splunk.com account, please create one at https://www.splunk.com/en_us/sign-up.html before proceeding with the enrollment link provided by your host.

Knowledge Requirements

Attendees should have a base knowledge of the Splunk interface and understand key concepts such as:

- What is an index?
- What is a sourcetype?
- What is a data model?

⚠️ Troubleshooting Connectivity

If you experience connectivity issues with accessing either your workshop environment or the event page, please try the following troubleshooting steps. If you still experience issues please reach out to the team running your workshop.

- **Use Google Chrome** (if you're not already)
- If the event page (i.e. *https://show.splunk.com/event/<eventID>*) didn't load when you clicked on the link, try **refreshing the page**

- **Disconnect from VPN** (if you’re using one)
- **Clear your browser cache and restart your browser** (if using Google Chrome, go to: Settings > Privacy and security > Clear browsing data)
- **Try using private browsing mode** (e.g. Incognito in Google Chrome) to rule out any cache issues
- **Try using another computer** such as your personal computer - all you need is a web browser! Cloud platforms like AWS can often be blocked on corporate laptops.

Table of Contents

Overview 1
Prerequisites 1
Table of Contents 3
Lab 0 - Register/Enroll and Login to Instance 4
Description 4
Steps 4
Lab 1 - File Monitor 8
Description 8
Option 1: Monitoring Through the GUI 8
Monitor the Syslog Directory 8
Adjust the Input Settings 9
Review and Confirm Your Monitoring Input 10
Option 2: Monitoring Through the CLI 12
SSH into Your Provided Machine 12
Monitor the Syslog Directory Through inputs.conf 13
Reload and confirm the monitoring input 15
Lab 2 - Data Parsing 16
Description 16
Select the badge.log File as your Source 16
Set the Source Type 17
Adjust the Input Settings 19
Submit and Search Your Data 20
Set Up the Add-on Builder 21
Lab 3 - Field Extraction and CIM Compliance 26
Description 26
Validate the Empty Authentication Dashboard 26
Extract Fields from the Badge Data 27
Map Source Type to the Authentication Data Model 30
Re-accelerate Your Data Model 34
Verify the Authentication Dashboard 36
Appendix 37
Troubleshooting for Lab 1, Option 2: Monitoring Through the CLI 37
Optional Activity: Lab 2, Tasks 1-4 Accomplished Through the CLI 41
Establish a Custom “badge” Source Type 41
Use Oneshot to Ingest and View badge.log Data 42

Lab 0 - Register/Enroll and Login to Instance

Description

You will need a Splunk training instance to take part in the labs for the workshop. In this lab, you will register for your own Splunk instance to use for the workshop.

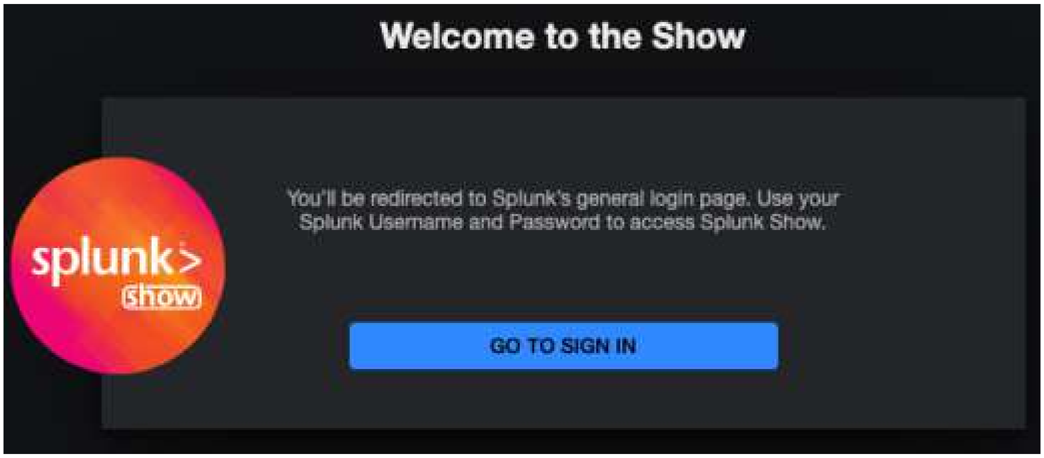
🔑 **Has your Host already provided you a link for your instance and login credentials?**
If your workshop host has already provided you with an instance link as well as login credentials, **you do NOT need to follow these instructions for Lab 0**. You can instead skip straight to Lab 1 - File Monitor!

Steps

Instance Creation and Logon

---

1. Browse to https://show.splunk.com - or the enrollment link provided by the host - and log in using your Splunk.com account credentials:



Welcome to the Show

You'll be redirected to Splunk's general login page. Use your Splunk Username and Password to access Splunk Show.

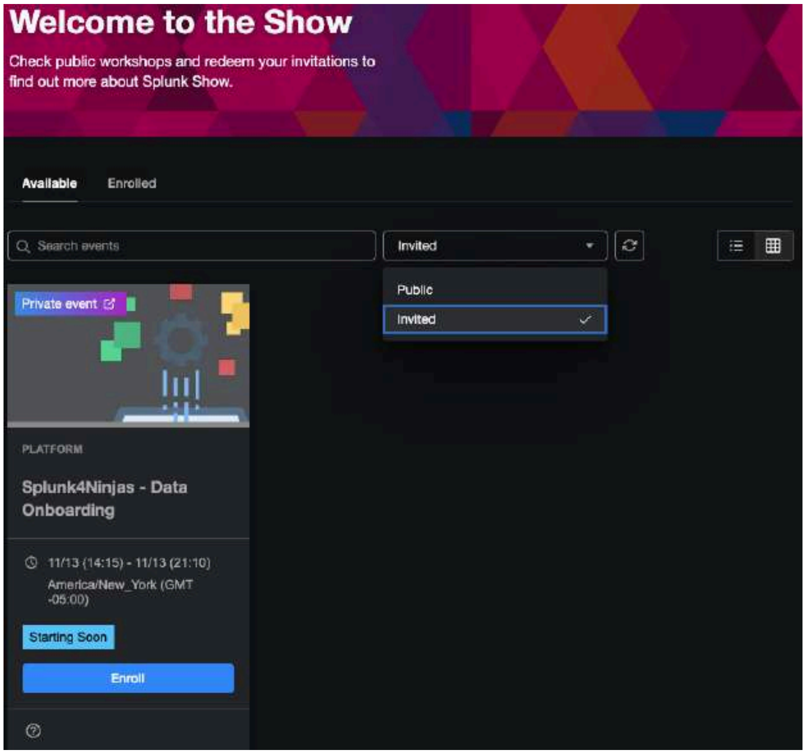
Don't have a Splunk.com account?

If you do not have a Splunk.com account, create one in a few minutes by clicking here. After creating your Splunk.com account, please navigate back to https://show.splunk.com or use the enrollment link your host provides.

---

2. Once logged into Splunk Show, you will see the event page for the event that you have been invited to. If nothing is showing, try selecting “Invited” from the dropdown list.

   (View if you go directly to https://show.splunk.com and login)



Welcome to the Show

Check public workshops and redeem your invitations to find out more about Splunk Show.

Invited

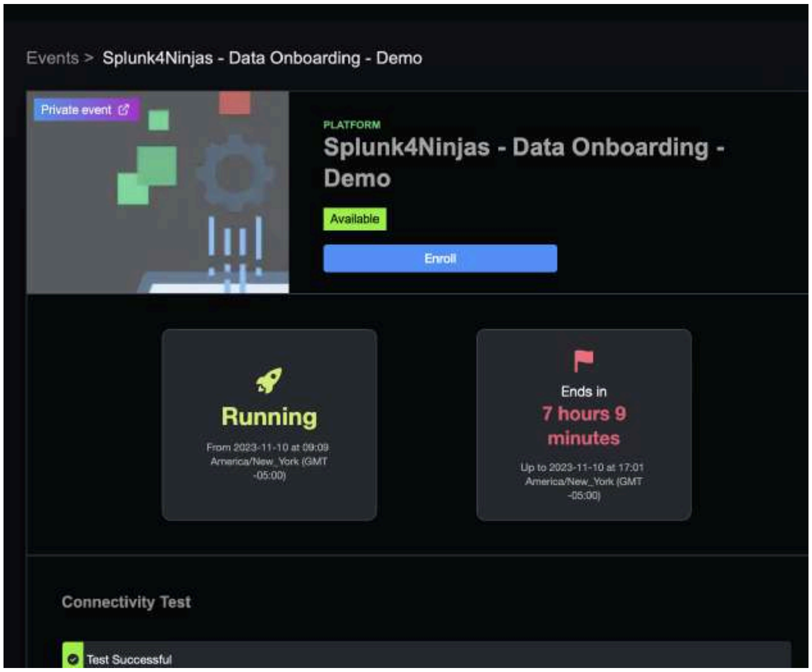
PLATFORM

Splunk4Ninjas - Data Onboarding

11/13 (14:15) - 11/13 (21:10) America/New_York (GMT -05:00)

Starting Soon

(View from the enrollment link directly)



Events > Splunk4Ninjas - Data Onboarding - Demo

PLATFORM

Splunk4Ninjas - Data Onboarding - Demo

Available

Running

From 2023-11-10 at 09:09 America/New_York (GMT -05:00)

Ends in

7 hours 9 minutes

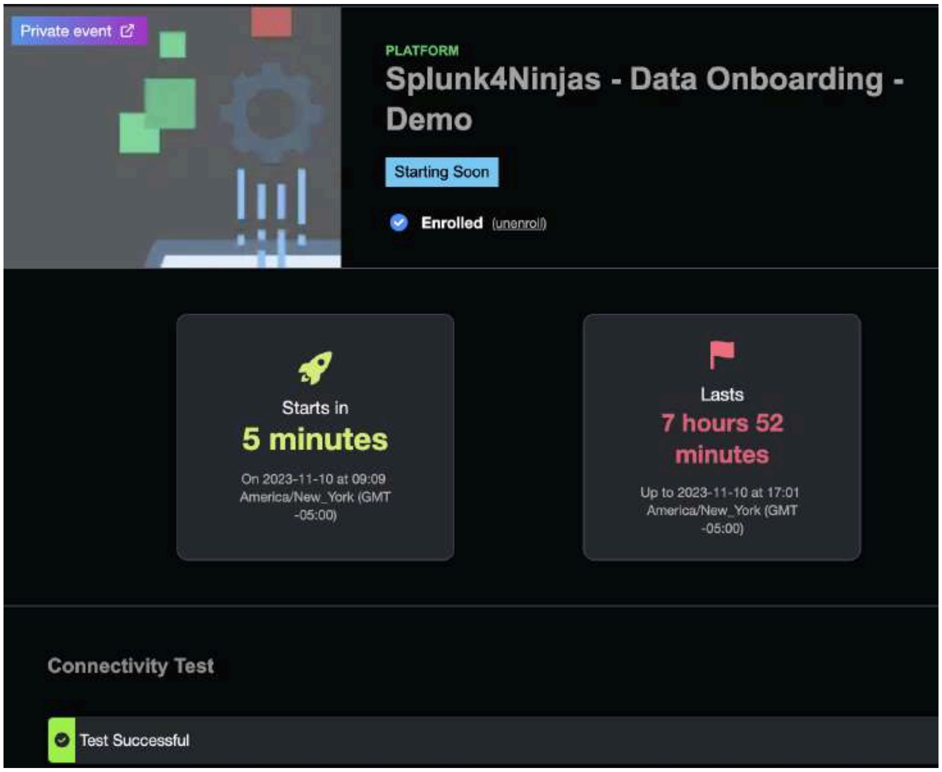
Up to 2023-11-10 at 17:01 America/New_York (GMT -05:00)

Connectivity Test

Test Successful

3. Click on **Enroll** to join the event.

4. The page will refresh and the event will now display ‘Enrolled’



Private event

PLATFORM

Splunk4Ninjas - Data Onboarding - Demo

Starting Soon

Enrolled (unenroll)

Starts in
5 minutes
On 2023-11-10 at 09:09 America/New_York (GMT -05:00)

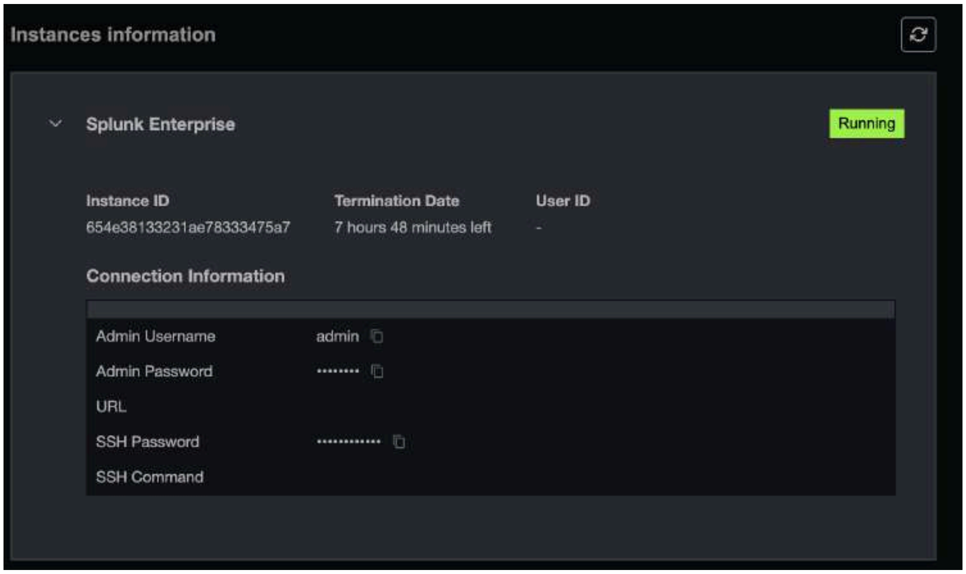
Lasts
7 hours 52 minutes
Up to 2023-11-10 at 17:01 America/New_York (GMT -05:00)

Connectivity Test

Test Successful

5. Once the workshop starts, your individual environment will start up.

6. Scroll down the page to the **Instances Information** section and expand the **Splunk Enterprise** section to locate the URL and login credentials for your lab environment.



Instances information

Splunk Enterprise

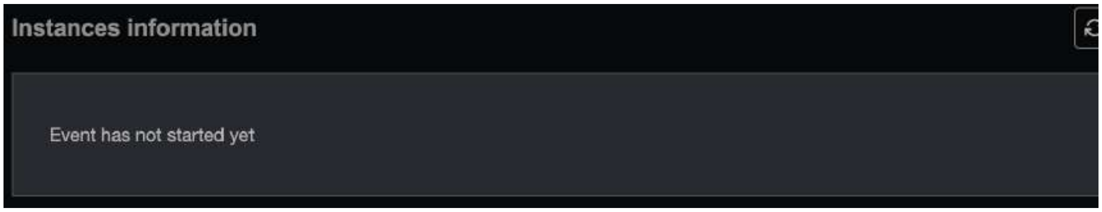
Running

Instance ID	Termination Date	User ID
654e38133231ae78333475a7	7 hours 48 minutes left	-

Connection Information

Admin Username	admin
Admin Password	••••••••
URL	
SSH Password	••••••••••••
SSH Command	

If you don’t see any connection information displayed yet, it means that your lab environment has not yet fully provisioned. Please check this page again in a few minutes.



Instances information

Event has not started yet

🕑 Lab environment expiration

All Splunk instances that are part of this workshop will automatically be shut down at the termination date specified under your instance information so feel free to continue to explore your lab environment until then!

Lab 1 - File Monitor

Description

Firewall logs collected by a Syslog server are stored on the server locally. We will bring those firewall logs into Splunk by monitoring the files and directories where those logs are stored. With Splunk Enterprise, we can do this from either the Splunk Web interface (GUI) or the inputs.conf file through the CLI:

- Option 1 - Monitoring through the GUI
- Option 2 - Monitoring through the CLI

To configure an input, a stanza needs to be added to the inputs.conf file in the **$SPLUNK_HOME/etc/system/local/** directory or an application directory in **$SPLUNK_HOME/etc/apps/<app_name>/local/**. The directory paths are locations on the machine that runs Splunk Enterprise or the Universal Forwarder. Settings we adjust in the GUI will be reflected in those underlying files.

ℹ️ **inputs.conf**

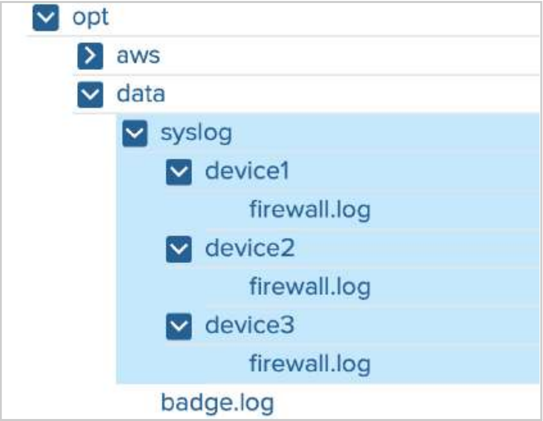
To learn more about the inputs.conf file, click here.

Option 1: Monitoring Through the GUI

Monitor the Syslog Directory

1. Select Source by navigating to **Settings > Add Data > Monitor > Files & Directories** and clicking on **Browse**.

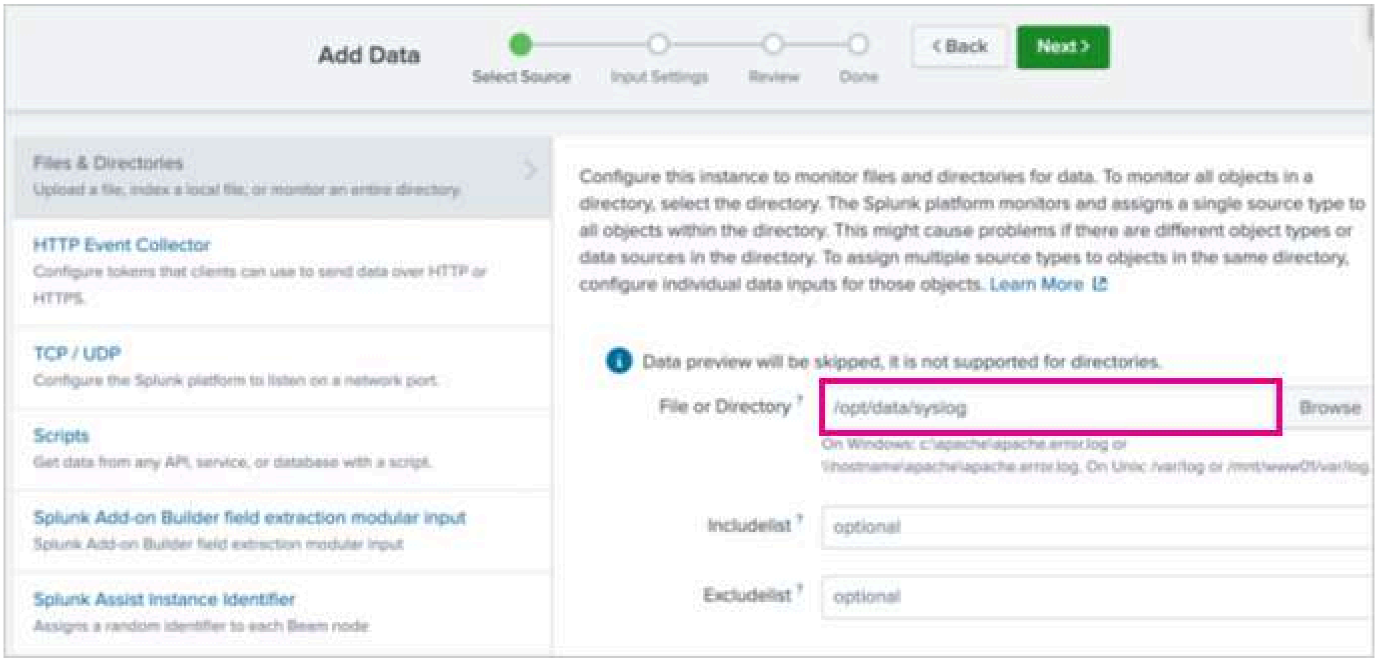
2. Select the **opt > data > syslog** directory. Ensure all devices and firewall.log files are highlighted and click the **Select** button in the bottom right of the pop up.



3. Back on the **Select Source** page, your **File or Directory** field should read:

```
/opt/data/syslog
```

With this set, click **Next**.



Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

Splunk Add-on Builder field extraction modular input
Splunk Add-on Builder field extraction modular input

Splunk Assist Instance Identifier
Assigns a random identifier to each Beam node

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. Learn More

Data preview will be skipped, it is not supported for directories.

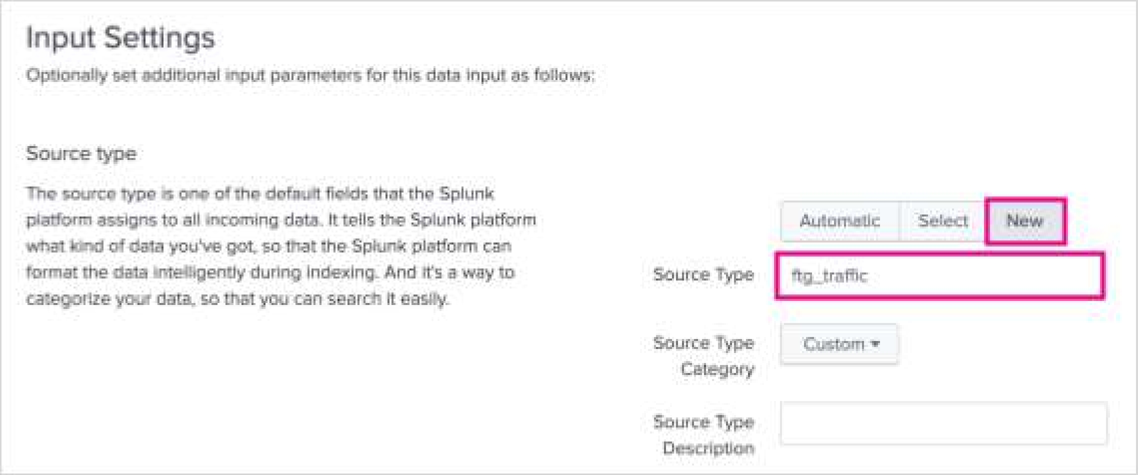
File or Directory ? /opt/data/syslog
On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

Includelist ? optional

Excludelist ? optional

Adjust the Input Settings

4. On the **Input Settings** page, set the Source type by selecting **New** and entering **ftg_traffic** for the **Source Type** field:



Input Settings

Optionally set additional input parameters for this data input as follows:

Source type

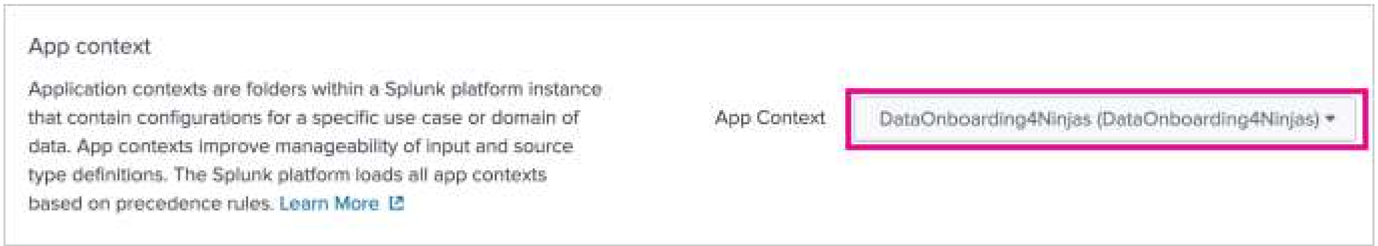
The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Source Type: ftg_traffic

Source Type Category: Custom ▾

Source Type Description:

5. Set the **App Context** to **DataOnboarding4Ninjas**:

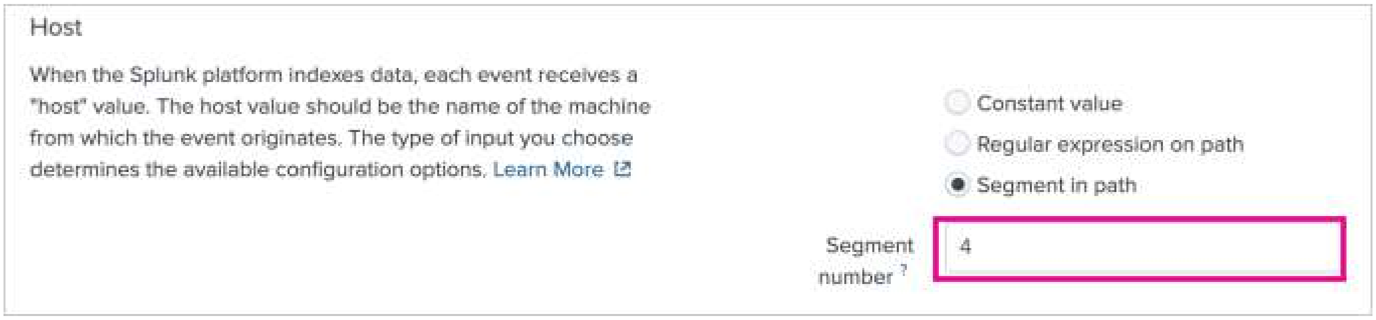


App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More

App Context: DataOnboarding4Ninjas (DataOnboarding4Ninjas) ▾

6. For the **Host** select **Segment in path** and set the **Segment number** to **4**:



Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More

○ Constant value
○ Regular expression on path
● Segment in path

Segment number: 4

ℹ️ Segment in path

These settings specify that the “host” value assigned to the events will align with whatever comes after the 4th slash in the directory path. We are monitoring firewall logs from the following directories:

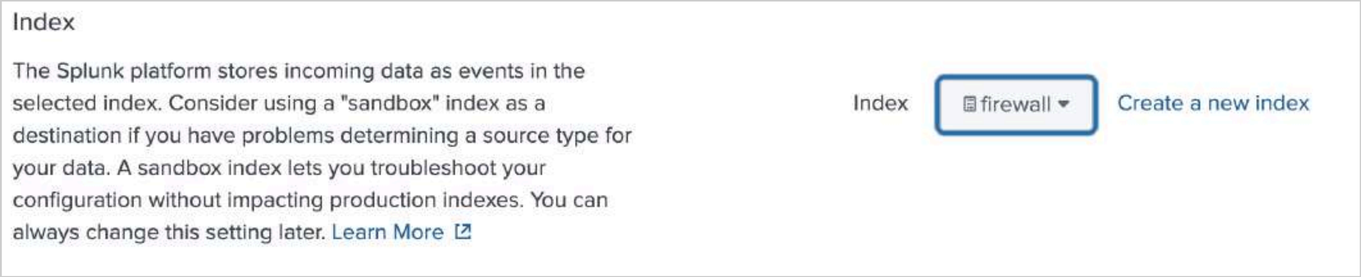
/opt/data/syslog/device1
/opt/data/syslog/device2
/opt/data/syslog/device3

which means that the device# is the 4th segment of the file path and will get assigned as the host depending on where the logs come from, i.e:

/opt = segment 1
/data = segment 2
/syslog = segment 3
/device* = segment 4

---

7. Set the **Index** to **firewall**:



Index

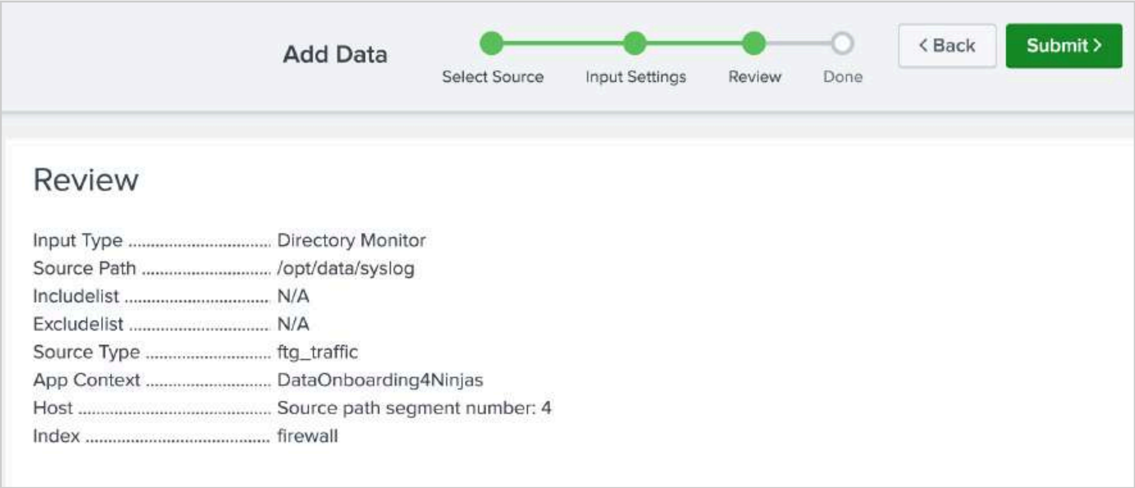
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

Index: firewall

8. Select **Review** in the top right corner.

Review and Confirm Your Monitoring Input

9. Ensure your input information is accurate and click on **Submit**.



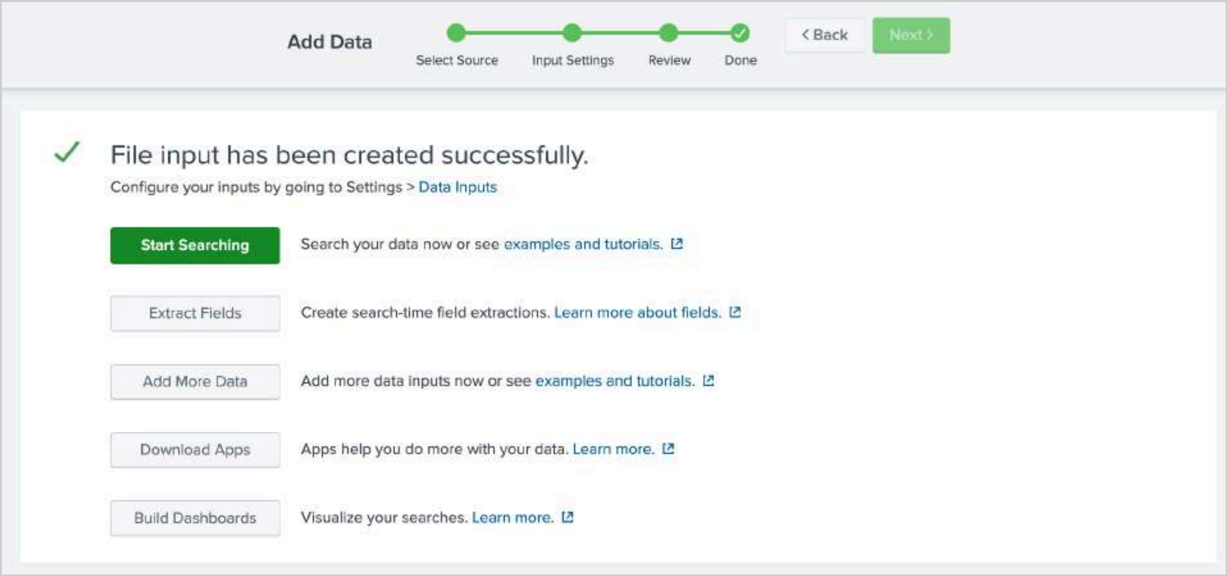
Review

Input Type .... Directory Monitor
Source Path .... /opt/data/syslog
Includelist .... N/A
Excludelist .... N/A
Source Type .... ftg_traffic
App Context DataOnboarding4Ninjas
Host .... Source path segment number: 4
Index .... firewall

10. Validate your data by clicking on **Start Searching** and entering the following search into the search bar:

```
| tstats count where index=firewall by host source
```

Set the time range picker to **All Time**.



✓ File input has been created successfully.

Configure your inputs by going to Settings > Data Inputs

Search your data now or see examples and tutorials.

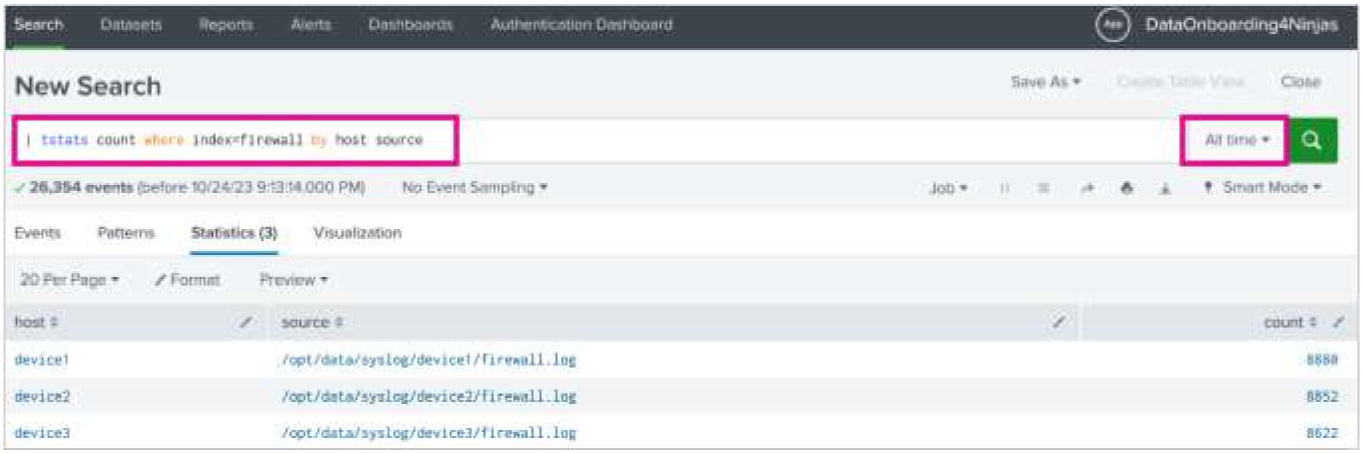
Create search-time field extractions. Learn more about fields.

Add more data inputs now or see examples and tutorials.

Apps help you do more with your data. Learn more.

Visualize your searches. Learn more.

Results should be a table with 3 columns:



```
| tstats count where index=firewall by host source
```

✓ 26,354 events (before 10/24/23 9:13:14.000 PM) No Event Sampling ▾

host	source	count
device1	/opt/data/syslog/device1/firewall.log	8880
device2	/opt/data/syslog/device2/firewall.log	8852
device3	/opt/data/syslog/device3/firewall.log	8622

Skip Option 2 if you have already completed Option 1 (GUI).

>> Jump to Lab 2 <<

Option 2: Monitoring Through the CLI

SSH into Your Provided Machine

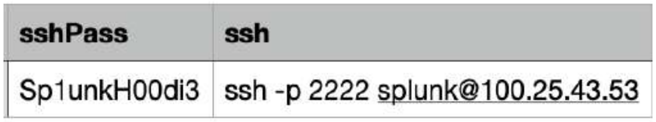
1. Open the Terminal app / CLI
2. Use your given SSH command to log into your individual machine.

🔑 **SSH Details**

The specific IP address for your instance will either be provided to you by the workshop host or will be presented alongside your other workshop instance information within the Splunk Show portal.

If you had to enroll in today's workshop (via Splunk Show) then please log in to https://show.splunk.com to locate your unique SSH command.

Example SSH details:



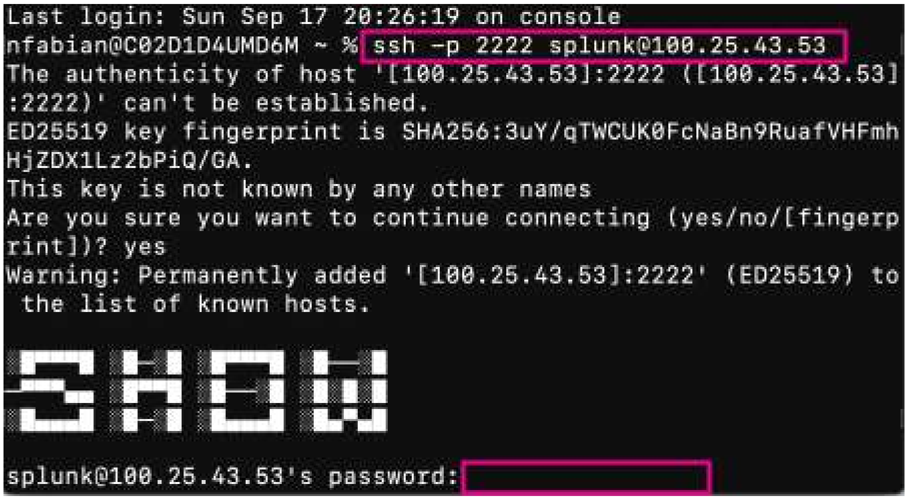
sshPass	ssh
Sp1unkH00di3	ssh -p 2222 splunk@100.25.43.53

Example SSH command to copy/paste:

```
ssh -p 2222 splunk@100.25.43.53
```

Note: Replace the IP address with the IP address of your workshop instance.

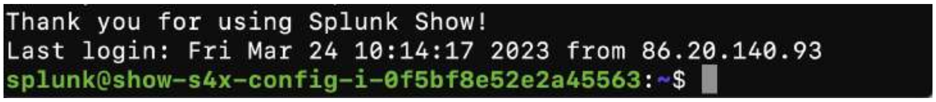
When prompted, enter the SSH password you were provided (this is different from the Splunk login password.)



```
Last login: Sun Sep 17 20:26:19 on console
nfabian@C02D1D4UMD6M ~ % ssh -p 2222 splunk@100.25.43.53
The authenticity of host '[100.25.43.53]:2222 ([100.25.43.53]
:2222)' can't be established.
ED25519 key fingerprint is SHA256:3uY/qTWCUK0FcNaBn9RuafVHFmh
HjZDX1Lz2bPiQ/GA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerp
rint])? yes
Warning: Permanently added '[100.25.43.53]:2222' (ED25519) to
 the list of known hosts.
```

```
splunk@100.25.43.53's password:
```

3. Upon entering the correct password, you should be logged into the remote machine:



```
Thank you for using Splunk Show!
Last login: Fri Mar 24 10:14:17 2023 from 86.20.140.93
splunk@show-s4x-config-i-0f5bf8e52e2a45563:~$
```

Monitor the Syslog Directory Through inputs.conf

4. Firstly, we will view the current **inputs.conf** settings. Start by switching to the root user:

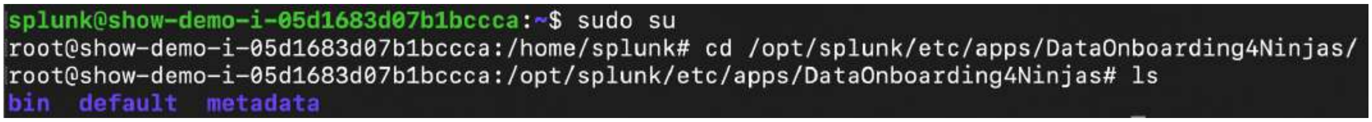
```
sudo su
```

5. Navigate to the **/opt/splunk/etc/apps/DataOnboarding4Ninjas** directory and list the underlying directories:

```
cd /opt/splunk/etc/apps/DataOnboarding4Ninjas/

ls
```

We should see three directories listed: **bin**, **default** and **metadata**:

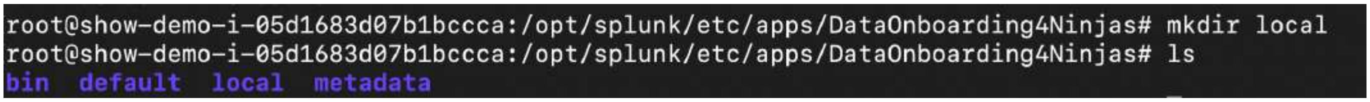


```
splunk@show-demo-i-05d1683d07b1bccca:~$ sudo su
root@show-demo-i-05d1683d07b1bccca:/home/splunk# cd /opt/splunk/etc/apps/DataOnboarding4Ninjas/
root@show-demo-i-05d1683d07b1bccca:/opt/splunk/etc/apps/DataOnboarding4Ninjas# ls
bin  default  metadata
```

6. Splunk app configuration changes should ONLY be made in the **local** directory of an app. Since the local directory does not yet exist, we need to create one:

```
mkdir local
```

Note: Ensure the folder name is all lowercase

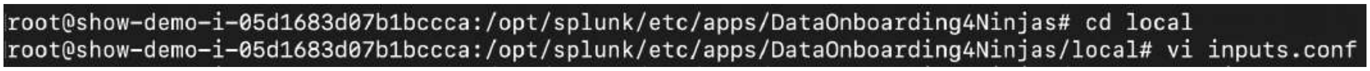


```
root@show-demo-i-05d1683d07b1bccca:/opt/splunk/etc/apps/DataOnboarding4Ninjas# mkdir local
root@show-demo-i-05d1683d07b1bccca:/opt/splunk/etc/apps/DataOnboarding4Ninjas# ls
bin  default  local  metadata
```

7. We will now add a monitoring stanza to the **inputs.conf** file to instruct Splunk to monitor our firewall log files. To do this, navigate to the newly created **local** directory and open the **inputs.conf** file to edit:

```
cd local

vi inputs.conf
```



```
root@show-demo-i-05d1683d07b1bccca:/opt/splunk/etc/apps/DataOnboarding4Ninjas# cd local
root@show-demo-i-05d1683d07b1bccca:/opt/splunk/etc/apps/DataOnboarding4Ninjas/local# vi inputs.conf
```

📝 **vi (Visual Editor)**

vi is a text editor used particularly for UNIX machines. There are many cheat sheets available online to help you navigate the commands when working with the editor. There are also other options for editing Splunk .conf files in Linux, such as nano.

---

8. Press the “ **i** ” key to start editing the file:

```
i
```

9. Within the configuration file, type or paste in the following stanza:

```
[monitor:///opt/data/syslog/*/firewall.log]
sourcetype = fgt_traffic
index = firewall
host_segment = 4
```

ℹ️ This stanza defines the input as firewall logs within the syslog directory. The data is being assigned a sourcetype of **fgt_traffic** and sent to the **firewall** index and assigning the host name to the **4th segment of the directory path**. In this case the host hame will be assigned whatever directory follows **/syslog/** in the stated path.

---

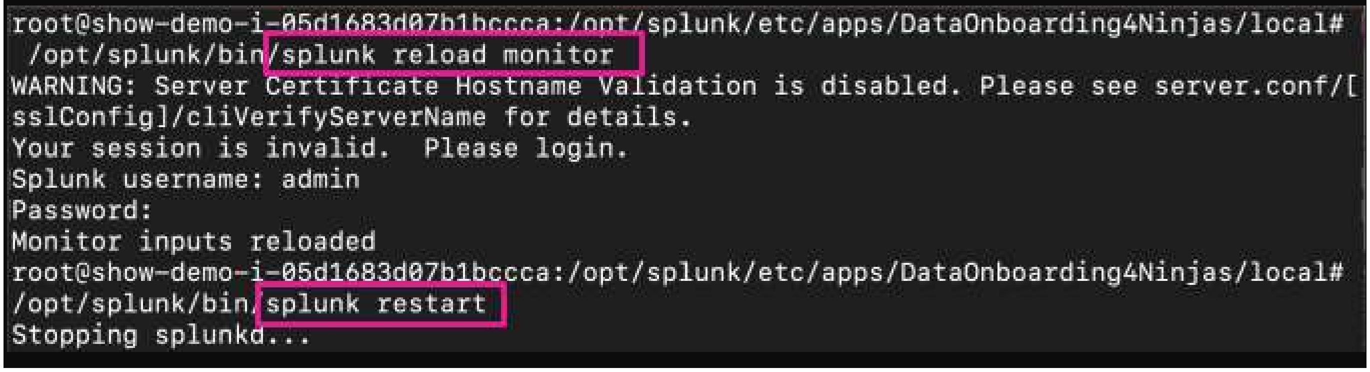
10. Exit the vi editor by pressing the **escape** key then typing **:wq** and hitting **enter**. This is telling the editor to save and exit back to the main CLI.

Reload and confirm the monitoring input

11. Reload the monitor input and restart Splunk:

```
/opt/splunk/bin/splunk reload monitor

sudo /opt/splunk/bin/splunk restart
```

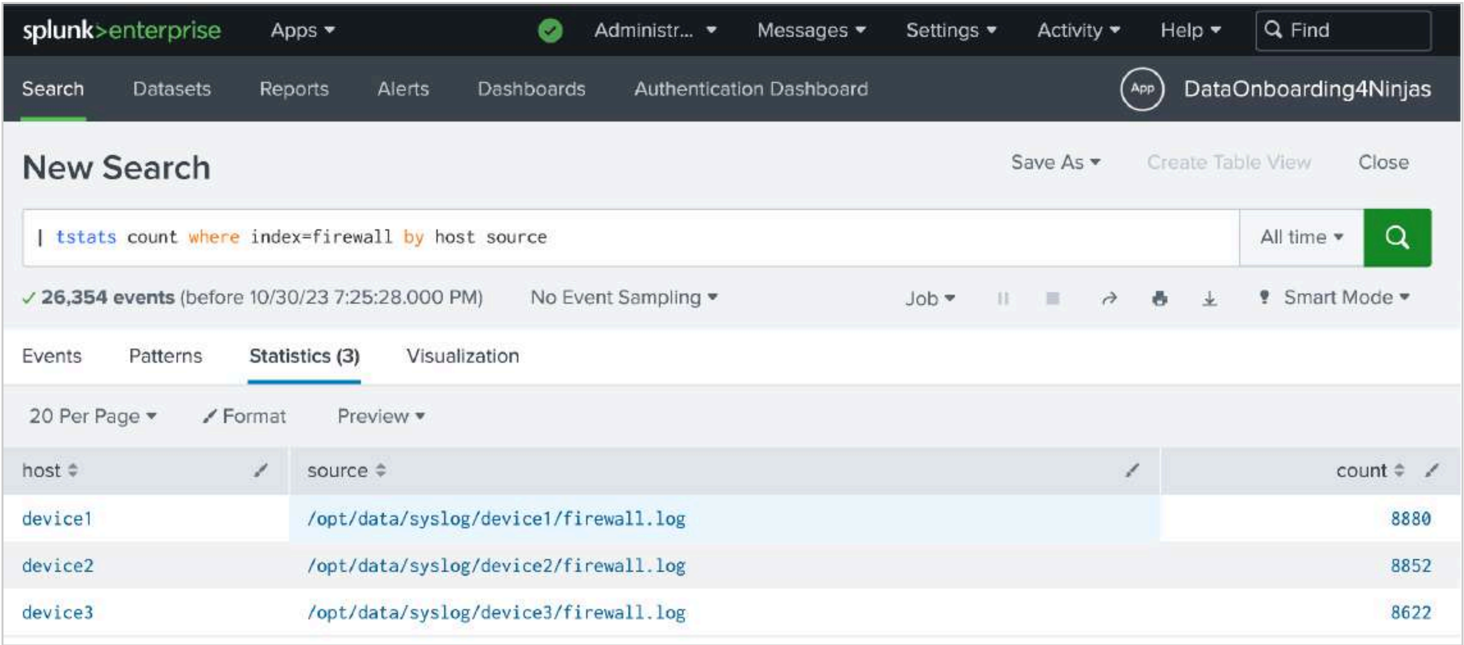


```
root@show-demo-i-05d1683d07b1bccca:/opt/splunk/etc/apps/DataOnboarding4Ninjas/local#
 /opt/splunk/bin/splunk reload monitor
WARNING: Server Certificate Hostname Validation is disabled. Please see server.conf/[
sslConfig]/cliVerifyServerName for details.
Your session is invalid.  Please login.
Splunk username: admin
Password:
Monitor inputs reloaded
root@show-demo-i-05d1683d07b1bccca:/opt/splunk/etc/apps/DataOnboarding4Ninjas/local#
/opt/splunk/bin/splunk restart
Stopping splunkd...
```

12. We now need to confirm that events are being ingested. To do this, log back in to Splunk (you will have been logged out due to the restart command we ran above) and navigate to **Apps > DataOnboarding4Ninjas**. Run the following search over **All Time**:

```
| tstats count where index=firewall by host source
```

13. Results should be a table with 3 columns:



```
| tstats count where index=firewall by host source
```

All time

✓ 26,354 events (before 10/30/23 7:25:28.000 PM)   No Event Sampling

host	source	count
device1	/opt/data/syslog/device1/firewall.log	8880
device2	/opt/data/syslog/device2/firewall.log	8852
device3	/opt/data/syslog/device3/firewall.log	8622

Lab 2 - Data Parsing

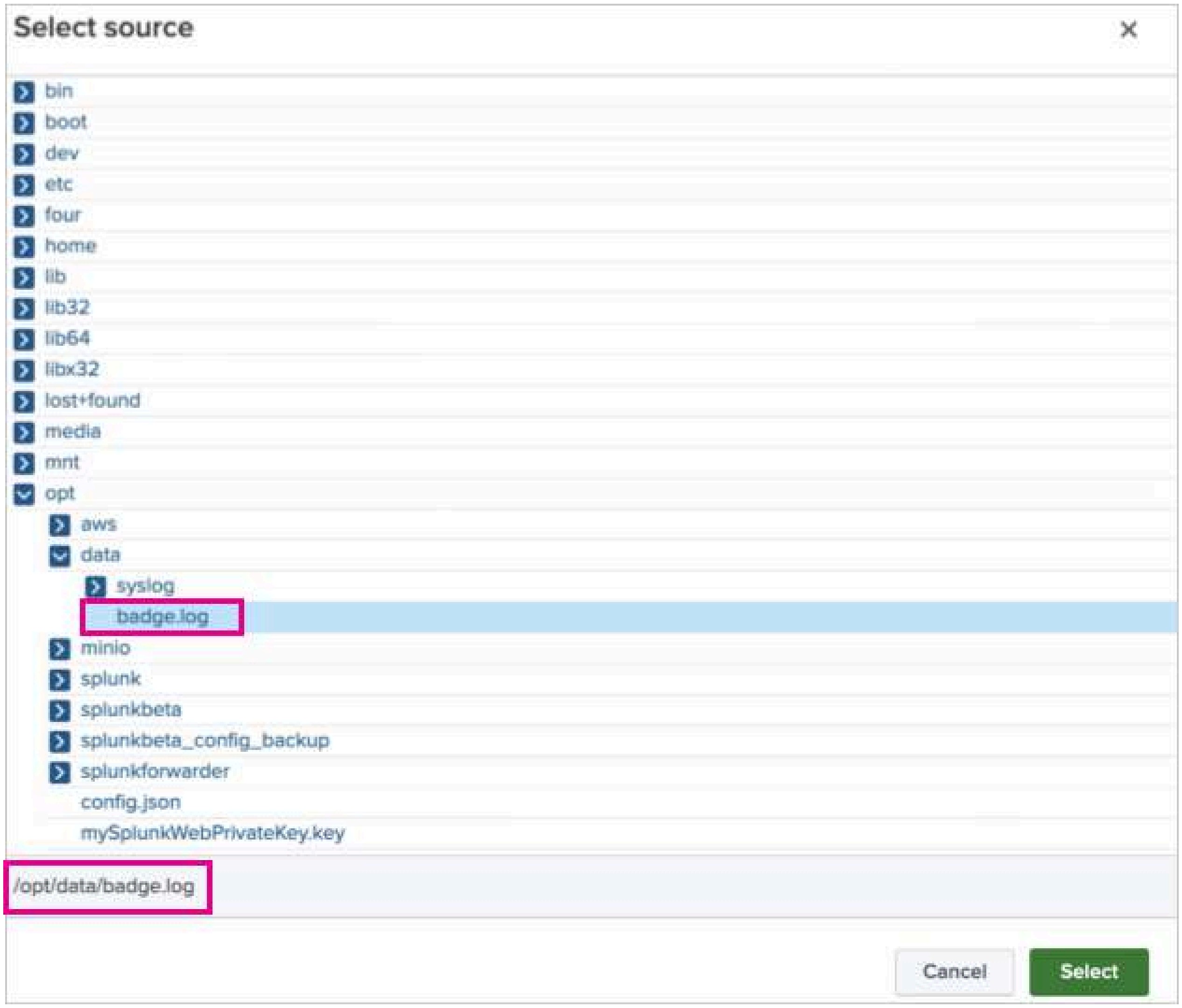
Description

In this activity, we ingest badge.log data into Splunk a single time (rather than monitoring continuously). We will set up a source type to correctly parse the data into individual events and then we will pivot into the Splunk Add-on Builder app where we import our source type into a new Add-on named ‘badge’.

This lab will be completed in the UI but several tasks can also be done in the CLI. See the Appendix Optional Activity on how tasks 1-4 can be accomplished through the CLI.

Select the badge.log File as your Source

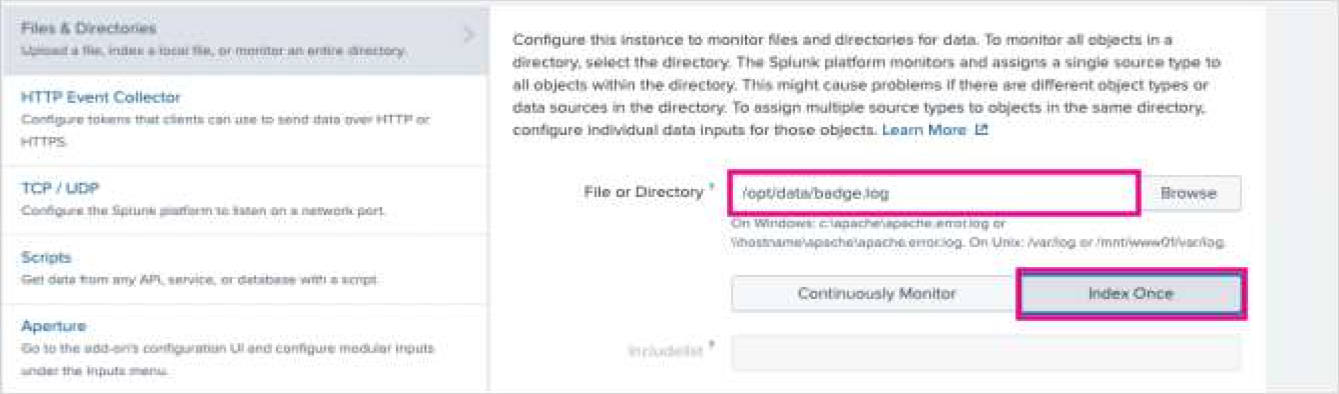
1. Navigate to **Settings > Add Data > Monitor > Files & Directories** and click on **Browse**.
2. Browse to **opt > data** and select **badge.log**.



/opt/data/badge.log

3. Ensure your **File or Directory** field now contains **/opt/data/badge.log**.

4. Select **Index Once** and click on **Next**.



Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

Aperture
Go to the add-on's configuration UI and configure modular inputs under the Inputs menu.

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. Learn More

File or Directory *: /opt/data/badge.log

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

ℹ️ Index Once

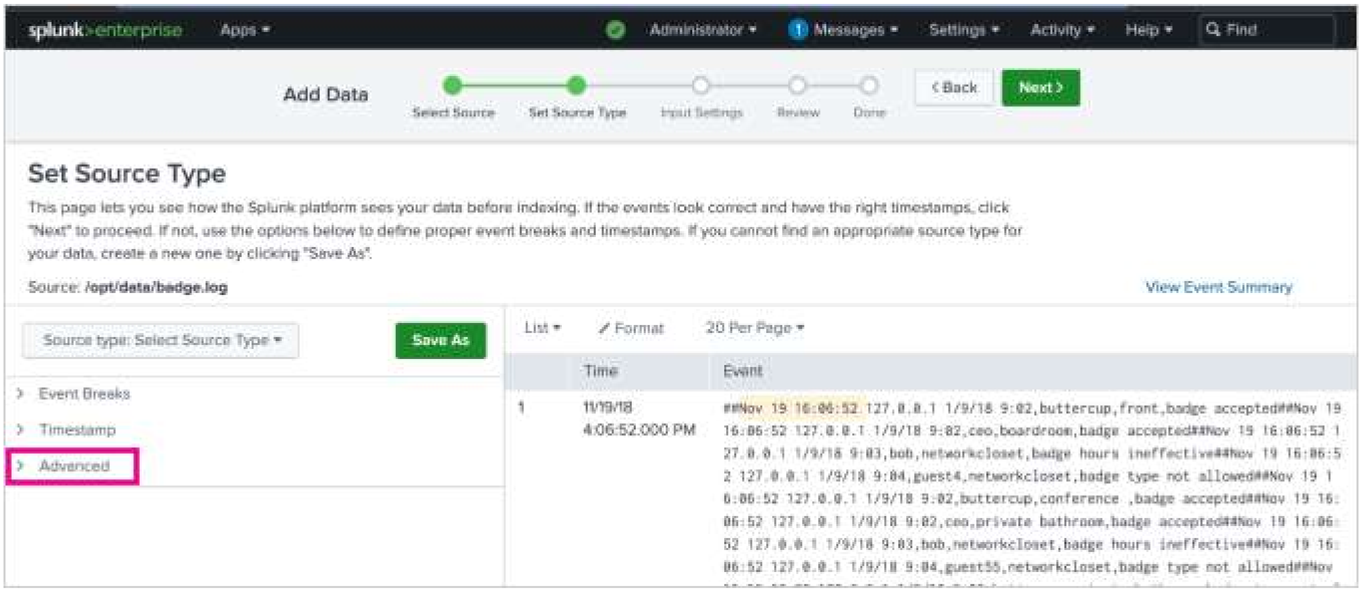
Selecting **Index Once** is equivalent to a 'oneshot' command in the CLI. This tells Splunk to read the file once, rather than establishing a continuous monitor of the file. This could be useful if there are segregated systems offline that cannot connect to Splunk; you can download the file and ingest it one time to enrich data or help investigate. This is also useful when testing data!

Set the Source Type

5. We now need to verify our data parsing settings. In the data preview pane on the right of the **Set Source Type** page we can see that the data is not getting ingested in the correct format; it is coming in as one big event rather than individual events, so we need to set a new source type to rectify this.

   On the left of the page, expand out the **Advanced** section and adjust the source type settings to match the following:

Name	**Value**
SHOULD_LINEMERGE	false
LINE_BREAKER	(##)
TIME_PREFIX	\d+\.\d+\.\d+\.\d+\s
TIME_FORMAT	%m/%d/%y %H:%M
MAX_TIMESTAMP_LOOKAHEAD	14
TRUNCATE	1000



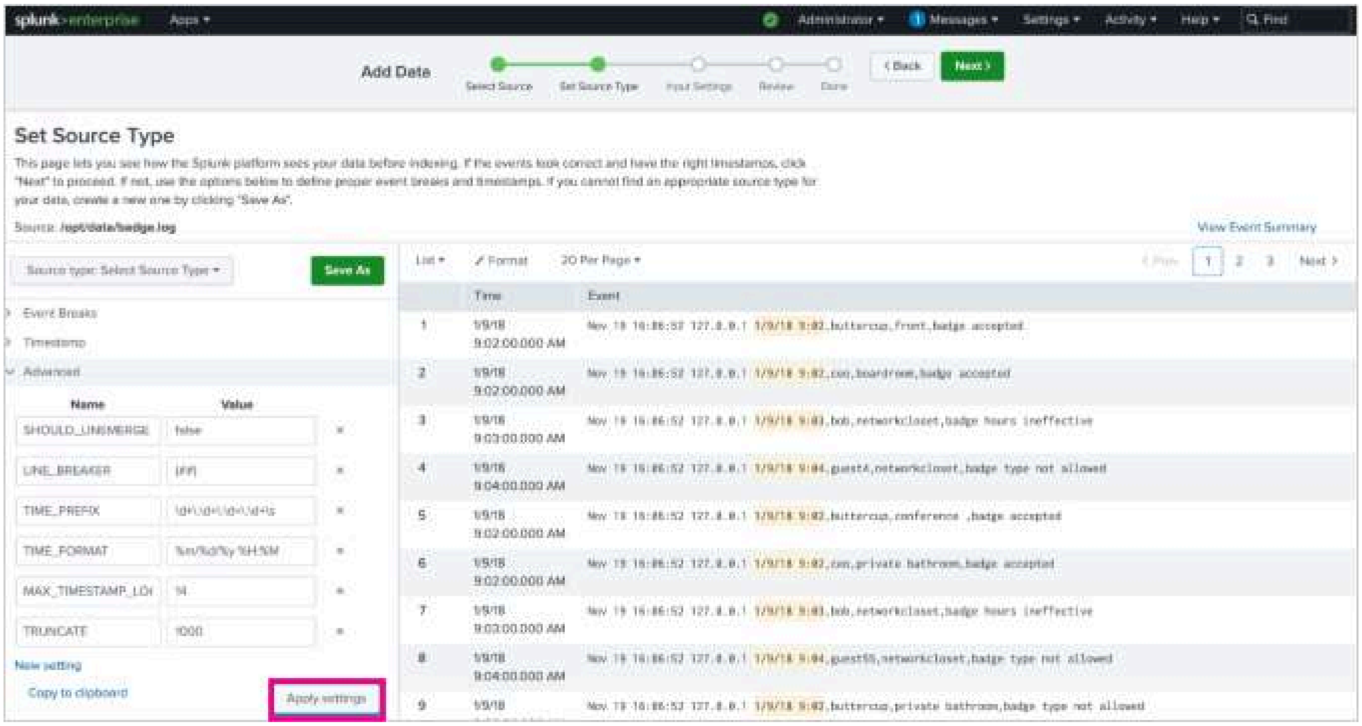
Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: **/opt/data/badge.log**

	Time	Event
1	11/19/18 4:06:52.000 PM	##Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,buttercup,front,badge accepted##Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,ceo,boardroom,badge accepted##Nov 19 16:06:52 127.0.0.1 1/9/18 9:03,bob,networkcloset,badge hours ineffective##Nov 19 16:06:52 127.0.0.1 1/9/18 9:04,guest4,networkcloset,badge type not allowed##Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,buttercup,conference ,badge accepted##Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,ceo,private bathroom,badge accepted##Nov 19 16:06:52 127.0.0.1 1/9/18 9:03,bob,networkcloset,badge hours ineffective##Nov 19 16:06:52 127.0.0.1 1/9/18 9:04,guest55,networkcloset,badge type not allowed##Nov

6. Click on **Apply Settings -** the single event will now be broken into individual events.



Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: **/opt/data/badge.log**

Name	Value
SHOULD_LINEMERGE	false
LINE_BREAKER	(##)
TIME_PREFIX	\d+\.\d+\.\d+\.\d+\s
TIME_FORMAT	%m/%d/%y %H:%M
MAX_TIMESTAMP_LOt	14
TRUNCATE	1000

	Time	Event
1	1/9/18 9:02:00.000 AM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,buttercup,front,badge accepted
2	1/9/18 9:02:00.000 AM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,ceo,boardroom,badge accepted
3	1/9/18 9:03:00.000 AM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:03,bob,networkcloset,badge hours ineffective
4	1/9/18 9:04:00.000 AM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:04,guest4,networkcloset,badge type not allowed
5	1/9/18 9:02:00.000 AM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,buttercup,conference ,badge accepted
6	1/9/18 9:02:00.000 AM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,ceo,private bathroom,badge accepted
7	1/9/18 9:03:00.000 AM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:03,bob,networkcloset,badge hours ineffective
8	1/9/18 9:04:00.000 AM	Nov 19 16:06:52 127.0.0.1 1/9/18 9:04,guest55,networkcloset,badge type not allowed
9	1/9/18	Nov 19 16:06:52 127.0.0.1 1/9/18 9:02,buttercup,private bathroom,badge type not allowed

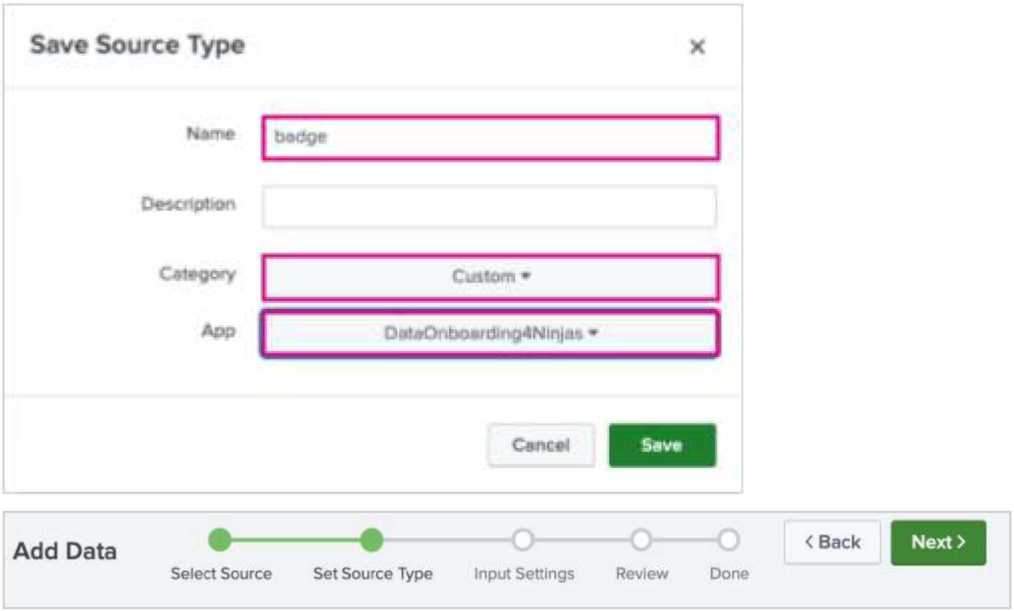
7. Now save the new source type by clicking on **Save As**.

8. For the source type name enter "**badge**".

9. Set the **Category** as **Custom**.

10. For the **App** select **DataOnboarding4Ninjas**.

11. Click **Save** and **Next**.



Save Source Type

Name: badge

Description:

Category: Custom

App: DataOnboarding4Ninjas

ℹ️ Saving Source Types

It is best practice to save source types to the specific apps they operate within rather than having them saved to the default Search & Reporting app, which is why we select DataOnboarding4Ninjas.

After saving, there may be additional settings added to the source type. For the purposes of this lab, we do not need to worry about these.

12. Upon saving, a badge sourcetype will now be visible in the props.conf for the DataOnboarding4Ninjas app. The props.conf file can be found in the directory **/opt/splunk/etc/apps/DataOnboarding4Ninjas/local**.

    To view the contents and see the new **[badge]** stanza that has been added, run the following CLI commands:

```
cd /opt/splunk/etc/apps/DataOnboarding4Ninjas/local

cat props.conf
```

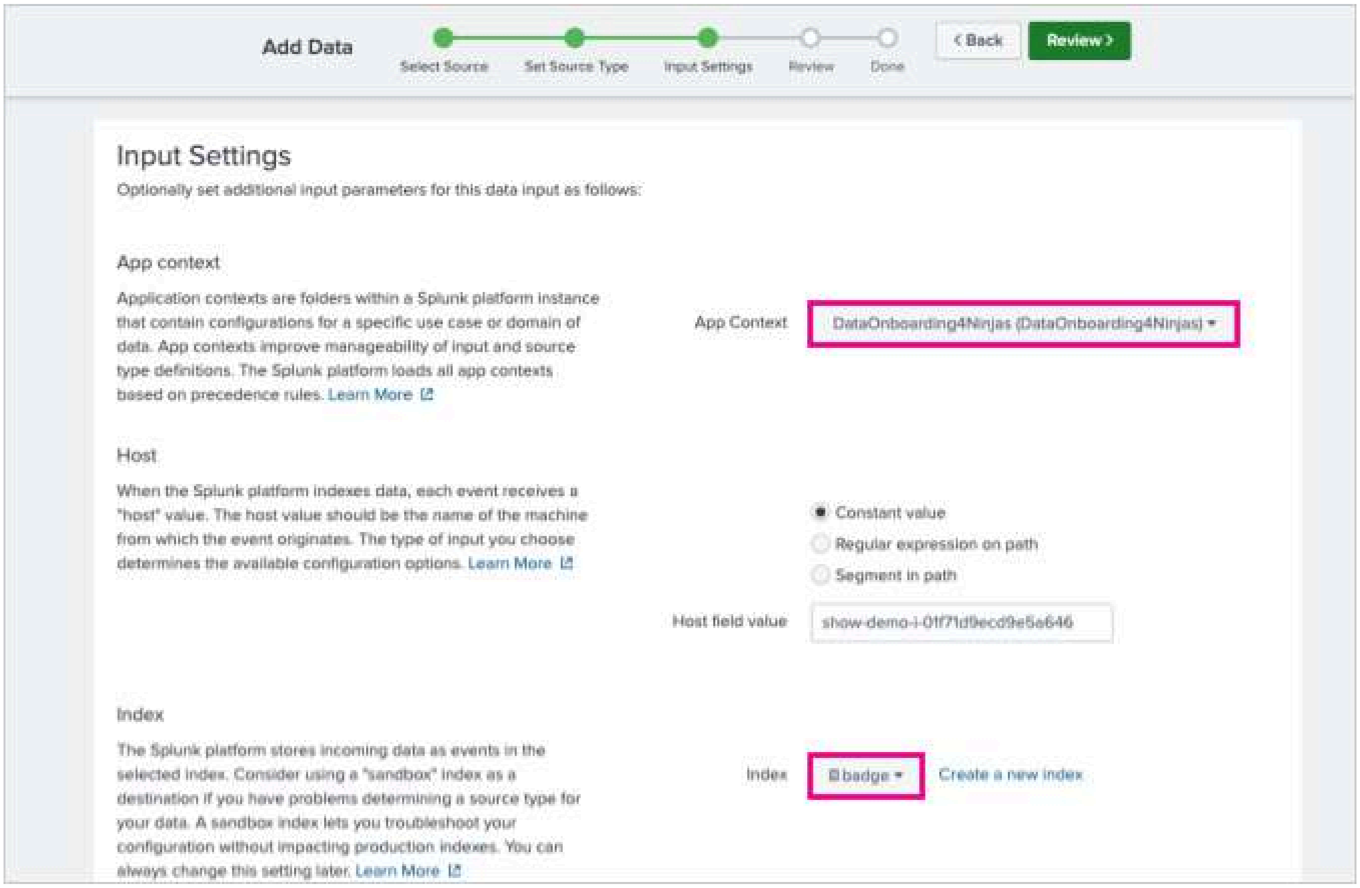
Adjust the Input Settings

13. On the **Input Settings** screen, set the **App Context** to **DataOnboarding4Ninjas.**

14. Set the **Index** to **badge**.

ℹ️ The badge Index

In this environment, we already have the badge index created. In production, ensure that you first create the proper index so you can route your data there when setting up data ingestion. Please note that it is not best practice to send your data to the default “main” index.



Input Settings

Optionally set additional input parameters for this data input as follows:

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. Learn More

App Context: DataOnboarding4Ninjas (DataOnboarding4Ninjas)

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More

● Constant value
○ Regular expression on path
○ Segment in path

Host field value: show-demo-i-01f71d9ecd9e5a646

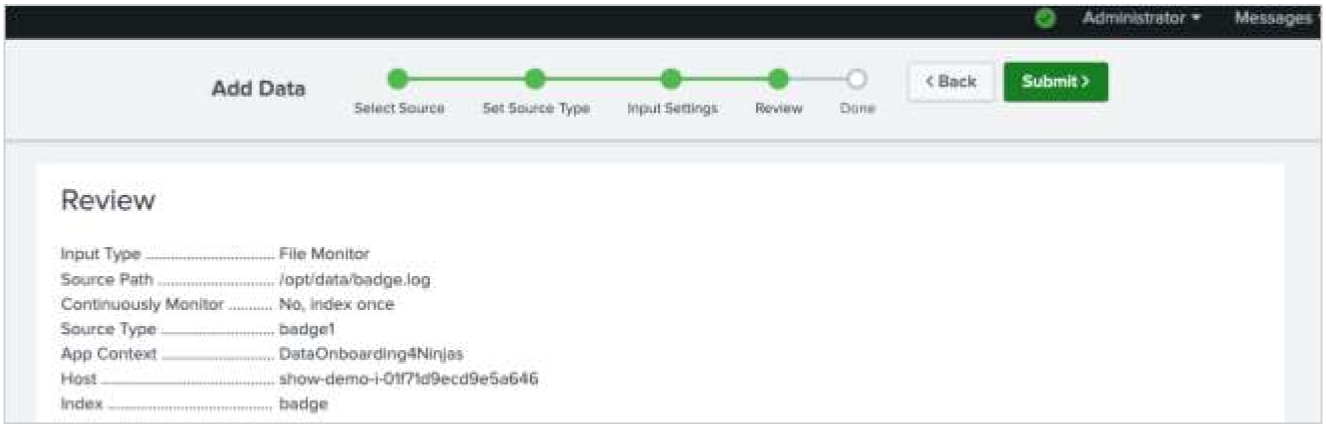
Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

Index: badge   Create a new index

Submit and Search Your Data

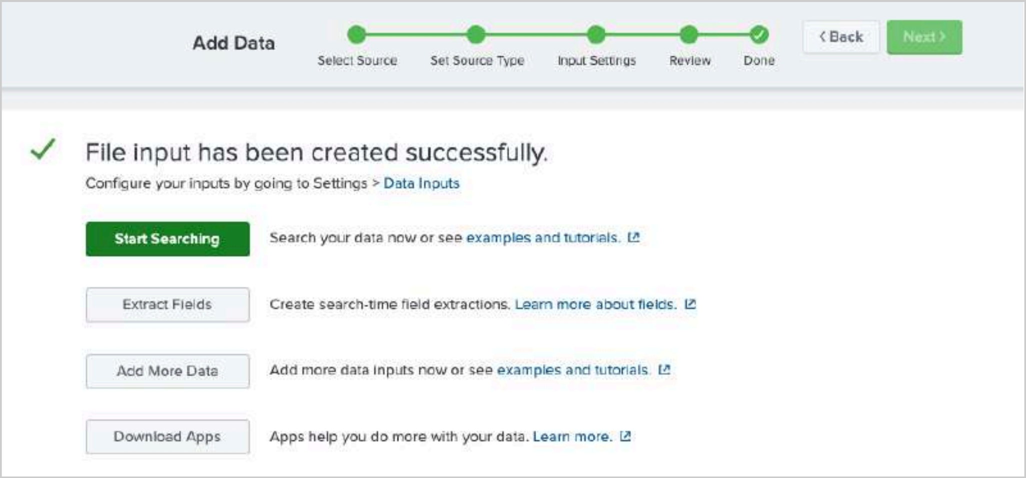
15. With the input settings adjusted, you can select **Review** and then **Submit** on the next page.



Review

Input Type .... File Monitor
Source Path .... /opt/data/badge.log
Continuously Monitor .... No, index once
Source Type badge1
App Context DataOnboarding4Ninjas
Host show-demo-i-01f71d9ecd9e5a646
Index .... badge

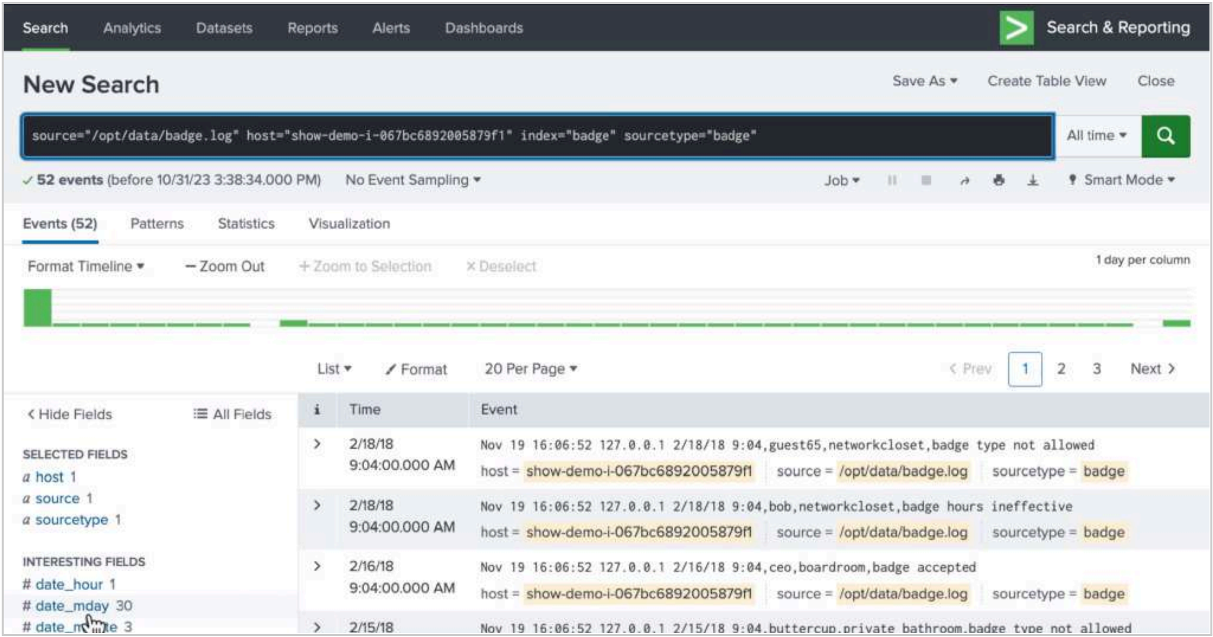
16. On the **File input has been created successfully** page click on **Start Searching**. This will take you to a new search - with the search query populated - where you can see your badge.log data now coming in.



File input has been created successfully.

Configure your inputs by going to Settings > Data Inputs

Start Searching	Search your data now or see examples and tutorials.
Extract Fields	Create search-time field extractions. Learn more about fields.
Add More Data	Add more data inputs now or see examples and tutorials.
Download Apps	Apps help you do more with your data. Learn more.



New Search

```
source="/opt/data/badge.log" host="show-demo-i-067bc6892005879f1" index="badge" sourcetype="badge"
```

✓ **52 events** (before 10/31/23 3:38:34.000 PM) No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 1
# date_mday 30
# date_m[illegible]e 3

i	Time	Event
›	2/18/18 9:04:00.000 AM	Nov 19 16:06:52 127.0.0.1 2/18/18 9:04,guest65,networkcloset,badge type not allowed host = show-demo-i-067bc6892005879f1 source = /opt/data/badge.log sourcetype = badge
›	2/18/18 9:04:00.000 AM	Nov 19 16:06:52 127.0.0.1 2/18/18 9:04,bob,networkcloset,badge hours ineffective host = show-demo-i-067bc6892005879f1 source = /opt/data/badge.log sourcetype = badge
›	2/16/18 9:04:00.000 AM	Nov 19 16:06:52 127.0.0.1 2/16/18 9:04,ceo,boardroom,badge accepted host = show-demo-i-067bc6892005879f1 source = /opt/data/badge.log sourcetype = badge
›	2/15/18	Nov 19 16:06:52 127.0.0.1 2/15/18 9:04.buttercup.private bathroom.badge type not allowed

Set Up the Add-on Builder

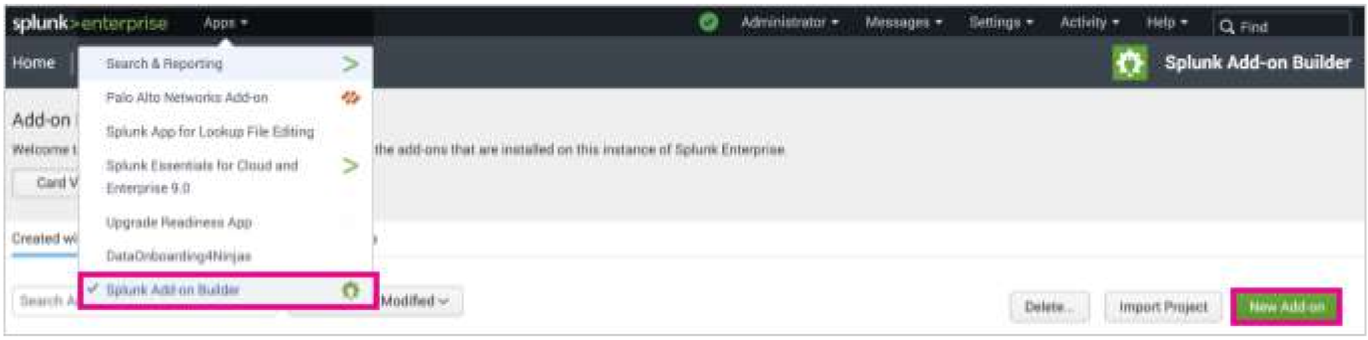
Earlier in this lab we created a source type during the “Add Data” process. Now we are going to import that source type into the Splunk Add-on Builder where we can save it for future use as a Technology Add-on, or “TA”. This way anyone can easily grab that add-on and install it to bring in badge data.

Splunk Add-on Builder

For more information about the Splunk Add-on Builder and Splunk add-ons in general, please see the following helpful resources:

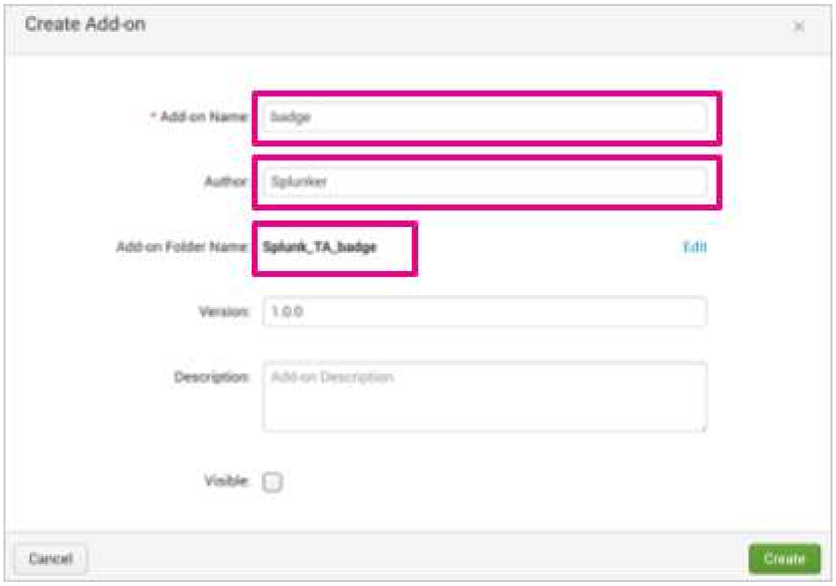
- https://docs.splunk.com/Documentation/AddonBuilder/latest/UserGuide/Overview
- https://docs.splunk.com/Documentation/AddOns/released/Overview/AboutSplunkadd-ons

17. Navigate to **Apps > Splunk Add-on Builder** and click on **New Add-on**.



18. For the **Add-on Name** enter "**badge**". For the author you can enter your own name or leave it blank.

Note the **Add-on Folder Name** that is generated, as this can change based on who the author is. This is the name of the app folder where you will find the underlying configuration files through the CLI.



* Add-on Name: badge

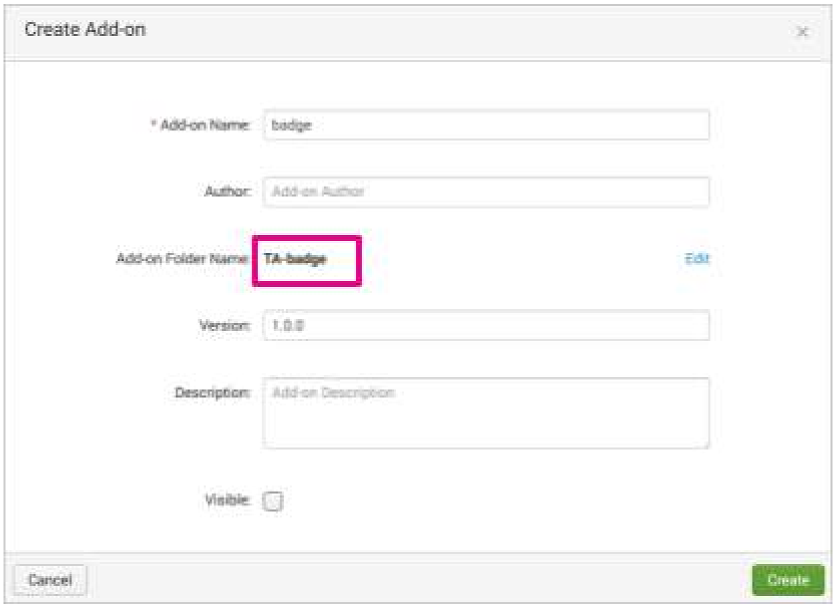
Author: Splunker

Add-on Folder Name: Splunk_TA_badge

Version: 1.0.0

Description: Add-on Description

Visible: □



* Add-on Name: badge

Author: Add-on Author

Add-on Folder Name: TA-badge

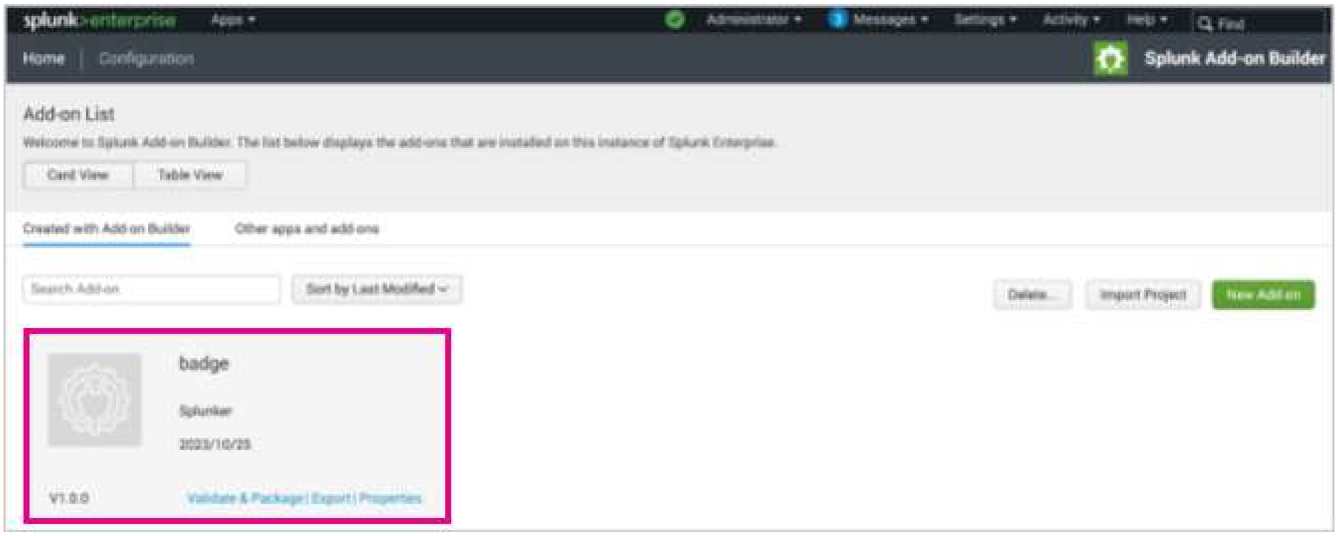
Version: 1.0.0

Description: Add-on Description

Visible: □

19. Click on **Create**.

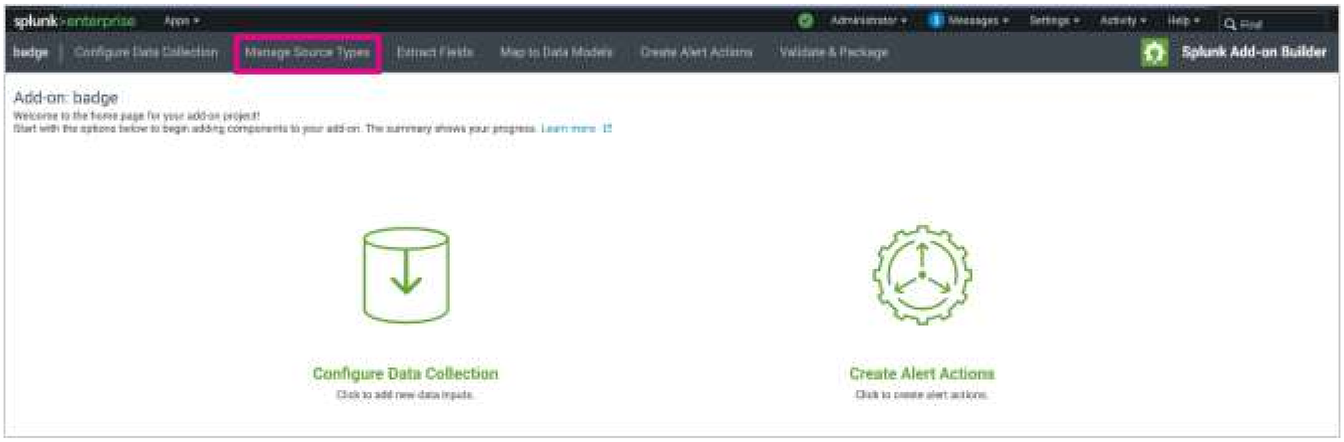
20. You can now see your badge add-on on the home screen of the Splunk Add-on Builder app. Open the badge add-on by clicking on it.



Add-on List

Welcome to Splunk Add-on Builder. The list below displays the add-ons that are installed on this instance of Splunk Enterprise.

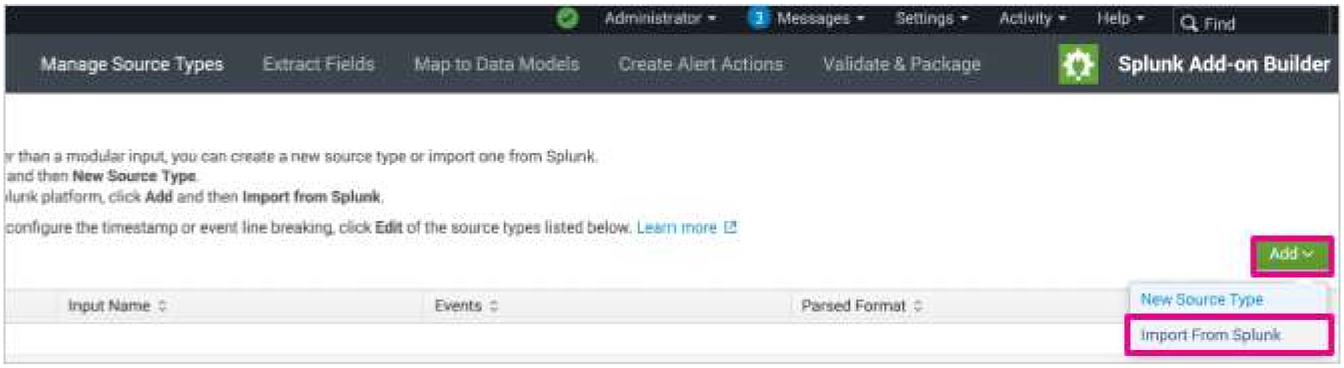
21. We will now import the source type we created earlier so it is contained within the badge add-on. To do this, click on **Manage Source Types** in the menu bar.



Add-on: badge

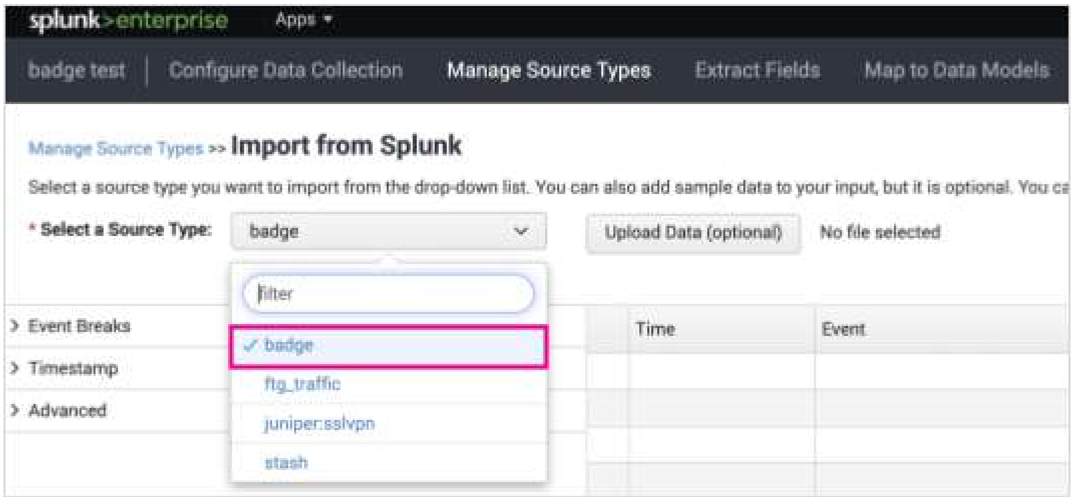
Welcome to the home page for your add-on project!
Start with the options below to begin adding components to your add-on. The summary shows your progress. Learn more

22. Click on the **Add** button and select **Import From Splunk** from the dropdown menu.



r than a modular input, you can create a new source type or import one from Splunk.
and then **New Source Type**.
lunk platform, click **Add** and then **Import from Splunk**.
configure the timestamp or event line breaking, click **Edit** of the source types listed below. Learn more

23. Select **badge** from the **Select a Source Type** dropdown.



Select a source type you want to import from the drop-down list. You can also add sample data to your input, but it is optional. You ca

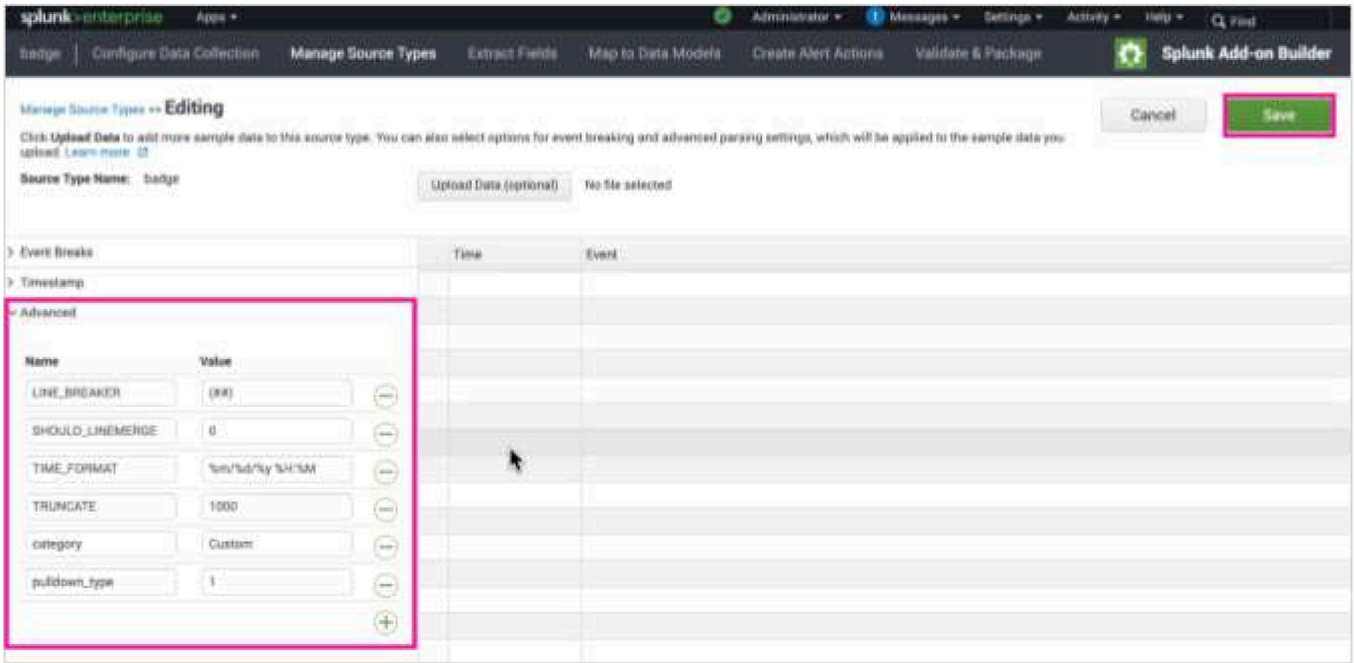
* Select a Source Type: badge

✓ badge
ftg_traffic
juniper:sslvpn
stash

The sourcetype parameters defined earlier (see Set the Source Type) will now be imported into the add-on builder and will be visible on the left under the **Advanced** section.

The Splunk Add-on Builder imports source type settings but it may also pull in other default settings. You can always continue to adjust your settings here as well.

24. Expand out the **Advanced** section on the left of the page and confirm that the field name and values we defined earlier are present. Click **Save**.

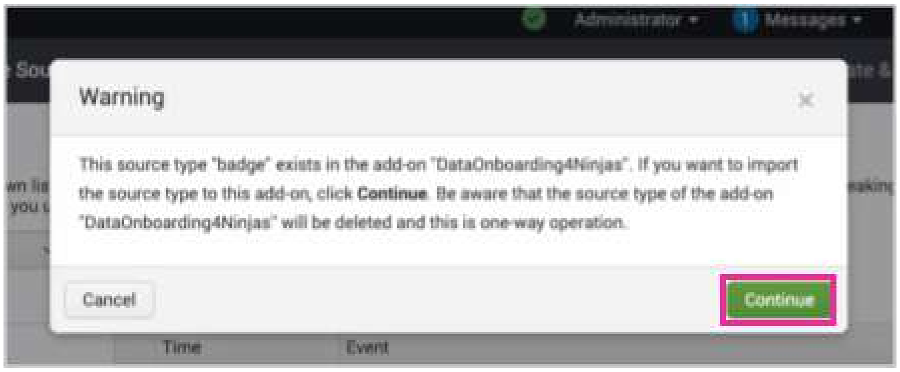


Click **Upload Data** to add more sample data to this source type. You can also select options for event breaking and advanced parsing settings, which will be applied to the sample data you upload. Learn more

Source Type Name: badge

Name	Value
LINE_BREAKER	(##)
SHOULD_LINEMERGE	0
TIME_FORMAT	%m/%d/%y %H:%M
TRUNCATE	1000
category	Custom
pulldown_type	1

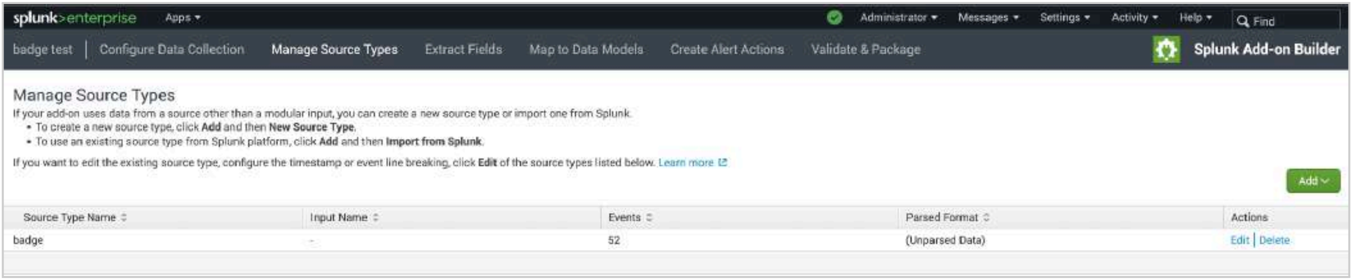
25. On the popup **Warning** message, click on **Continue**. The Warning is letting you know that the source type will no longer be associated with the **DataOnboarding4Ninjas** app but will instead be associated with the Splunk Add-on Builder app. Since this is the intention we can ignore the warning.



Warning

This source type "badge" exists in the add-on "DataOnboarding4Ninjas". If you want to import the source type to this add-on, click **Continue**. Be aware that the source type of the add-on "DataOnboarding4Ninjas" will be deleted and this is one-way operation.

26. Click **Save** to navigate back to the **Manage Source Types** home screen.



Manage Source Types

If your add-on uses data from a source other than a modular input, you can create a new source type or import one from Splunk.

- To create a new source type, click **Add** and then **New Source Type**.
- To use an existing source type from Splunk platform, click **Add** and then **Import from Splunk**.

If you want to edit the existing source type, configure the timestamp or event line breaking, click **Edit** of the source types listed below. Learn more

Source Type Name	Input Name	Events	Parsed Format	Actions
badge	-	52	(Unparsed Data)	Edit | Delete

ℹ️ Add-on Folders

As previously mentioned, when creating a new add-on within the Splunk Add-on Builder (see step 18), an **Add-on Folder Name** directory will be created under the Splunk **/etc/apps** directory. Then, when importing and saving a sourcetype within the new add-on (step 24) Splunk will save that sourcetype within a local props.conf of the TA.

You can now find your badge add-on listed as **/opt/splunk/etc/apps/<TA FOLDER NAME>** and your updated **[badge]** sourcetype within props.conf under **/opt/splunk/etc/apps/<TA FOLDER NAME>/local/props.conf**

Command to see a list of Splunk apps where your badge add-on sits:

```
ls /opt/splunk/etc/apps
```

Command to see your new props.conf file:

```
sudo cat /opt/splunk/etc/apps/<TA FOLDER NAME>/local/props.conf
```

Lab 3 - Field Extraction and CIM Compliance

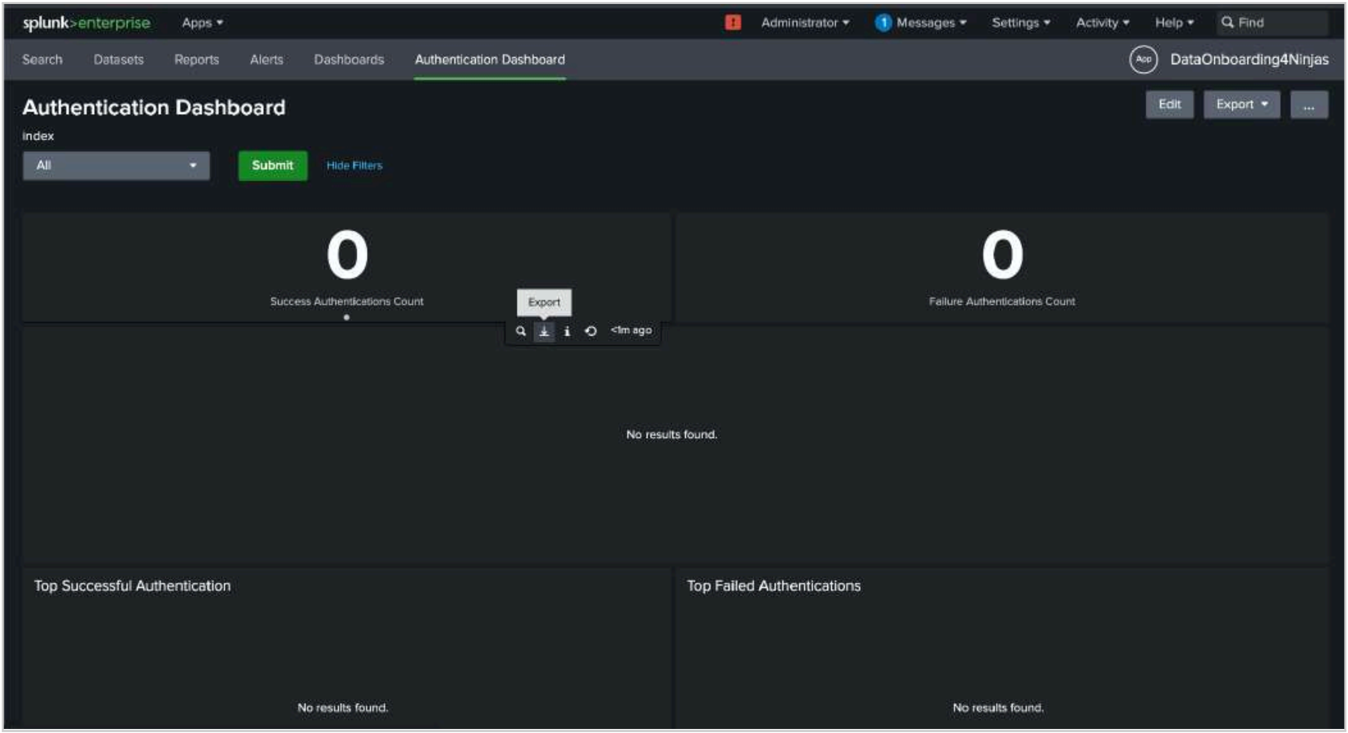
Description

In this activity we configure our badge add-on to extract fields from our badge.log data and we map our data to the Authentication data model available through Splunk's Common Information Model (CIM). In mapping our data to the data model, the Authentication Dashboard available in the DataOnboarding4Ninjas app will start to populate.

Validate the Empty Authentication Dashboard

1. Navigate to **Apps > DataOnboarding4Ninjas** and click on **Authentication Dashboard** in the menu bar.

   There should be no content populating the dashboard yet.



   Although we have badge authentication data ingested, the searches written for this dashboard are looking for information tied to the Authentication data model. This data model is available as part of the Splunk Common Information Model (CIM). We are going to map our badge TA to the authentication data model so the searches in the dashboard know to pick up the badge data we have coming in.

ℹ️ Data Models

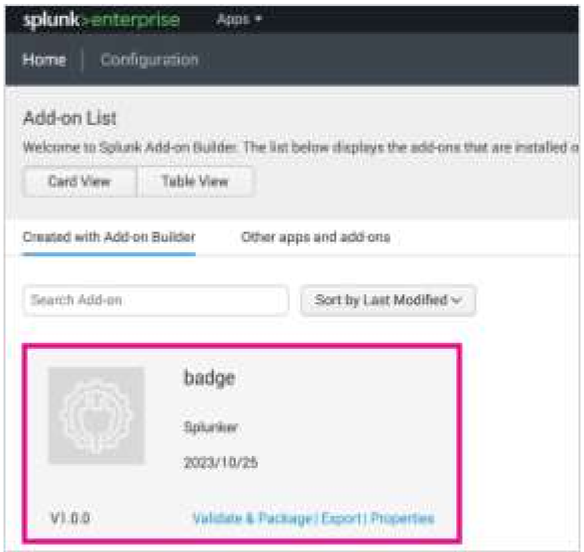
Further information about data models can be found in the Knowledge Manager Manual: https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/WhatisSplunkknowledge

To learn about the Splunk Common Information Model (CIM) please see: https://docs.splunk.com/Documentation/CIM/latest/User/Overview

Further information about the Authentication data model specifically can be found here: https://docs.splunk.com/Documentation/CIM/latest/User/Authentication

Extract Fields from the Badge Data

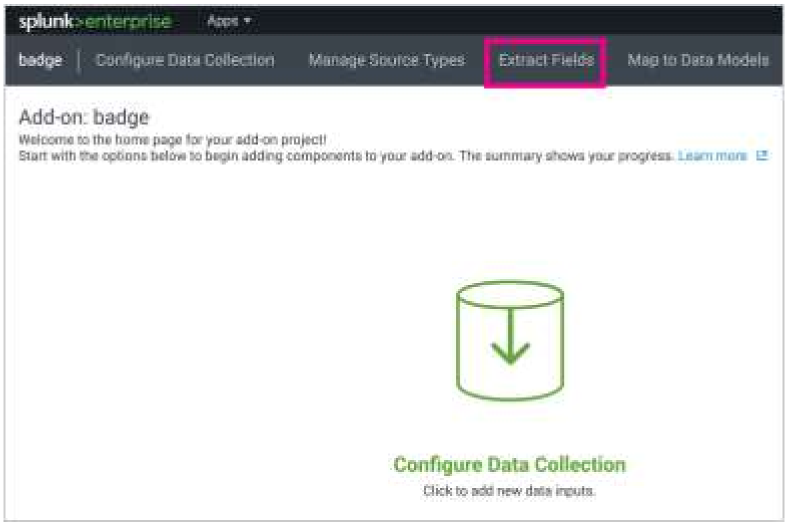
2. Navigate to the **Splunk Add-on Builder App**. On the **Add-on List** page click on the **badge** add-on.



Add-on List

Welcome to Splunk Add-on Builder. The list below displays the add-ons that are installed o

3. In the top menu click on **Extract Fields**.

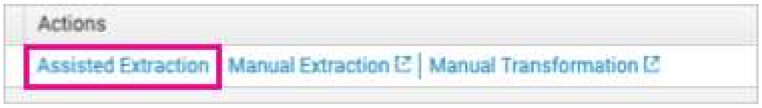

splunk>enterprise
Apps ▾
badge
Configure Data Collection
Manage Source Types
Extract Fields
Map to Data Models
Configure Data Collection
Click to add new data inputs.

Add-on: badge

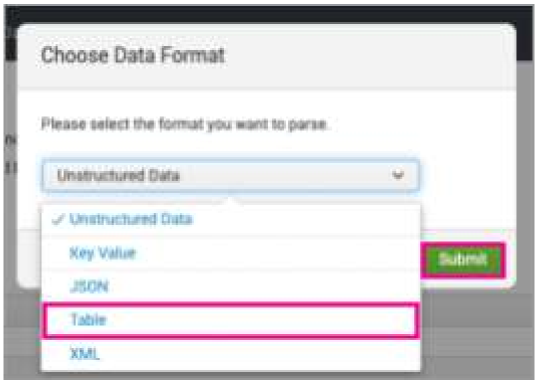
Welcome to the home page for your add-on project!
Start with the options below to begin adding components to your add-on. The summary shows your progress. Learn more

4. We will now establish a table format to help parse the data.

   To do this, on the **Extract Fields** page you will see your badge source type listed. Under **Actions**, click **Assisted Extraction**.

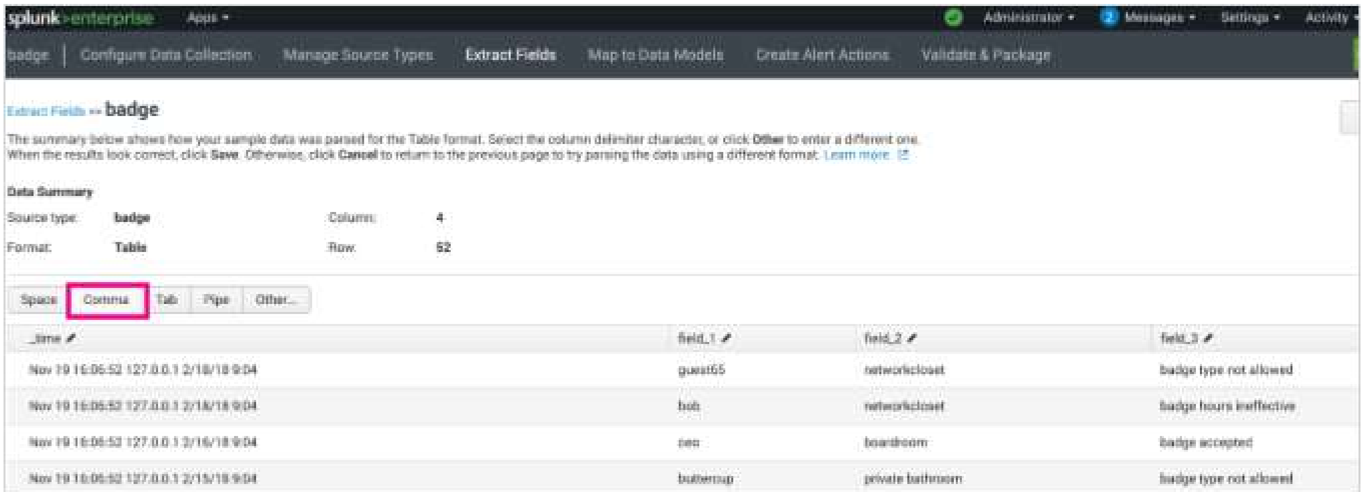


5. On the **Choose Data Format** popup, select the **Table** data format and click **Submit**.



Please select the format you want to parse.

6. Results are returned broken down by delimited fields in a table format. Select **Comma** as the separator.



The summary below shows how your sample data was parsed for the Table format. Select the column delimiter character, or click **Other** to enter a different one. When the results look correct, click **Save**. Otherwise, click **Cancel** to return to the previous page to try parsing the data using a different format. Learn more

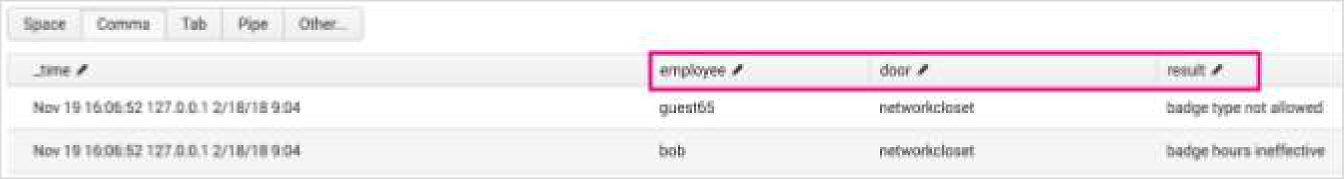
Data Summary

Source type:	**badge**	Column:	4
Format:	**Table**	Row:	52

_time	field_1	field_2	field_3
Nov 19 16:06:52 127.0.0.1 2/18/18 9:04	guest65	networkcloset	badge type not allowed
Nov 19 16:06:52 127.0.0.1 2/18/18 9:04	bob	networkcloset	badge hours ineffective
Nov 19 16:06:52 127.0.0.1 2/16/18 9:04	ceo	boardroom	badge accepted
Nov 19 16:06:52 127.0.0.1 2/15/18 9:04	buttercup	private bathroom	badge type not allowed

7. Add a field name as the header of each column:

   field_1 = **employee**
   field_2 = **door**
   field_3 = **result**



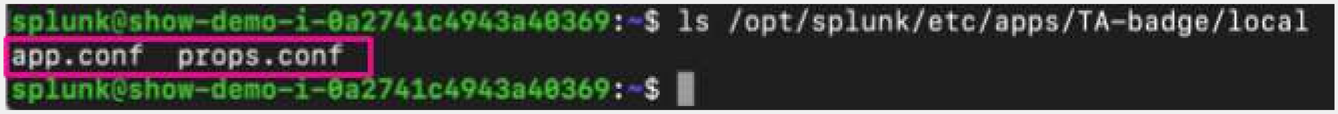
_time	employee	door	result
Nov 19 16:06:52 127.0.0.1 2/18/18 9:04	guest65	networkcloset	badge type not allowed
Nov 19 16:06:52 127.0.0.1 2/18/18 9:04	bob	networkcloset	badge hours ineffective

Optional Step - view the underlying .conf files that get built as we adjust the Add-on in the GUI

8. Prior to saving, view your local directory configuration files via the CLI. List the files in the local directory of your TA by running the following command:

```
ls /opt/splunk/etc/apps/<TA_FOLDER_NAME>/local
```

There is an **app.conf** and a **props.conf** file listed, but currently no **transforms.conf**. Upon saving the field names as the extraction, a transforms.conf will be created to store the configurations.



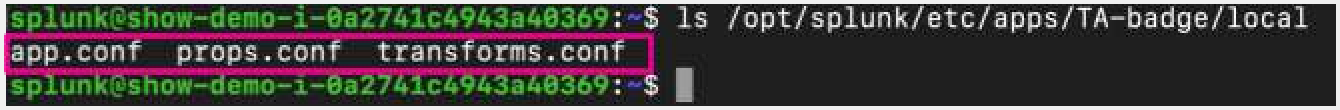
```
splunk@show-demo-i-0a2741c4943a40369:~$ ls /opt/splunk/etc/apps/TA-badge/local
app.conf  props.conf
splunk@show-demo-i-0a2741c4943a40369:~$
```

9. Back in the GUI, click **Save** in the Splunk Add-on Builder.

Optional Step - view the underlying .conf files that get built as we adjust the Add-on in the GUI

10. Verify the transforms.conf file by running the following CLI command to list the files in the **local** directory of your TA:

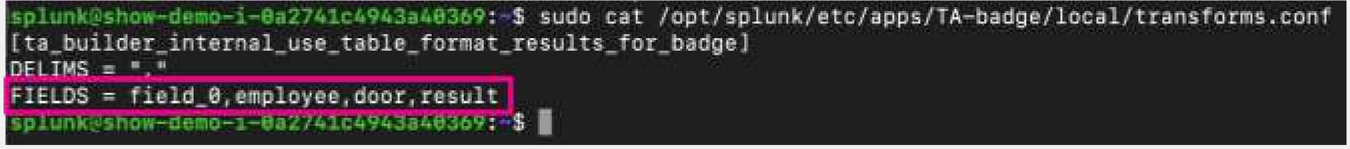
```
ls /opt/splunk/etc/apps/<TA_FOLDER_NAME>/local
```



```
splunk@show-demo-i-0a2741c4943a40369:~$ ls /opt/splunk/etc/apps/TA-badge/local
app.conf  props.conf  transforms.conf
splunk@show-demo-i-0a2741c4943a40369:~$
```

11. View the **transforms.conf** and see the new field names defined:

```
sudo cat /opt/splunk/etc/apps/<TA_FOLDER_NAME>/local/transforms.conf
```



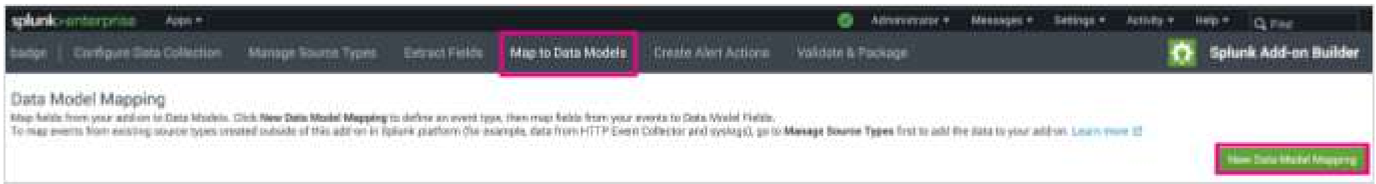
```
splunk@show-demo-i-0a2741c4943a40369:~$ sudo cat /opt/splunk/etc/apps/TA-badge/local/transforms.conf
[ta_builder_internal_use_table_format_results_for_badge]
DELIMS = ","
FIELDS = field_0,employee,door,result
splunk@show-demo-i-0a2741c4943a40369:~$
```

ℹ️ **transforms.conf**

More information about transforms.conf can be found in the Admin Manual:
https://docs.splunk.com/Documentation/Splunk/latest/Admin/Transformsconf

12. Open the **Splunk Add-on Builder** and click on **Map to Data Models** in the menu bar.

13. Click on **New Data Model Mapping**.

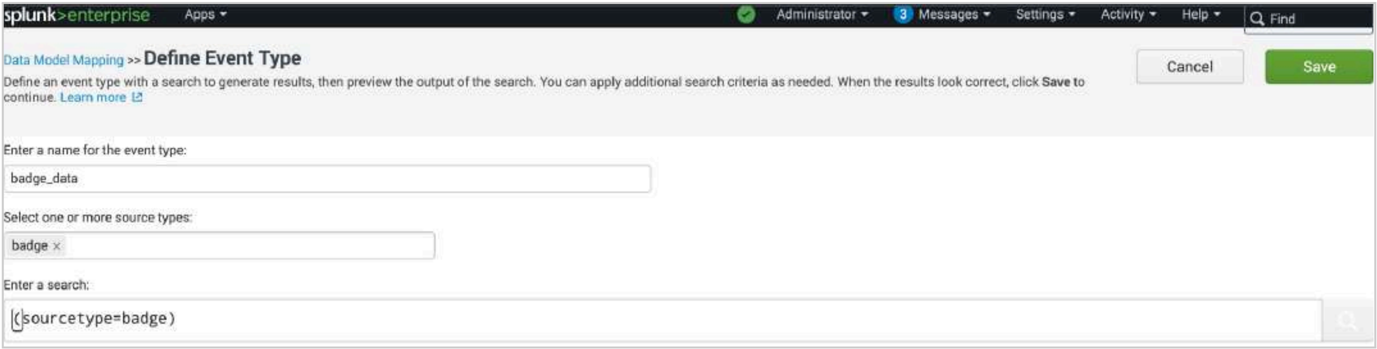


Data Model Mapping

Map fields from your add-on to Data Models. Click **New Data Model Mapping** to define an event type, then map fields from your events to Data Model Fields.
To map events from existing source types created outside of this add-on in Splunk platform (for example, data from HTTP Event Collector and syslog), go to **Manage Source Types** first to add the data to your add-on. Learn more

14. On the **Define Event Type** page, enter the following into the fields:

Enter a name for the event type:	**badge_data**
Select one or more source types:	**badge**
Enter a search:	`(sourcetype=badge)`



Data Model Mapping >> Define Event Type

Define an event type with a search to generate results, then preview the output of the search. You can apply additional search criteria as needed. When the results look correct, click **Save** to continue. Learn more

Enter a name for the event type:
badge_data

Select one or more source types:
badge ×

Enter a search:
(sourcetype=badge)

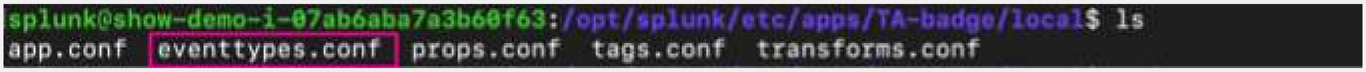
Click on **Save**.

Optional Step - view the underlying .conf files that get built as we adjust the add-on in the GUI

15. Verify the **eventtypes.conf** file by running the following CLI command to list the files in the local directory of your TA:

```
ls /opt/splunk/etc/apps/<TA_FOLDER_NAME>/local
```

You should see the eventtypes.conf file listed:

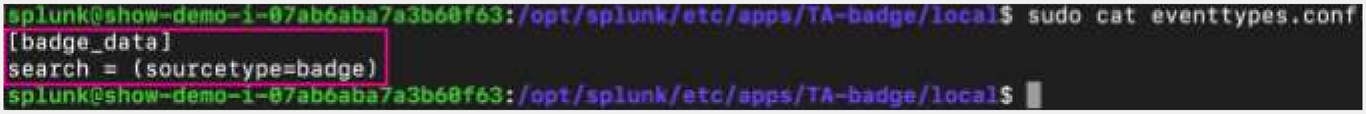


```
splunk@show-demo-i-07ab6aba7a3b60f63:/opt/splunk/etc/apps/TA-badge/local$ ls
app.conf  eventtypes.conf  props.conf  tags.conf  transforms.conf
```

16. View the contents of **eventtypes.conf** and see the newly defined **[badge_data]** stanza:

```
sudo cat /opt/splunk/etc/apps/<TA_FOLDER_NAME>/local/eventtypes.conf
```

You should see the **[badge_data]** stanza and the accompanying search you defined:



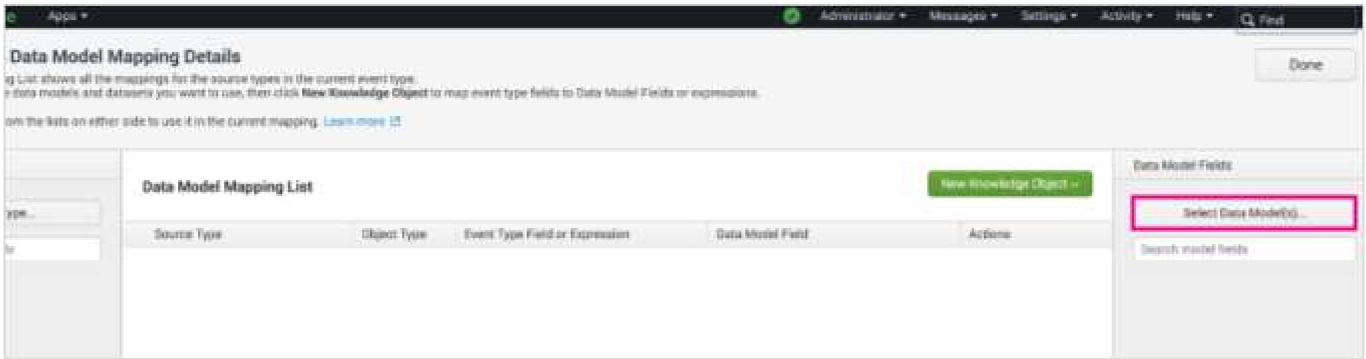
```
splunk@show-demo-i-07ab6aba7a3b60f63:/opt/splunk/etc/apps/TA-badge/local$ sudo cat eventtypes.conf
[badge_data]
search = (sourcetype=badge)
splunk@show-demo-i-07ab6aba7a3b60f63:/opt/splunk/etc/apps/TA-badge/local$
```

ℹ️ eventtypes.conf

More information about eventtypes.conf can be found in the Admin Manual:
https://docs.splunk.com/Documentation/Splunk/latest/Admin/eventtypesconf

17. We will now choose which data model to map to.

    Back in the Splunk GUI, you should be on the **Data Model Mapping Details** page, where you can add knowledge objects to enhance the badge data. On the right side of the page click on **Select Data Model(s)...**



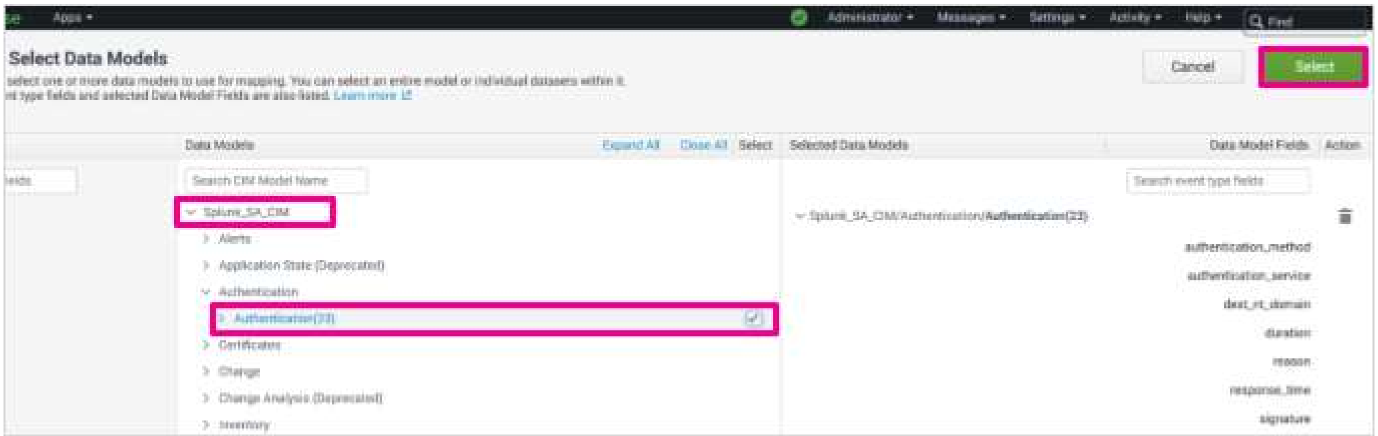
Data Model Mapping Details

g List shows all the mappings for the source types in the current event type.
data models and datasets you want to use, then click **New Knowledge Object** to map event type fields to Data Model Fields or expressions.

om the lists on either side to use it in the current mapping. Learn more

18. Under the **Data Models** panel, expand out the **Splunk_SA_CIM** list of data models. Select the **Authentication** data model and the corresponding Data Model Fields will appear on the right side of the page.

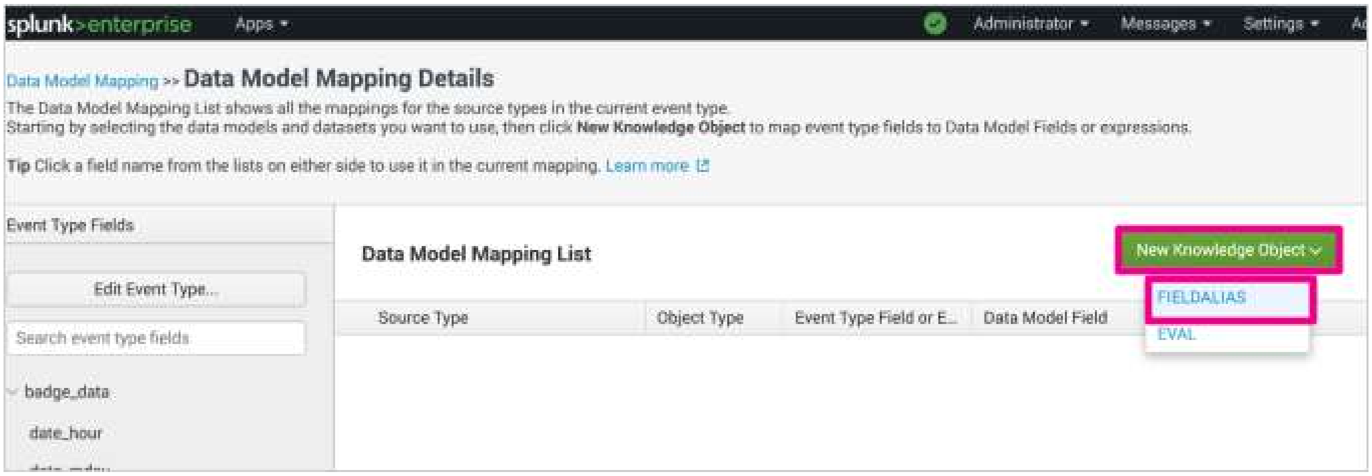
    Click on **Select**.



Select Data Models

select one or more data models to use for mapping. You can select an entire model or individual datasets within it.
nt type fields and selected Data Model Fields are also listed. Learn more

19. On the **Data Model Mapping Details** page, add the field alias knowledge object by clicking on **New Knowledge Object > FIELDALIAS**.



Data Model Mapping Details

The Data Model Mapping List shows all the mappings for the source types in the current event type.
Starting by selecting the data models and datasets you want to use, then click **New Knowledge Object** to map event type fields to Data Model Fields or expressions.

Tip Click a field name from the lists on either side to use it in the current mapping. Learn more

ℹ️ Field Aliases

Field aliases are an alternate name that you assign to a field, allowing you to search for those events using both the original field name and/or the alias.

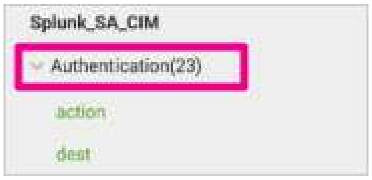
More information about field alias can be found in the Knowledge Manager Manual:
https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Addaliasestofields

20. On the next page in the **Data Model Mapping List** panel, select the **badge** source type.

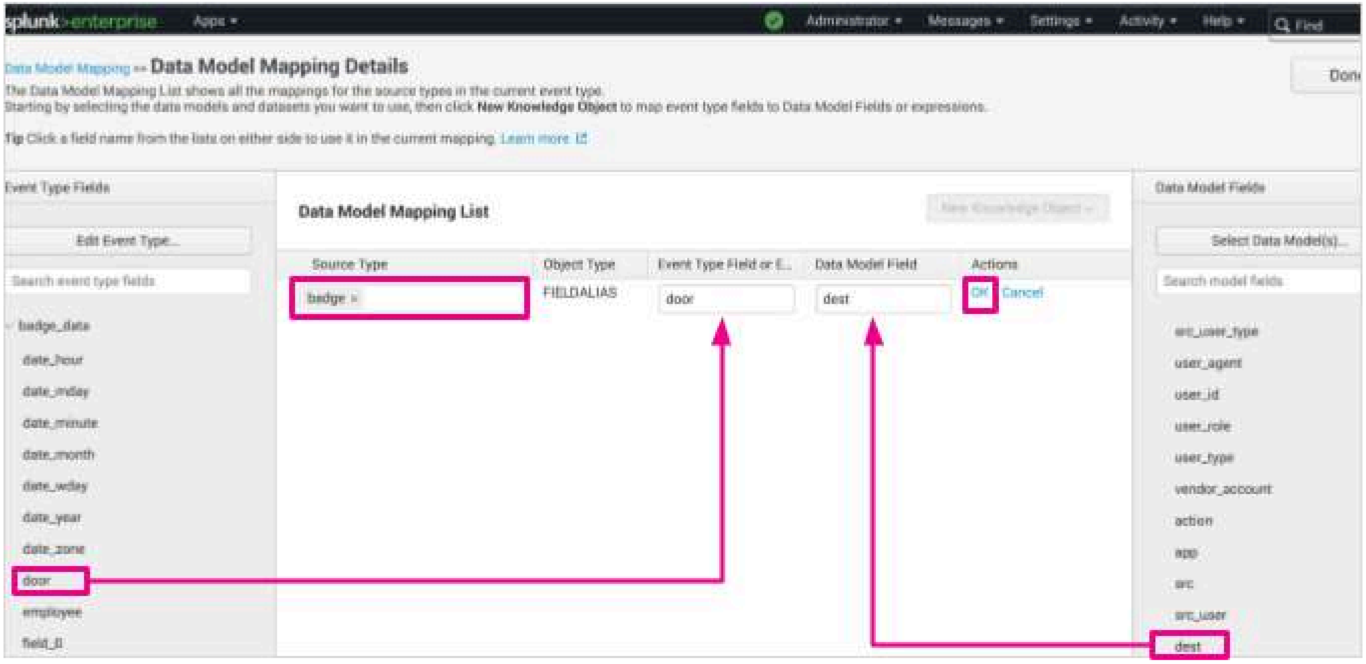
21. In the **Event Type Fields** section on the left, expand out the **badge_data** section (if not already expanded) and click on “**door**” - this will populate the **Event Type Field or Expression** column with this field name.

22. In the **Data Model Fields** panel on the right, click on “**dest**” - this will populate the **Data Model Field** name.

    Note: If you do not see a list of fields in the **Data Model Fields** panel, you may need to expand the **Authentication(23)** section to view them.



When the values are correctly populated, click on **OK** to save them.



Data Model Mapping >> **Data Model Mapping Details**

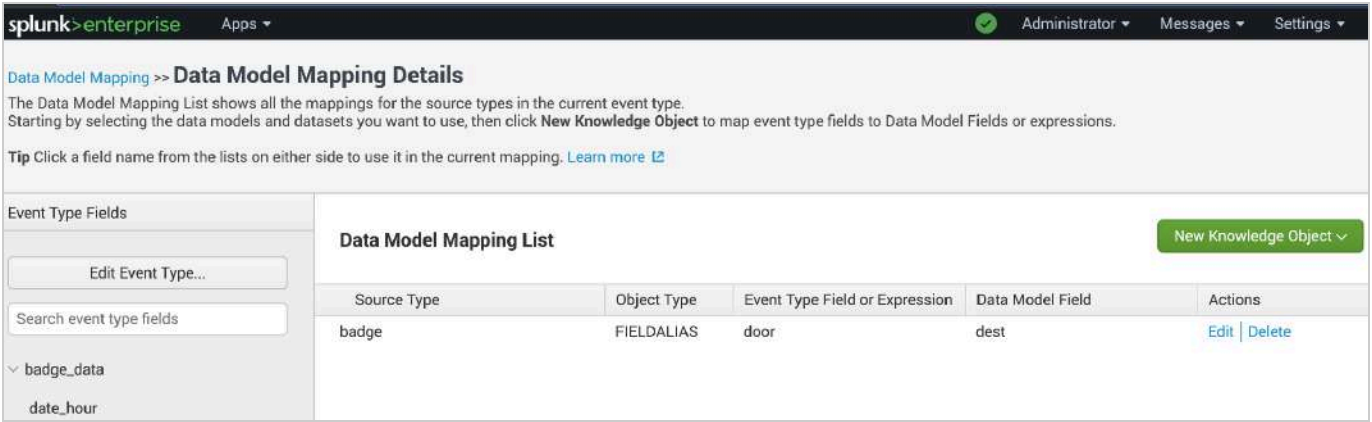
The Data Model Mapping List shows all the mappings for the source types in the current event type.
Starting by selecting the data models and datasets you want to use, then click **New Knowledge Object** to map event type fields to Data Model Fields or expresions.

Tip Click a field name from the lists on either side to use it in the current mapping. Learn more

Data Model Mapping List

Source Type	Object Type	Event Type Field or E...	Data Model Field	Actions
badge ×	FIELDALIAS	door	dest	OK Cancel

23. Your mapping will now look like this:



Data Model Mapping >> **Data Model Mapping Details**

The Data Model Mapping List shows all the mappings for the source types in the current event type.
Starting by selecting the data models and datasets you want to use, then click **New Knowledge Object** to map event type fields to Data Model Fields or expressions.

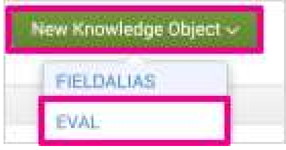
Tip Click a field name from the lists on either side to use it in the current mapping. Learn more

Data Model Mapping List

Source Type	Object Type	Event Type Field or Expression	Data Model Field	Actions
badge	FIELDALIAS	door	dest	Edit | Delete

24. We will now add a new knowledge object to populate the **action** field depending on whether a badge scan was successful or unsuccessful. To do this we will use an EVAL knowledge object (this works the same way as using `eval` in a search query).

    Add the new knowledge object by clicking on **New Knowledge Object > EVAL**.



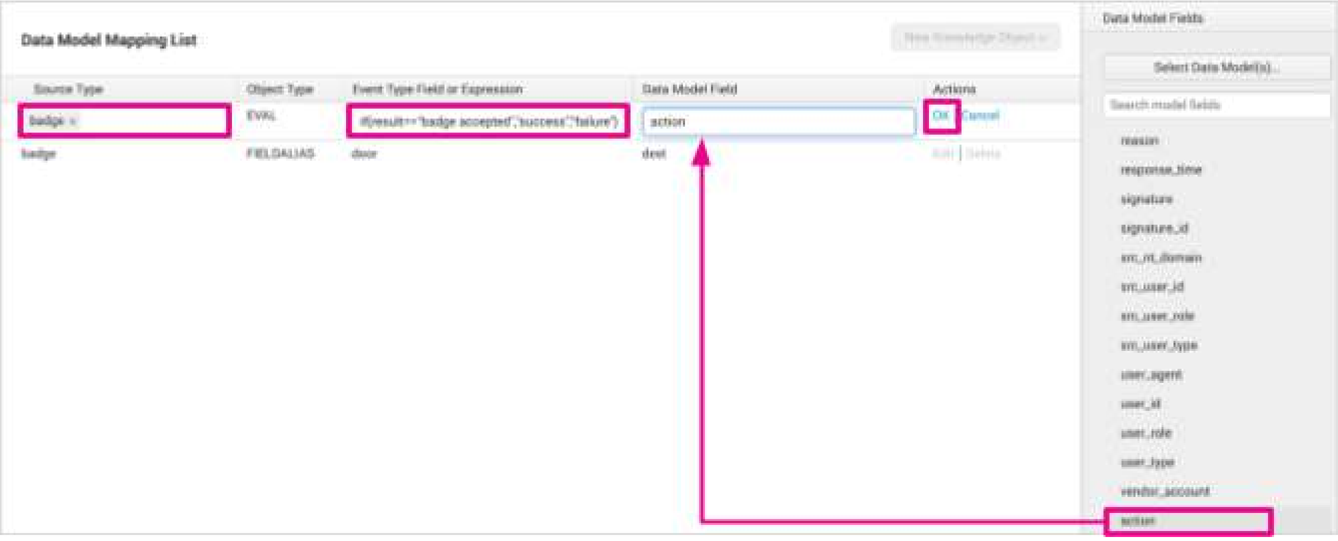
25. In the **Data Model Mapping List** panel, select the **badge** source type.

26. For **Event Type Field or Expression**, enter:

```
if(result=="badge accepted","success","failure")
```

27. For the **Data Model Field**, add the **action** field by clicking on it under the **Data Model Fields** panel on the right side of the page.

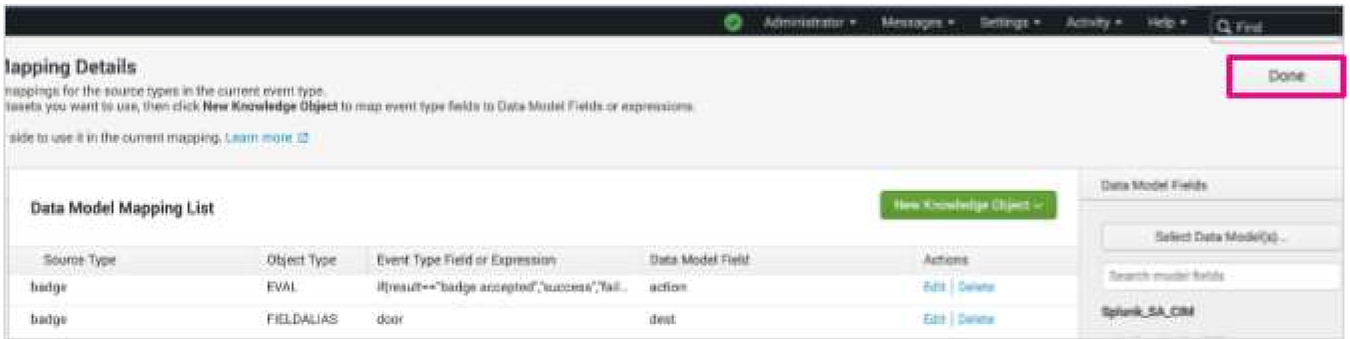
    When the values are correctly populated, click on **OK** to save them.



Data Model Mapping List

Source Type	Object Type	Event Type Field or Expression	Data Model Field	Actions
badge ×	EVAL	if(result=="badge accepted","success","failure")	action	OK Cancel
badge	FIELDALIAS	door	dest	Edit | Delete

28. When your complete mapping looks like this, click on **Done**.



lapping Details

nappings for the source types in the current event type.
tasets you want to use, then click **New Knowledge Object** to map event type fields to Data Model Fields or expressions.

side to use it in the current mapping. Learn more

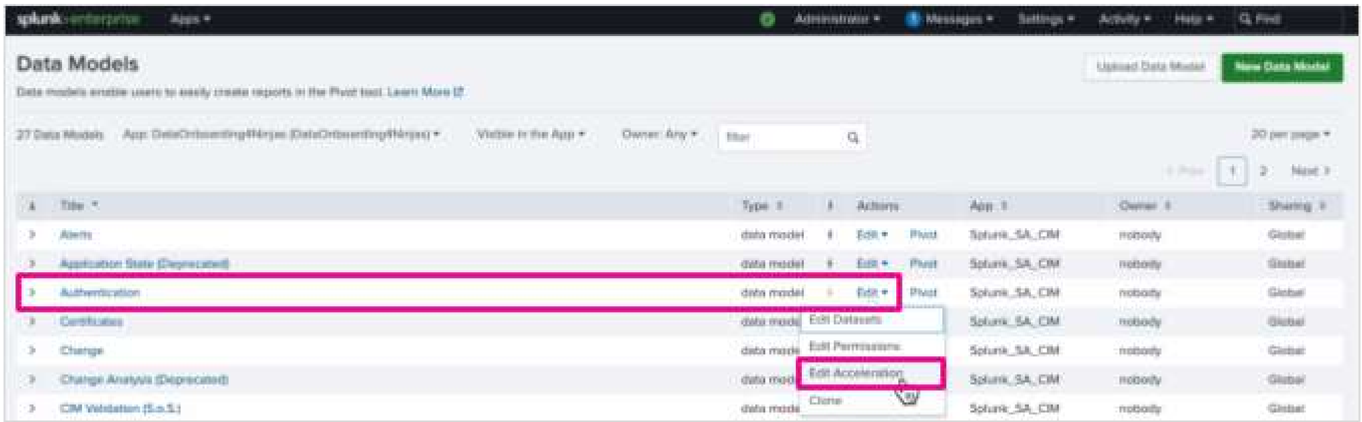
Data Model Mapping List

Source Type	Object Type	Event Type Field or Expression	Data Model Field	Actions
badge	EVAL	if(result=="badge accepted","success","fail...	action	Edit | Delete
badge	FIELDALIAS	door	dest	Edit | Delete

Re-accelerate Your Data Model

29. Now that we have updated our data model mappings we need to re-accelerate it so Splunk regenerates the summaries for the data model. This will ensure that our search results are both fast and accurate.

    To do this, navigate to **Settings > Data Models** and click on **Edit** next to the **Authentication** data Model. On the dropdown, select **Edit Acceleration.**



Data Models

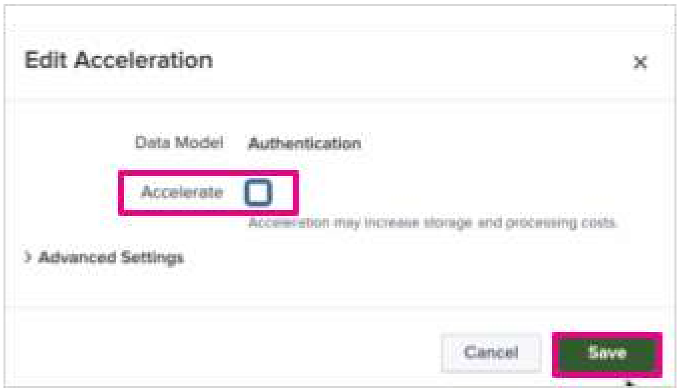
Data models enable users to easily create reports in the Pivot tool. Learn More

27 Data Models App: DataOnboardingNinjas (DataOnboardingNinjas) ▾ Visible in the App ▾ Owner: Any ▾ filter 20 per page ▾

‹ Prev 1 2 Next ›

	Title ▾	Type		Actions		App	Owner	Sharing
›	Alerts	data model		Edit ▾	Pivot	Splunk_SA_CIM	nobody	Global
›	Application State (Deprecated)	data model		Edit ▾	Pivot	Splunk_SA_CIM	nobody	Global
›	Authentication	data model		Edit ▾	Pivot	Splunk_SA_CIM	nobody	Global
›	Certificates	data model				Splunk_SA_CIM	nobody	Global
›	Change	data model				Splunk_SA_CIM	nobody	Global
›	Change Analysis (Deprecated)	data model				Splunk_SA_CIM	nobody	Global
›	CIM Validation (S.o.S.)	data model				Splunk_SA_CIM	nobody	Global

30. On the **Edit Acceleration** popup uncheck the **Accelerate** box and click on **Save**.



Data Model Authentication

Accelerate □

Acceleration may increase storage and processing costs.

› Advanced Settings

31. Now go back into **Edit Acceleration** again and re-accelerate the data model by re-checking the acceleration box and clicking **Save**.

ℹ️ Data Model Acceleration

The Splunk Add-On Builder is typically used to create TAs with Data Model Acceleration (DMA) in a local or development environment, rather than a production environment. The Splunk Add-on Builder does not automatically rebuild the DMA and your use case will determine whether you will need to disable and re-enable acceleration as we have just done.

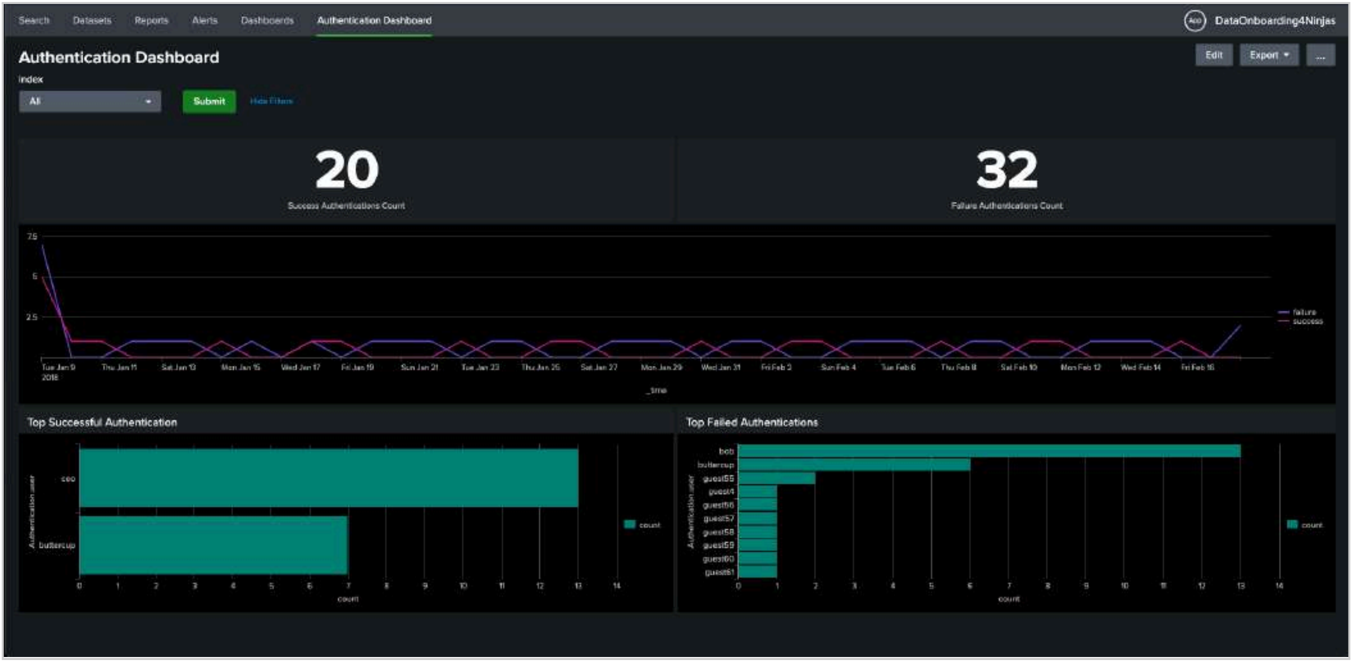
In the case of updating/appending/removing fields for data model mapping, data models only need to be re-accelerated if a user wants the old data to be populated with the new/updated extractions. The user does not need to re-accelerate any data models if they are okay with new mappings not being applied to the old data.

To learn more about periodic updating for accelerated data models, refer to the following documentation: https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Acceleratedatamodels#After_you_enable_acceleration_for_a_data_model

Verify the Authentication Dashboard

32. Navigate to **Apps > DataOnboarding4Ninjas** and click on **Authentication Dashboard** in the menu bar.

    The dashboard should now be populated. This is because the underlying dashboard searches are looking for events that map back to the Authentication data model - events that have fields like **action** and **dest**. While our original events may not have contained action and dest, we have now mapped our events to those data model field names and our data is now being returned in the results.



Appendix

Troubleshooting for Lab 1, Option 2: Monitoring Through the CLI

If an error was made in the monitoring stanza - for example, a typo or host_segment was set incorrectly - there are a couple of steps to fix the monitoring input.

1. Adjust the monitoring stanza in inputs.conf. To do this, edit the local inputs.conf file:

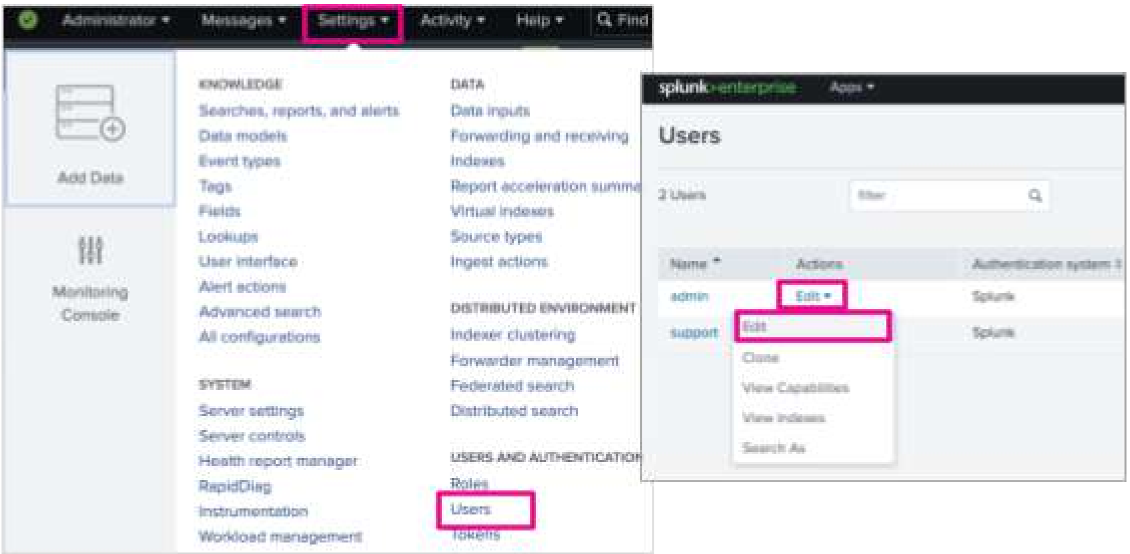
```
vi /opt/splunk/etc/system/local/inputs.conf
```

2. Type “ **i** ” to insert text into the file and adjust any errors in the monitoring stanza

3. Exit the vi editor by pressing the **escape** key then typing **:wq** and hitting **enter**. This is telling the editor to save and exit back to the main CLI.

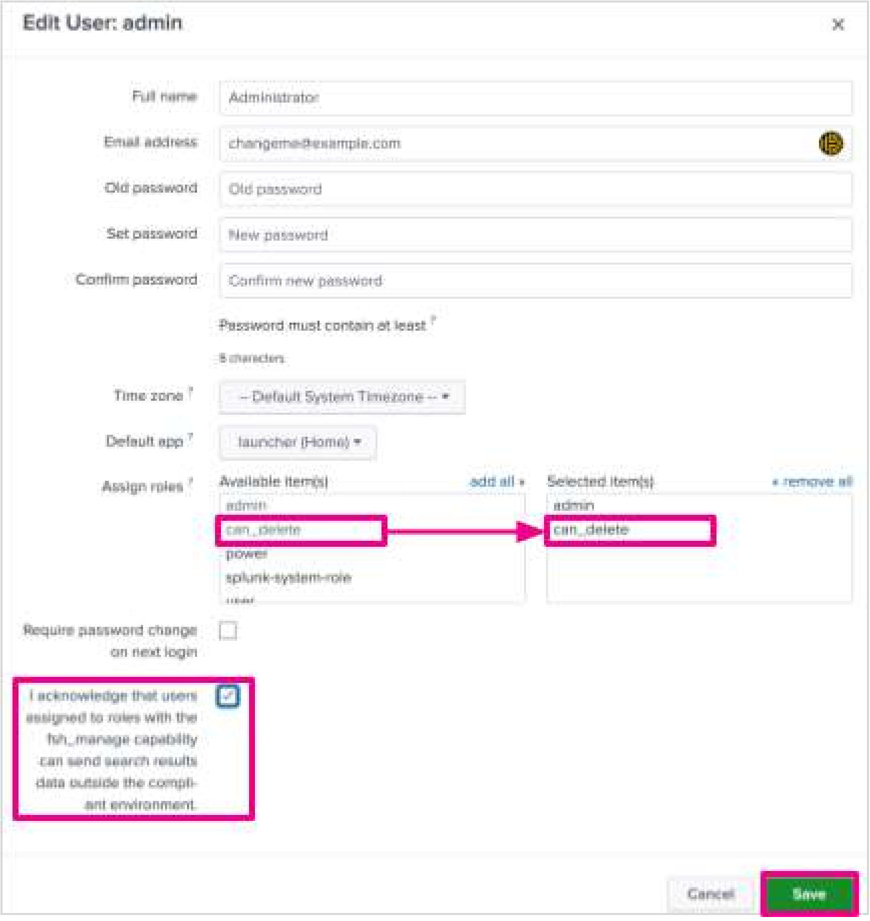
4. Clean up the incorrectly parsed event data in Splunk using the `delete` command. This will prevent the incorrect event data from showing up in search results.

   To do this, log in to Splunk and go to **Settings > Users and** click **Edit** next to the **admin** user. On the dropdown menu select **Edit**.



5. Under **Available item(s)** click on the **can_delete** role - this will add it to the **Selected item(s)** list on the right side of the screen.

6. Check the “**I acknowledge…**” box and click on **Save**.



Edit User: admin

Full name: Administrator

Email address: changeme@example.com

Old password: Old password

Set password: New password

Confirm password: Confirm new password

Password must contain at least ?

8 characters

Time zone ?: -- Default System Timezone --

Default app ?: launcher (Home)

Assign roles ?

Available item(s) — add all »
- admin
- can_delete
- power
- splunk-system-role
- user

Selected item(s) — « remove all
- admin
- can_delete

Require password change on next login ☐

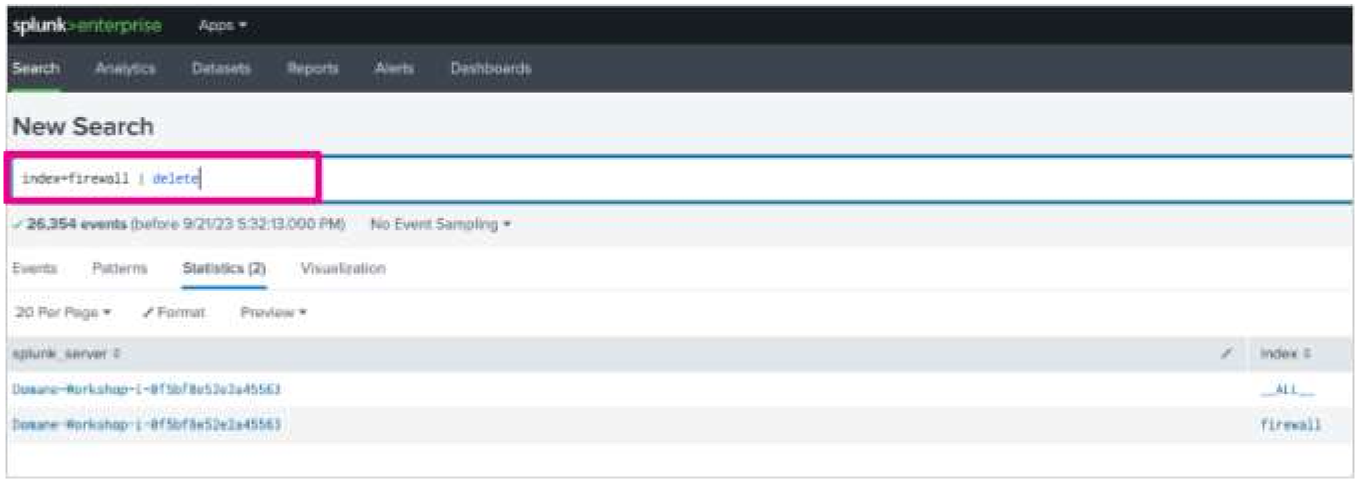
I acknowledge that users assigned to roles with the fsh_manage capability can send search results data outside the compliant environment. ☑

⚠️ **can_delete**

The can_delete role is disabled by default for admin users to prevent accidental deletion of data. It is recommended to remove this role once you have deleted the required data.

7. Remove the incorrectly parsed event data by running the following search over **All time**. This will remove all of the previously ingested data in our **firewall** index:

```
index=firewall | delete
```



```
index=firewall | delete
```

✓ 26,354 events (before 9/21/23 5:32:13.000 PM) No Event Sampling ▾

splunk_server	index
Domane-Workshop-i-0f5bf8e52e2a45563	__ALL__
Domane-Workshop-i-0f5bf8e52e2a45563	firewall

Before we can re-ingest the firewall data (with the correct settings from inputs.conf) we need to clean the fishbucket - this will tell Splunk to clear out the cached markers for where it was monitoring our inputs and will ensure that Splunk will start collecting data from the very beginning of the log files.

To do this, open your terminal app and run the following commands:

8. Switch to the root user:

```
sudo su
```

9. Stop Splunk:

```
/opt/splunk/bin/splunk stop
```

10. Reset the fishbucket cache for each of the paths it was monitoring:

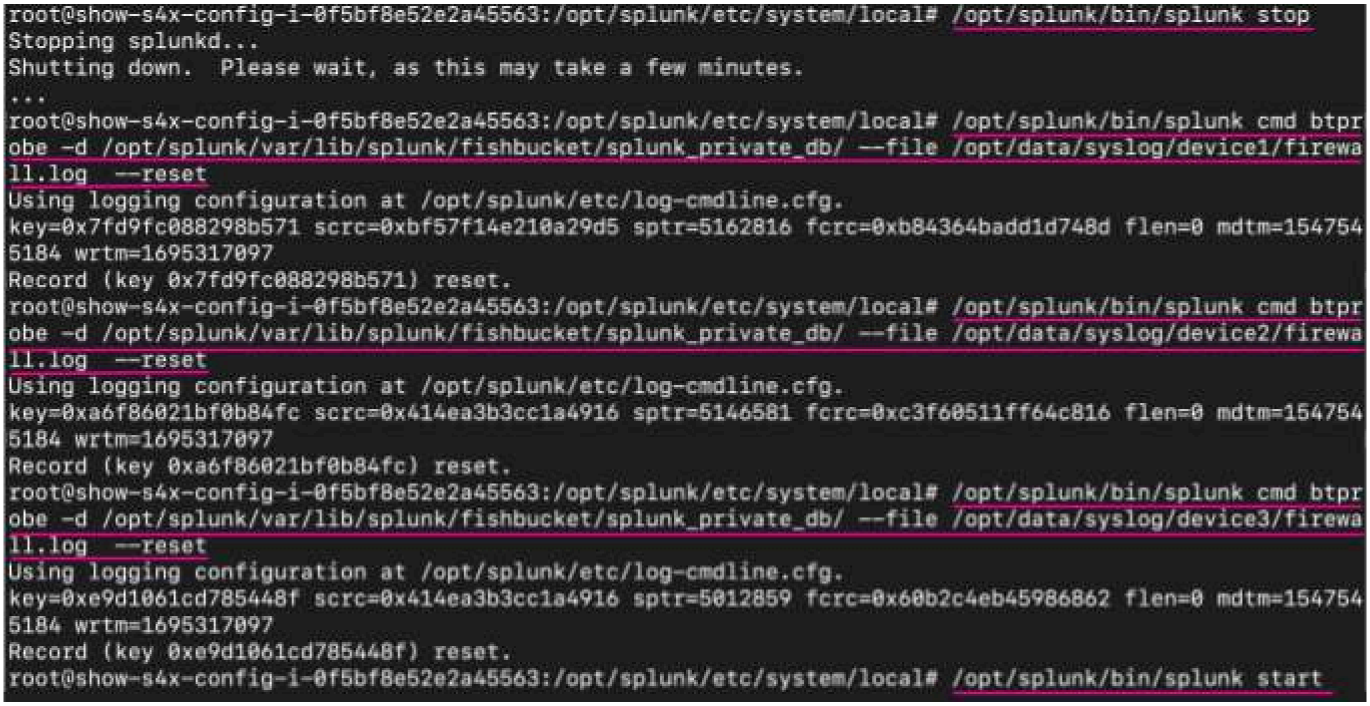
```
/opt/splunk/bin/splunk cmd btprobe -d
/opt/splunk/var/lib/splunk/fishbucket/splunk_private_db/ --file
/opt/data/syslog/device1/firewall.log --reset
```

```
/opt/splunk/bin/splunk cmd btprobe -d
/opt/splunk/var/lib/splunk/fishbucket/splunk_private_db/ --file
/opt/data/syslog/device2/firewall.log --reset
```

```
/opt/splunk/bin/splunk cmd btprobe -d
/opt/splunk/var/lib/splunk/fishbucket/splunk_private_db/ --file
/opt/data/syslog/device3/firewall.log --reset
```

11. Start Splunk:

```
/opt/splunk/bin/splunk start
```

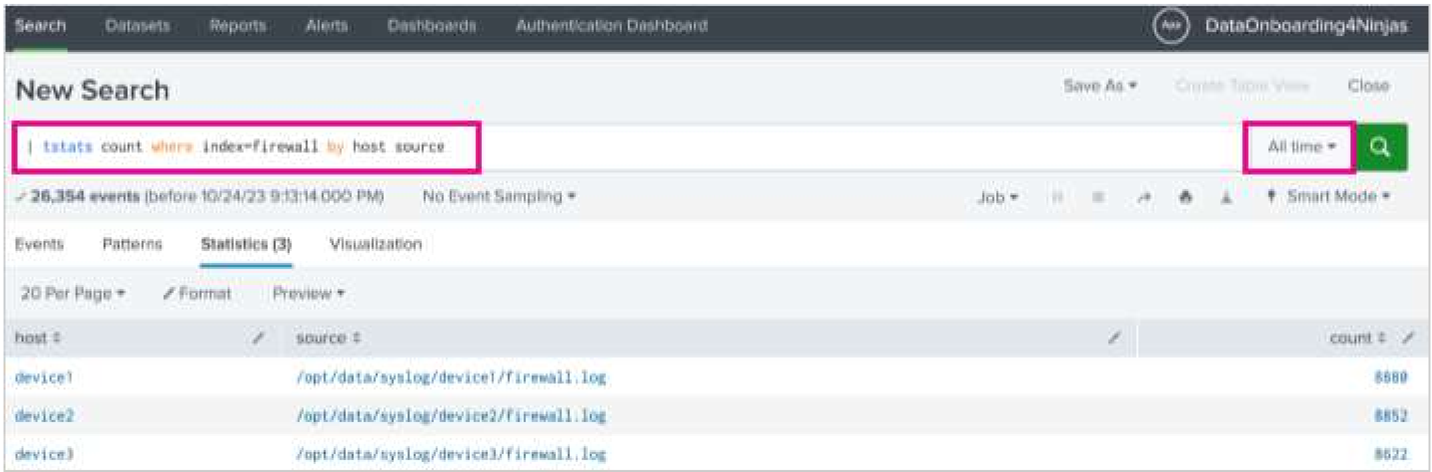


```
root@show-s4x-config-i-0f5bf8e52e2a45563:/opt/splunk/etc/system/local# /opt/splunk/bin/splunk stop
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
...
root@show-s4x-config-i-0f5bf8e52e2a45563:/opt/splunk/etc/system/local# /opt/splunk/bin/splunk cmd btpr
obe -d /opt/splunk/var/lib/splunk/fishbucket/splunk_private_db/ --file /opt/data/syslog/device1/firewa
ll.log  --reset
Using logging configuration at /opt/splunk/etc/log-cmdline.cfg.
key=0x7fd9fc088298b571 scrc=0xbf57f14e210a29d5 sptr=5162816 fcrc=0xb84364badd1d748d flen=0 mdtm=154754
5184 wrtm=1695317097
Record (key 0x7fd9fc088298b571) reset.
root@show-s4x-config-i-0f5bf8e52e2a45563:/opt/splunk/etc/system/local# /opt/splunk/bin/splunk cmd btpr
obe -d /opt/splunk/var/lib/splunk/fishbucket/splunk_private_db/ --file /opt/data/syslog/device2/firewa
ll.log  --reset
Using logging configuration at /opt/splunk/etc/log-cmdline.cfg.
key=0xa6f86021bf0b84fc scrc=0x414ea3b3cc1a4916 sptr=5146581 fcrc=0xc3f60511ff64c816 flen=0 mdtm=154754
5184 wrtm=1695317097
Record (key 0xa6f86021bf0b84fc) reset.
root@show-s4x-config-i-0f5bf8e52e2a45563:/opt/splunk/etc/system/local# /opt/splunk/bin/splunk cmd btpr
obe -d /opt/splunk/var/lib/splunk/fishbucket/splunk_private_db/ --file /opt/data/syslog/device3/firewa
ll.log  --reset
Using logging configuration at /opt/splunk/etc/log-cmdline.cfg.
key=0xe9d1061cd785448f scrc=0x414ea3b3cc1a4916 sptr=5012859 fcrc=0x60b2c4eb45986862 flen=0 mdtm=154754
5184 wrtm=1695317097
Record (key 0xe9d1061cd785448f) reset.
root@show-s4x-config-i-0f5bf8e52e2a45563:/opt/splunk/etc/system/local# /opt/splunk/bin/splunk start
```

12. Validate your data by logging in to Splunk and running the following search over **All time**:

```
| tstats count where index=firewall by host source
```

13. Results should be a table with 3 columns:



```
| tstats count where index=firewall by host source
```

✓ 26,354 events (before 10/24/23 9:13:14.000 PM)   No Event Sampling ▾

host	source	count
device1	/opt/data/syslog/device1/firewall.log	8880
device2	/opt/data/syslog/device2/firewall.log	8852
device3	/opt/data/syslog/device3/firewall.log	8622

Optional Activity: Lab 2, Tasks 1-4 Accomplished Through the CLI

Description:

These 2 tasks are optional replacements of tasks 1-4 in Lab 2. You will create a sourcetype called **badge** that correctly parses our badge.log data. Then you will bring in the badge.log data via a CLI command called oneshot. You will then assign that data to the sourcetype named **badge** and the index named **badge**. Finally, you will verify that parsed events are coming into the UI.

Establish a Custom “badge” Source Type

1. Open your terminal app and run the following commands:

2. Switch to the root user:

```
sudo su
```

3. Navigate to the DataOnboarding4Ninjas directory:

```
cd /opt/splunk/etc/apps/DataOnboarding4Ninjas/
```

4. Create and open a **props.conf** file using the **vi** visual editor:

```
vi props.conf
```

5. Press the “ **i** ” key to start editing the file:

```
i
```

6. Within the configuration file, type or paste in the following stanza:

```
[badge]
SHOULD_LINEMERGE=false
LINE_BREAKER=(##)
TIME_PREFIX=\d+\.\d+\.\d+\.\d+\s
TIME_FORMAT=%m%d%y %H:%M
MAX_TIMESTAMP_LOOKAHEAD=14
TRUNCATE=1000
```

7. Exit the vi editor by pressing the **escape** key then typing **:wq** and hitting **enter**. This is telling the editor to save and exit back to the main CLI.

8. Restart Splunk:

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

9. Ingest data using oneshot by running the following command in the CLI. This is the same as "index once" in the Splunk GUI.

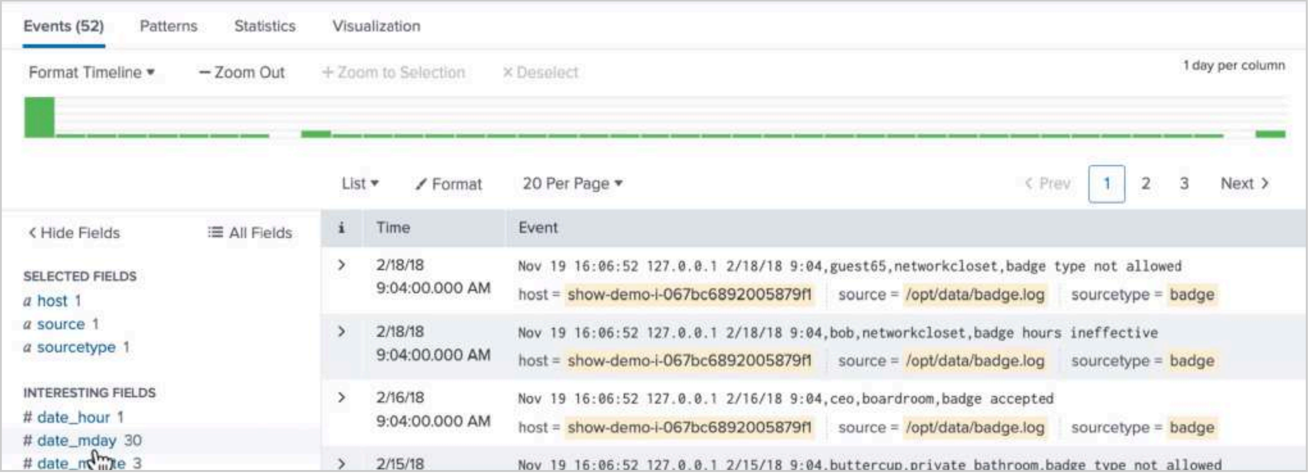
```
/opt/splunk/bin/splunk add oneshot /opt/data/badge.log -index badge -sourcetype
badge
```

10. Verify the badge data in Splunk by logging in to Splunk and navigating to the **DataOnboarding4Ninjas** app.

11. Click **Search** in the menu bar and run the following search over **All time**.

```
index=firewall sourcetype=badge
```

You should now see your badge data in the search results:



SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 1
# date_mday 30
# date_minute 3

i	Time	Event
›	2/18/18 9:04:00.000 AM	Nov 19 16:06:52 127.0.0.1 2/18/18 9:04,guest65,networkcloset,badge type not allowed host = show-demo-i-067bc6892005879f1 source = /opt/data/badge.log sourcetype = badge
›	2/18/18 9:04:00.000 AM	Nov 19 16:06:52 127.0.0.1 2/18/18 9:04,bob,networkcloset,badge hours ineffective host = show-demo-i-067bc6892005879f1 source = /opt/data/badge.log sourcetype = badge
›	2/16/18 9:04:00.000 AM	Nov 19 16:06:52 127.0.0.1 2/16/18 9:04,ceo,boardroom,badge accepted host = show-demo-i-067bc6892005879f1 source = /opt/data/badge.log sourcetype = badge
›	2/15/18	Nov 19 16:06:52 127.0.0.1 2/15/18 9:04,buttercup,private bathroom,badge type not allowed