Splunk Enterprise 7.1 System Administration

Document Usage Guidelines

- Should be used only for enrolled students
- Not meant to be a self-paced document, an instructor is needed
- Do not distribute

Course Prerequisites

- Required:
  - Splunk Fundamentals 1
- Strongly Recommended:
  - Splunk Fundamentals 2

Course Goals

- Identify Splunk components and understand the basics of a Splunk deployment
- Manage Splunk licensing
- Install a Splunk app
- Understand Splunk configuration files
- Create and manage Splunk indexes
- Create users and roles in Splunk
- Introduce distributed search and Splunk clustering

Course Outline

Module 1: Splunk Deployment Overview

Module 2: License Management

Module 3: Splunk Apps

Module 4: Splunk Configuration Files

Module 5: Splunk Indexes

Module 6: Splunk Index Management

Module 7: Splunk User Management

Module 8: Splunk Authentication Management

Module 9: Configuring Basic Forwarding

Module 10: Distributed Search

Module 11: Introduction to Splunk Clusters

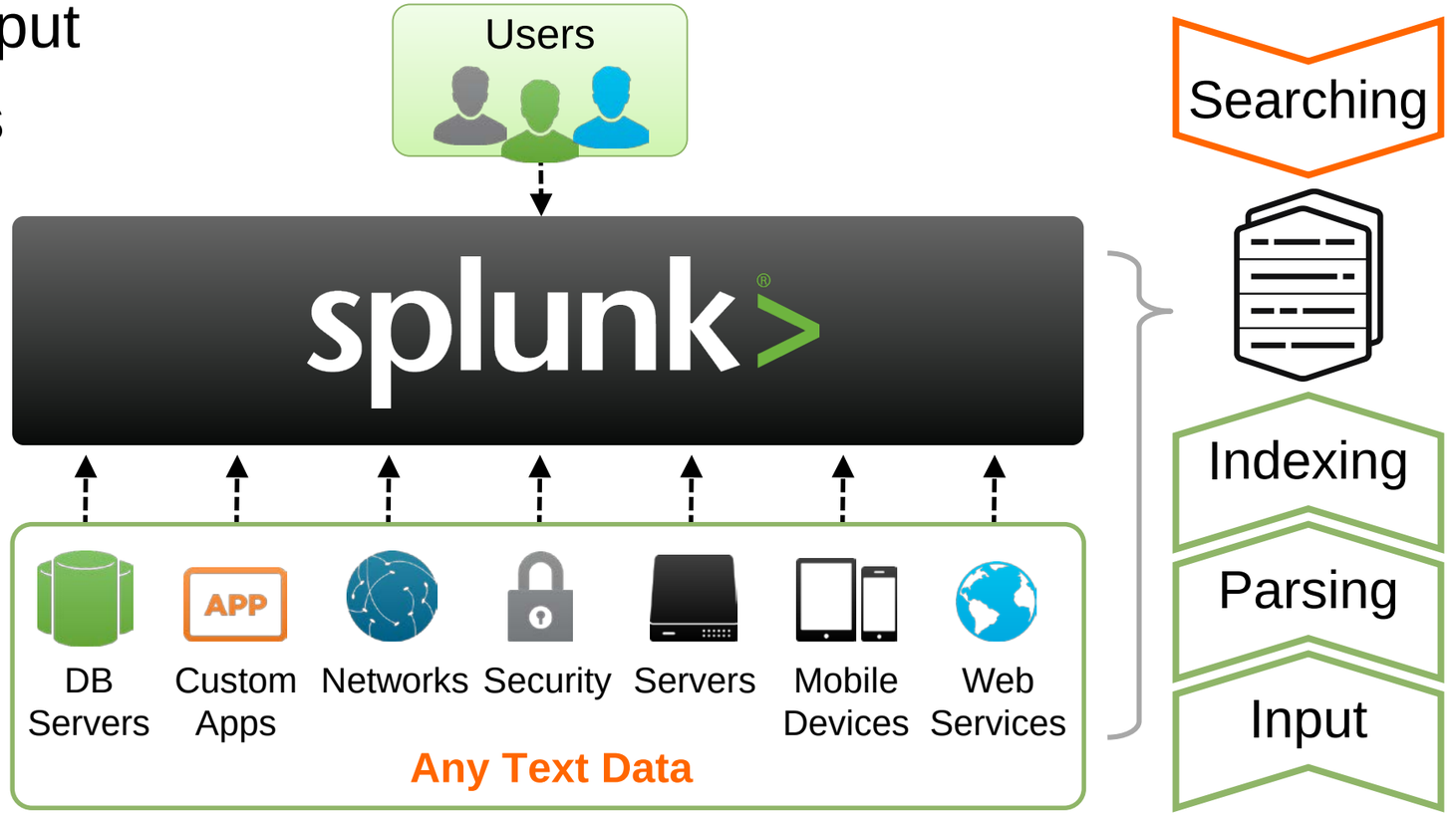
Module 1: Splunk Deployment Overview

Module Objectives

- Provide an overview of Splunk
- Identify Splunk Enterprise components
- Identify the types of Splunk deployments
- Describe the Splunk System Administrator role
- List the steps to install Splunk
- Use Splunk CLI commands
- Enable the Monitoring Console (MC)

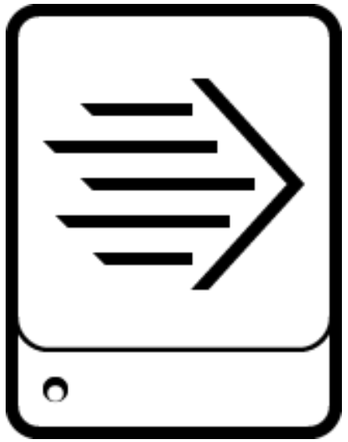
Splunk Overview

- Splunk can be deployed in a variety of configurations
- Scales from a single server to a distributed infrastructure
  - Accepts any text data as input
  - Parses the data into events
  - Stores events in indexes
  - Searches and reports
  - Authenticates users

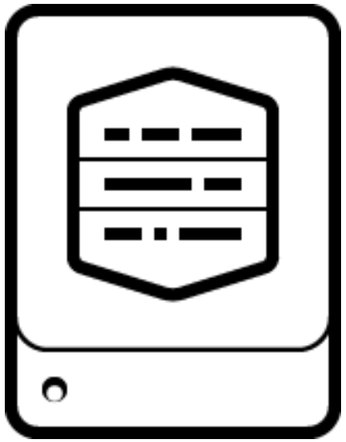


Splunk Enterprise Components

The most common processing Splunk components are:



Forwarder

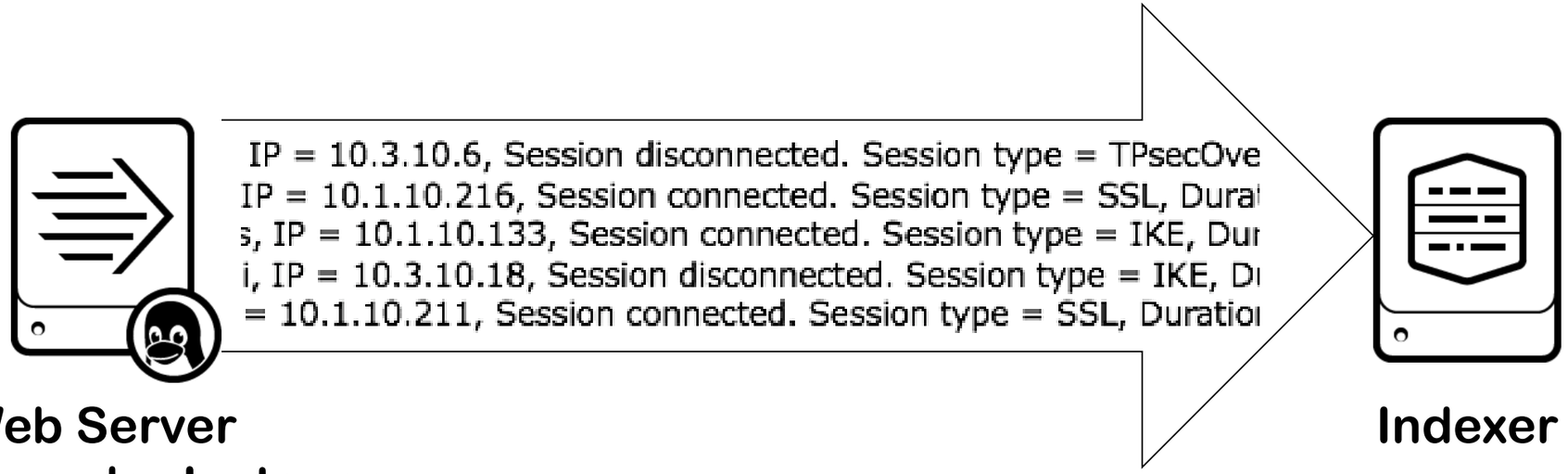


Indexer

Search Head

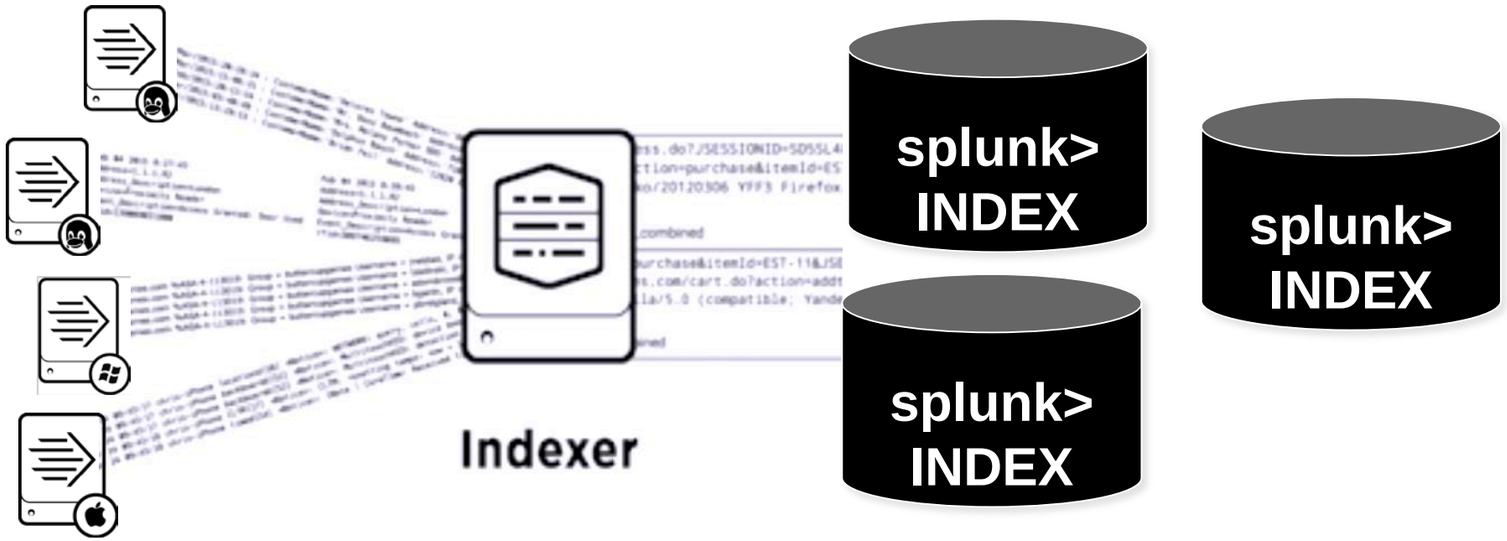
Splunk Components – Forwarders

- Splunk instances that monitor configured inputs and forward the data to the index
  - Best practice data collection method
- Requires minimal resources and typically installed on the machines that produce the data



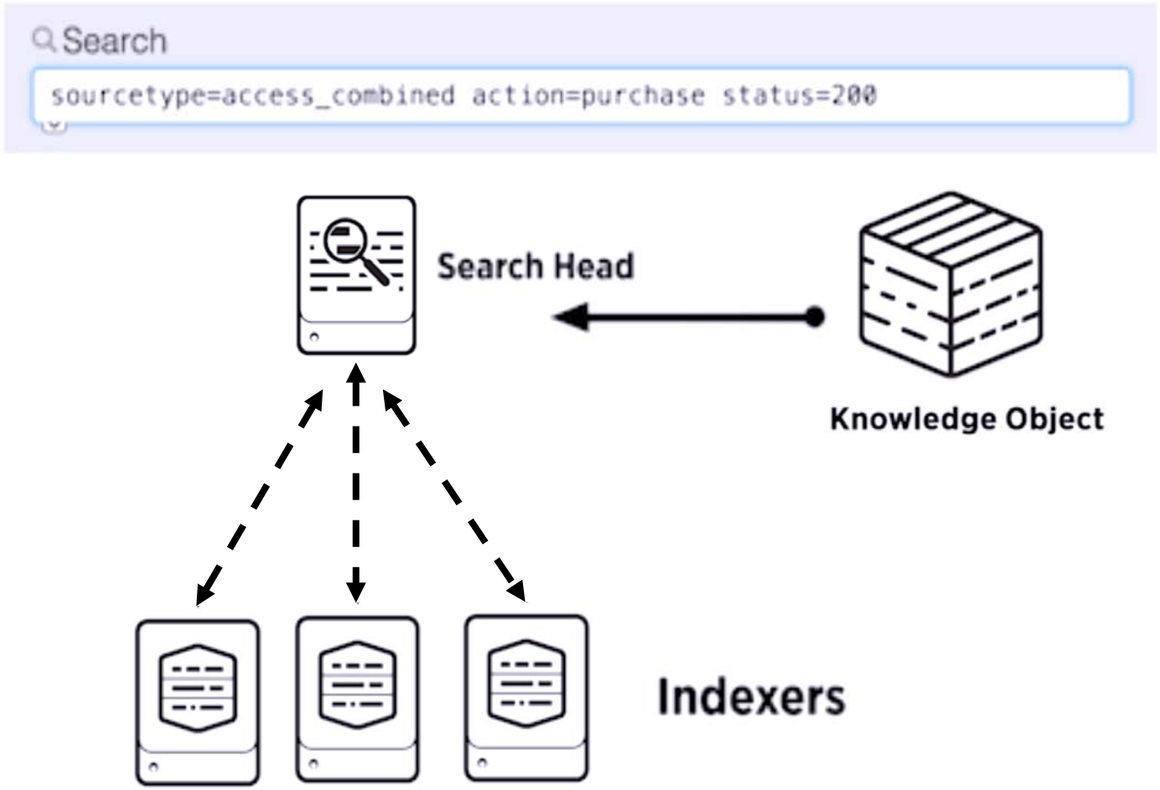
Splunk Components – Indexers

- Reside on dedicated machines
- Receive, index, and store incoming data from forwarders
- Search data in response to requests received from the search heads



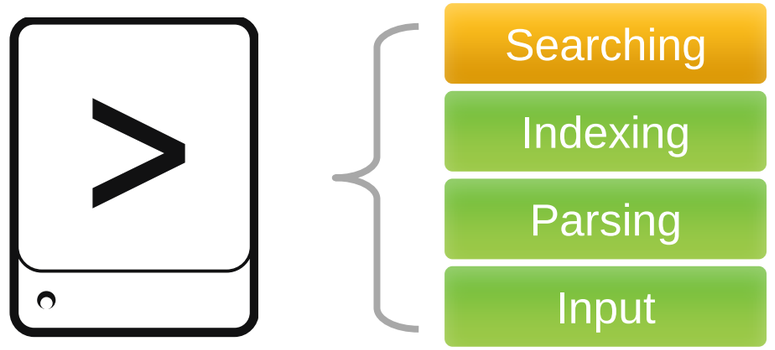
Splunk Components – Search Heads

- Allow users to submit search requests using SPL
- Distribute search requests to the Indexers
- Consolidate results and render visualizations of results
- Search-time knowledge objects are stored on the search heads Examples include:
  - Field extractions
  - Alerts
  - Dashboards



Splunk Deployment – Standalone

- Single Server
  - All functions in a single instance of Splunk
  - For testing, proof of concept, personal use, and learning
  - This is what you get when you download Splunk and install with default settings
- Recommendation
  - Have at least one test/development setup at your site

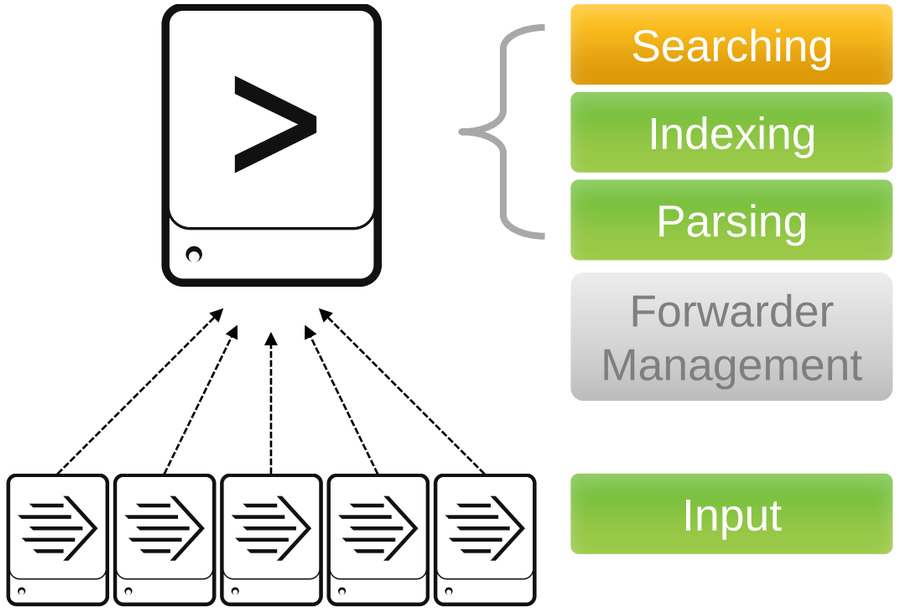


Note

This is the initial configuration in class.

Splunk Deployment – Basic

- Splunk server
  - Similar to server in standalone configuration
  - Manage deployment of forwarder configurations
- Forwarders
  - Forwarders collect data and send it to Splunk servers
  - Install forwarders at data source (usually production servers)

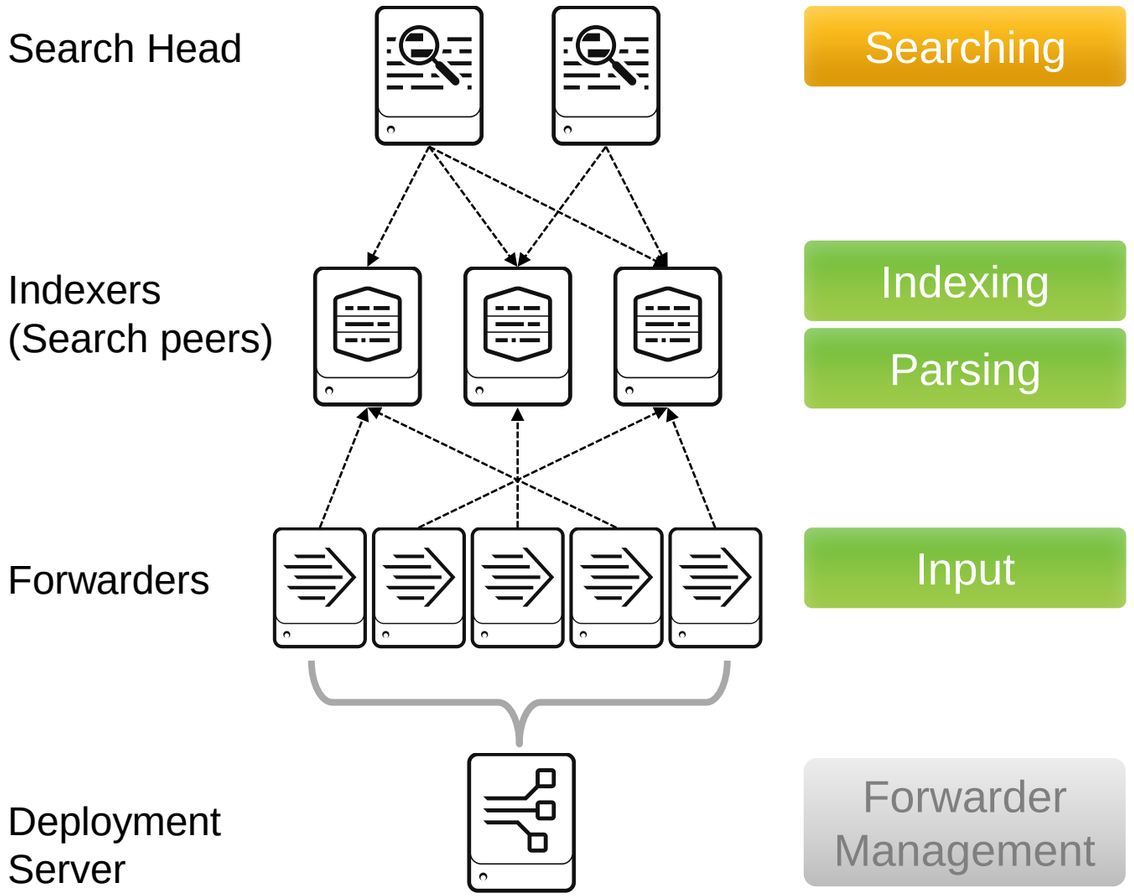


Note

Your lab environment will evolve to include a separate forwarder.

Splunk Deployment – Distributed

- Splunk can be distributed and scaled in a variety of ways
  - More indexers to handle more inputs
  - More indexers AND search heads to handle more searching
- Manage forwarder configurations from a dedicated Deployment Server



Note

You will add a single search peer to your environment in a later lab exercise.

System Administrator vs Data Administrator

- The Splunk System Administrator is primarily responsible for system management efforts which include:
  - Monitor MC and respond to system health alerts
  - Install and manage Splunk apps
  - Manage Splunk licensing
  - Manage Splunk indexes
  - Manage Splunk users and authentication
  - Manage Splunk configuration files
- The Splunk Data Administrator is primarily responsible for data onboarding and management efforts which include:
  - Work with users requesting new data sources
  - Document existing and newly ingested data sources
  - Design and manage inputs for UFs/HFs to capture data
  - Manage parsing, event line breaking, timestamp extraction
  - Move configuration through non-production testing as required
  - Deploy changes to production
  - Manage Splunk configuration files

Reference Servers Hardware

	Indexer	Search Head
OS	Linux or Windows 64-bit distribution	
Network	1Gb Ethernet NIC Optional second NIC for a management network	
Memory	12 GB RAM	
CPU	Intel 64-bit chip architecture **12 CPU cores** Running at 2+ GHz	Intel 64-bit chip architecture **4 CPUs, quad-core per CPU** Running at 2+ GHz
Disk	Disk subsystem capable of 800 IOPS RAID 10	2 x 10K RPM 300GB SAS drives - RAID 1

- Hardware requirements and sizing are discussed in detail in Architecting and Deploying Splunk class
  docs.splunk.com/Documentation/Splunk/latest/Capacity/Referencehardware

Splunk Installation Overview

- Pre-installation Checklist
  - Start-up account
  - Time synchronization
  - Splunk ports
  - Linux setting recommendations
- Installation
  - Splunk directory structure
- Post-installation configuration
  - Run Splunk at boot
  - Configure system settings
  - Optionally, enable Monitoring Console

Start-up Account

- **Best practice**: Do not run Splunk as ***super-user***
  - For example, **root** on *NIX, **administrator** on Windows
- Create a user account that is used to run Splunk
  - For input, Splunk must be able to access data sources
    - On *NIX, **`/var/log`** is not typically open to non-root accounts
  - On *NIX, non-root accounts cannot access ports < 1024
  - On Windows
    - Use a domain account if Splunk has to connect to other servers
    - Otherwise, use a local machine account that can run services
  - Make sure the Splunk account can access scripts used for inputs and alerts

Time Synchronization

- **Best practice:** Use a time synchronization service such as **NTP**
- Splunk searches depend on accurate time
  - Correct event timestamping is essential
- It is imperative that your Splunk indexer and production servers have standardized time configuration
  - Clock skew between hosts can affect search results

Splunk Default Ports

Usage	Splunk Enterprise	Universal Forwarder
splunkd	**8089**	**8089**
Splunk Web	**8000**	-
Web app-server proxy	**8065**	-
KV Store	**8191**	-
S2S receiving port(s)	No default	-
Any network/http input(s)	No default	No default
Index replication port(s)	No default	-
Search replication port(s)	No default	-

Linux Setting Recommendations

- Increase **`ulimit`** settings
  - The following OS parameters need to be increased to allow for a large number of buckets/forwarders/users

docs.splunk.com/Documentation/Splunk/latest/Troubleshooting/ulimitErrors

```
ulimit -a
ulimit -c 1073741824   (1 GB)                    (unlimited)
ulimit -n 48 x default (48 x 1024 = 49,152) (65536)
ulimit -u 12 x default (12 x 1024 = 12,288) (258048)
```

core file size
open files
max user processes

- Turn Transparent Huge Pages (THP) off on Splunk Enterprise servers

docs.splunk.com/Documentation/Splunk/latest/ReleaseNotes/SplunkandTHP

Installation

- Download Splunk Enterprise from www.splunk.com/download
- Installation: (as account running Splunk)
  - ***NIX** – un-compress the **`.tar.gz`** file in the path you want Splunk to run from
    - Also available as **`rpm`**, **`deb`**
  - **Windows** – execute the **`.msi`** installer and follow the wizard steps
- Complete installation instructions at:
  docs.splunk.com/Documentation/Splunk/latest/Installation/Chooseyourplatform
- After installation:
  - Splunk starts automatically on Windows
  - Splunk must be manually started on *NIX until **boot-start** is enabled

Run Splunk at Boot

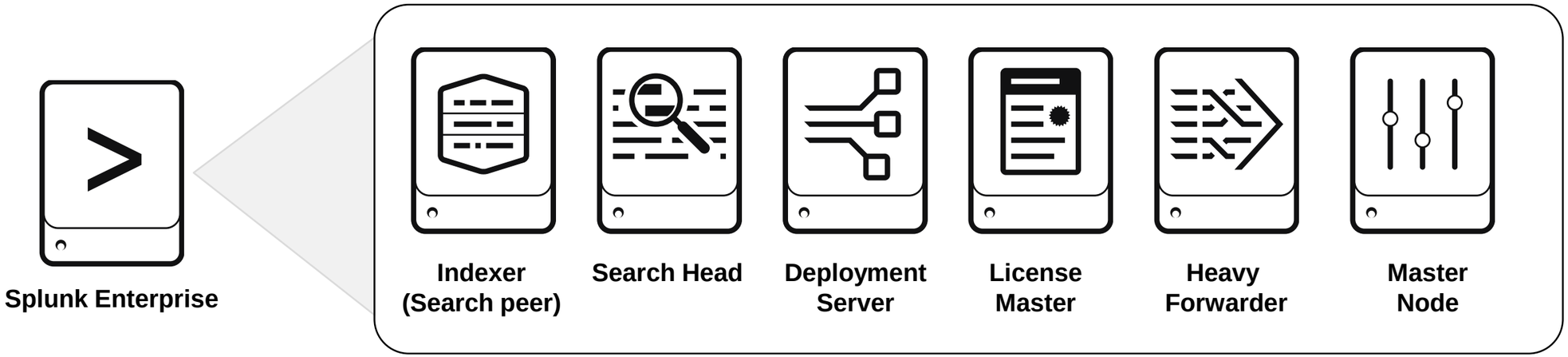
- *NIX
  - Splunk on *NIX does not auto-start at boot time (default)
  - Required practice to enable boot-start, run as **`root`**:

```
# ./splunk enable boot-start -user splunker
```

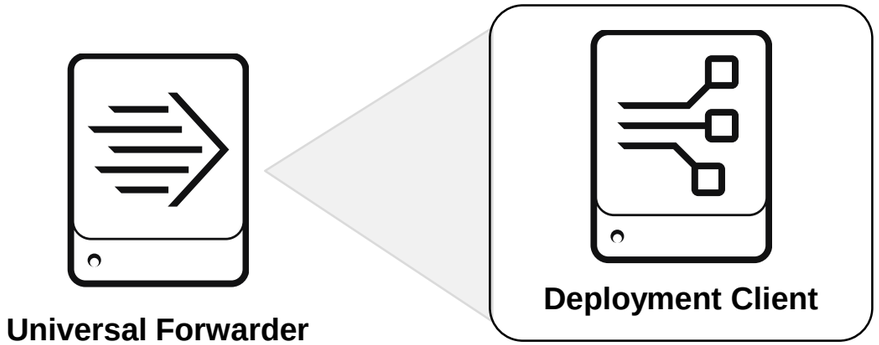
  - This modifies the *NIX boot-up configuration
    - Modifies **`/etc/init.d`** depending on your *NIX flavor
  - Pass the **`-user`** parameter to start Splunk as the correct user
- Windows
  - Runs as **`splunkd`** service and starts child processes
  - The service starts and stops like any Windows services

What Software Do You Install?

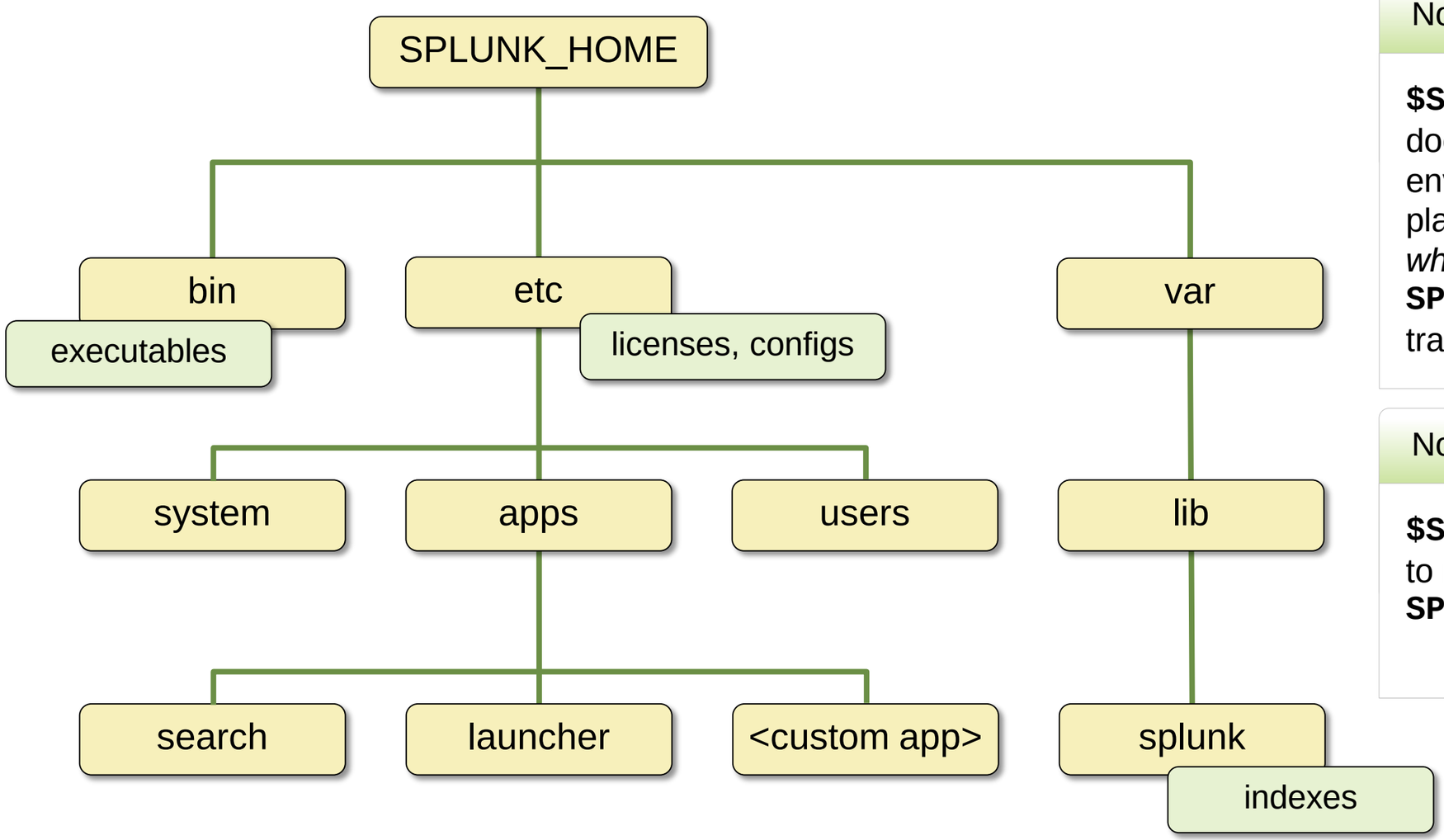
- Included in the Splunk Enterprise software package



- Included in the Universal Forwarder software package



Splunk Directory Structure



Note

$SPLUNK_HOME depicted in the documentation is not an exported environment variable. It is used as a placeholder for "*the top directory where Splunk is installed.*" **SPLUNK_HOME** is used in this training.

Note

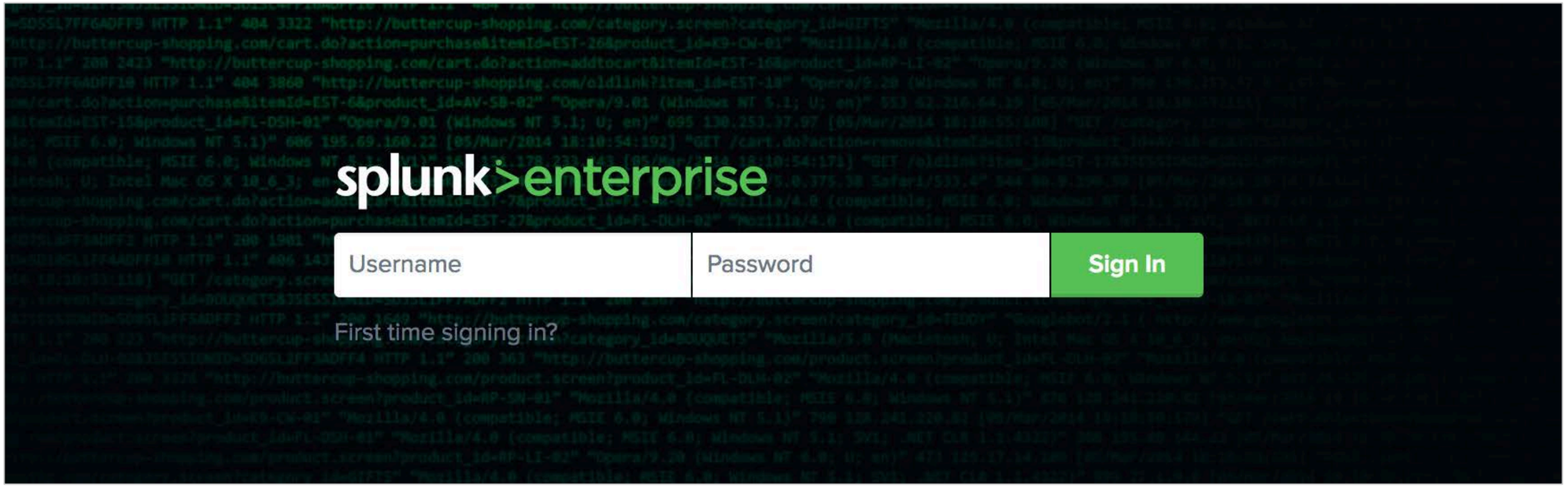
$SPLUNK_DB is used in this training to refer to **SPLUNK_HOME/var/lib/splunk**

splunkd

- Runs on port 8089 (default) using SSL
- Spawns and controls Splunk child processes (helpers):
  - Splunk Web proxy, KV store, and Introspection services
  - Each search, scripted input, or scripted alert
- Accesses, processes, and indexes incoming data
- Handles all search requests and returns results

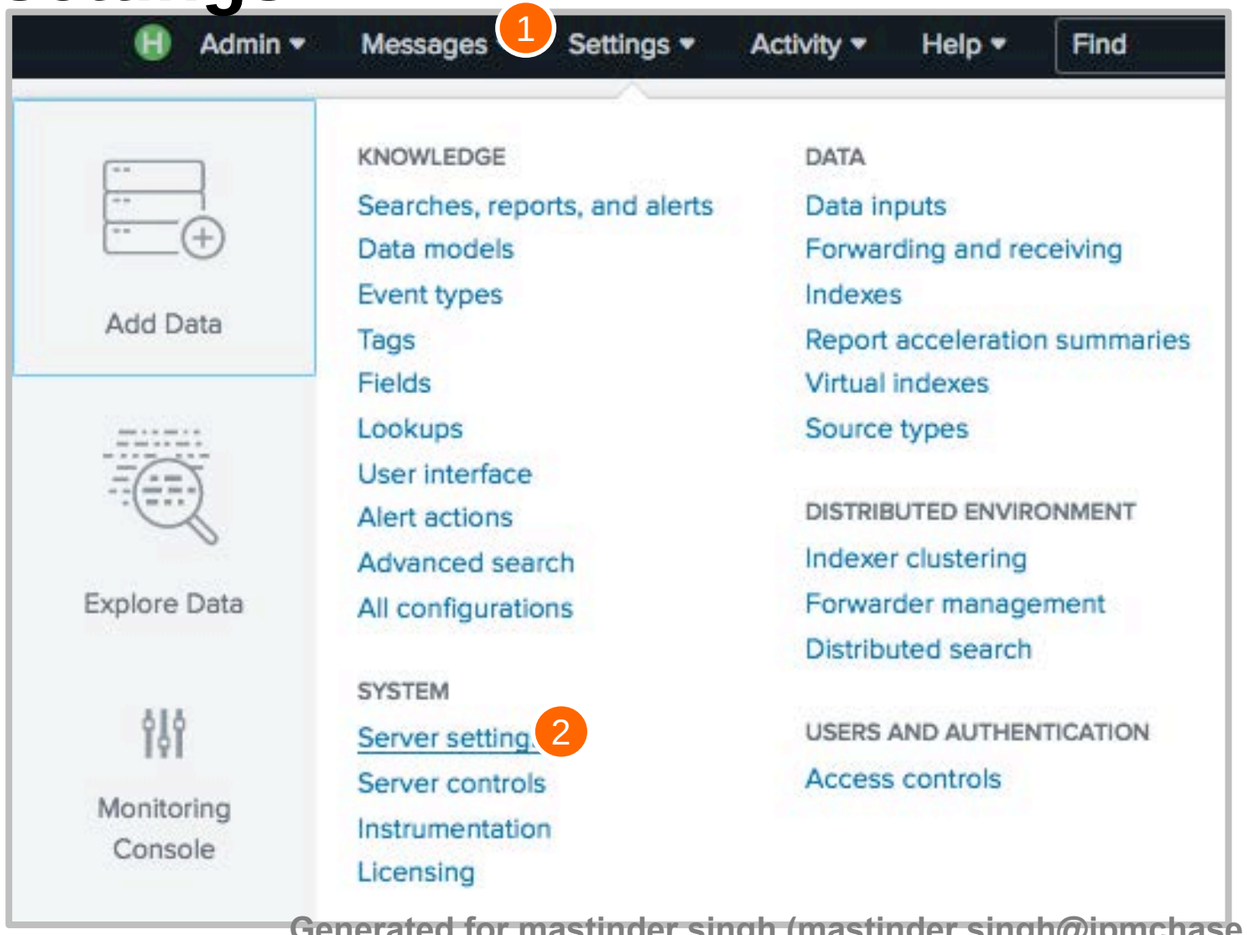
Splunk Web

- Splunk Web is browser-based user interface
  - Provides both a search and management front end for **splunkd** process
- Runs on port 8000 by default
  - **`http://<server_name>:<port>`**

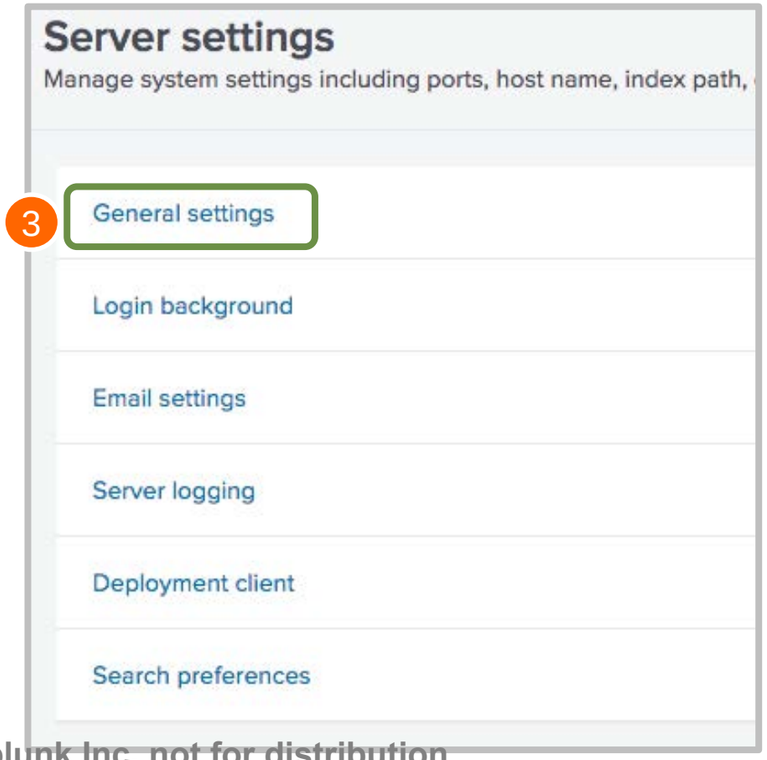


Splunk Web - Server Settings

- Administrators can select **Settings > Server settings > General settings**

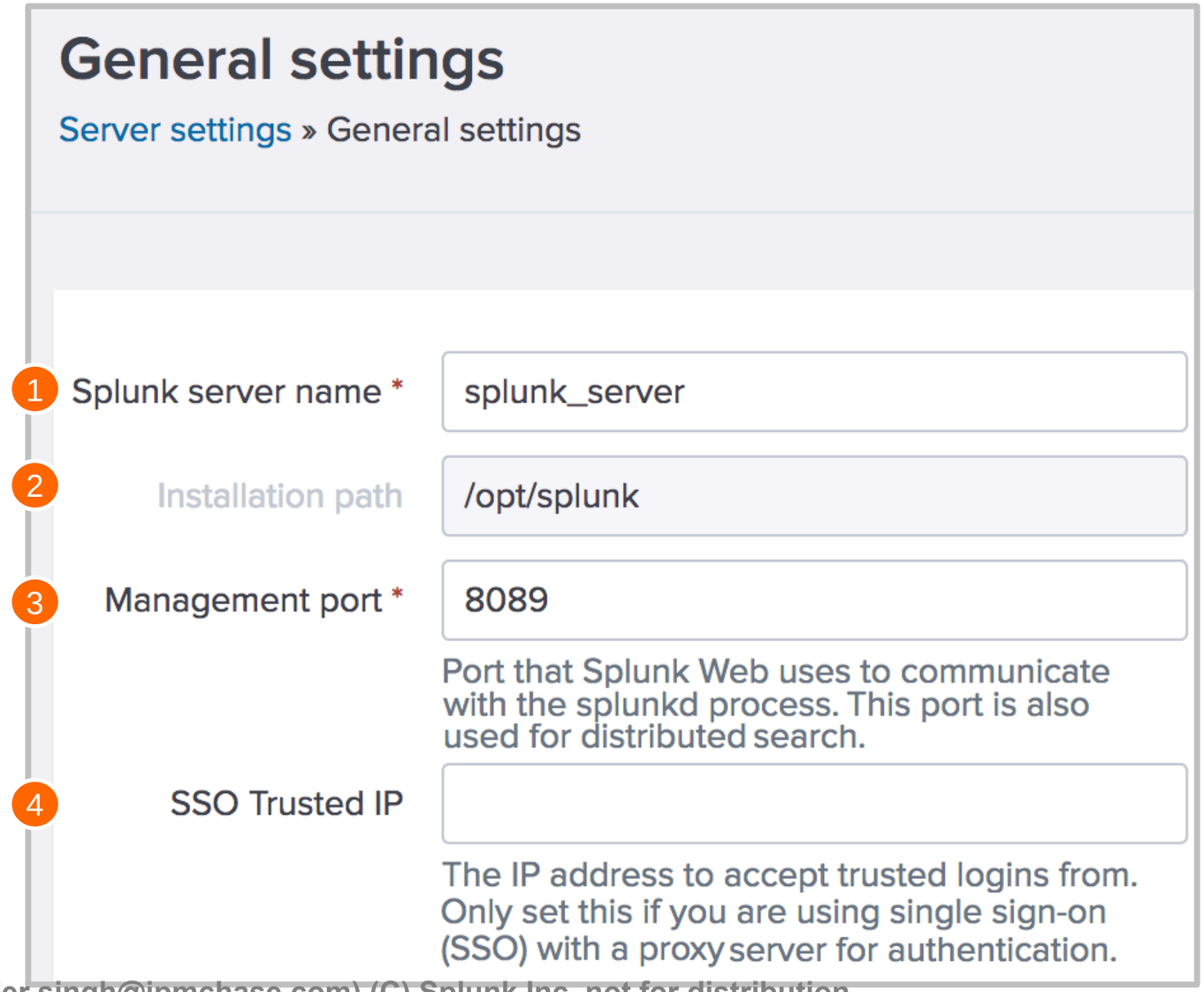


- Overall server configuration
- Used to set server options



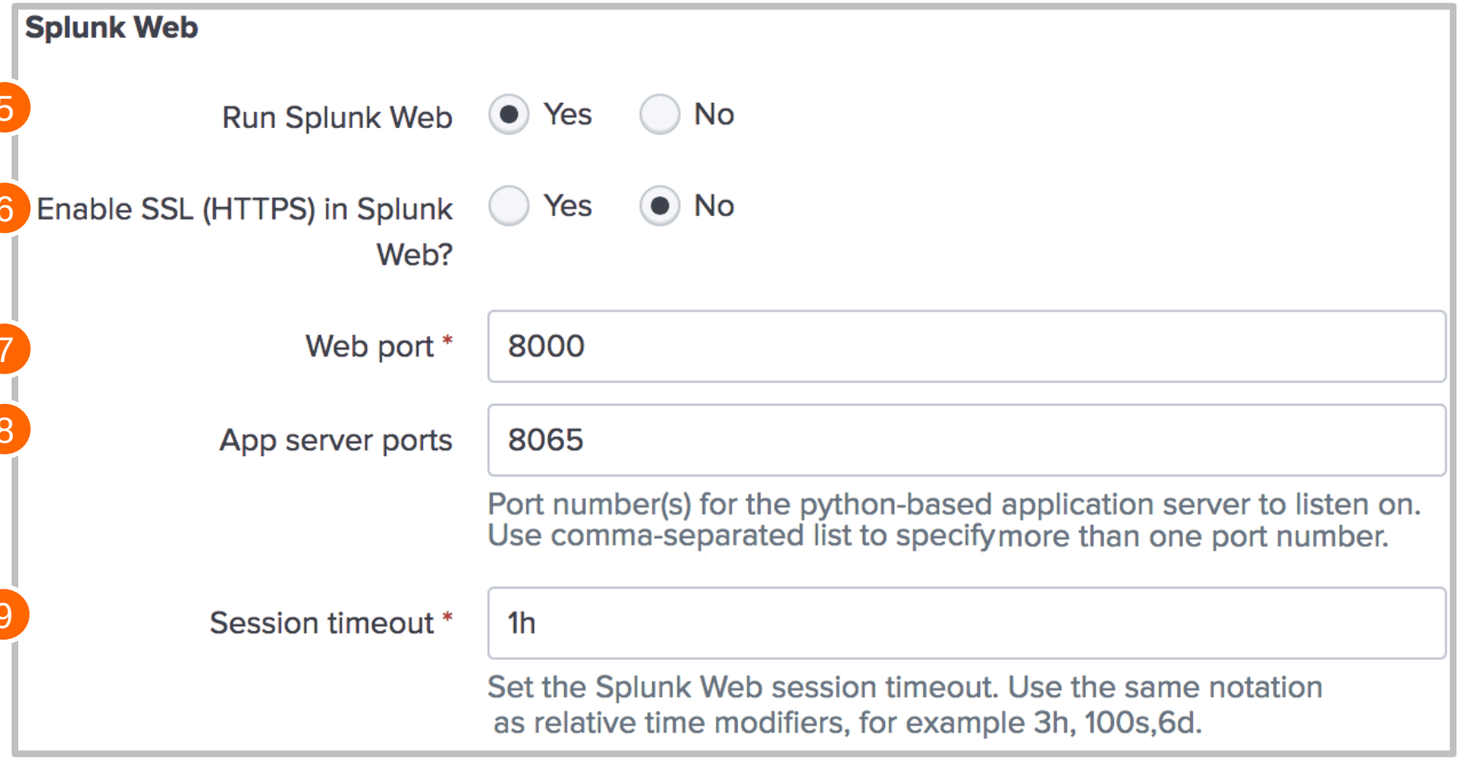
Describing General Settings

1. Identifies this server to other Splunk servers
2. Identifies the installation path **`SPLUNK_HOME`**
3. Identifies the splunkd port
4. Identifies the IP address used for SSO authentication configurations



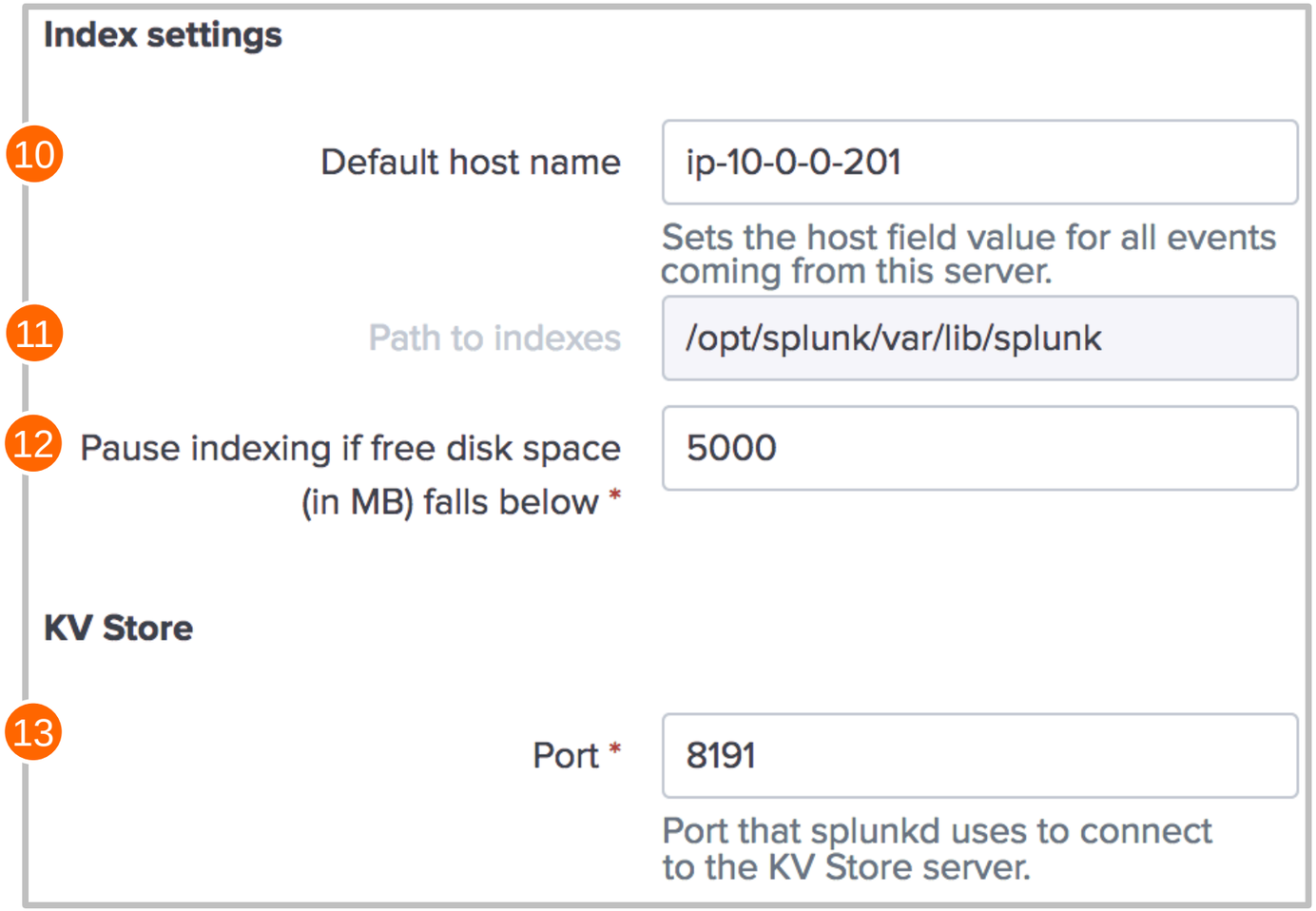
Describing General Settings – Splunk Web

5. Enables Splunk Web
6. Enables HTTPS for Splunk Web
7. Identifies the Splunk Web port
8. **App server ports** (8065) is the python-based application server to listen on. Set to "0" only if you want to run Splunk Web in legacy mode (not compatible with SHC)
9. Sets the Splunk Web session timeout



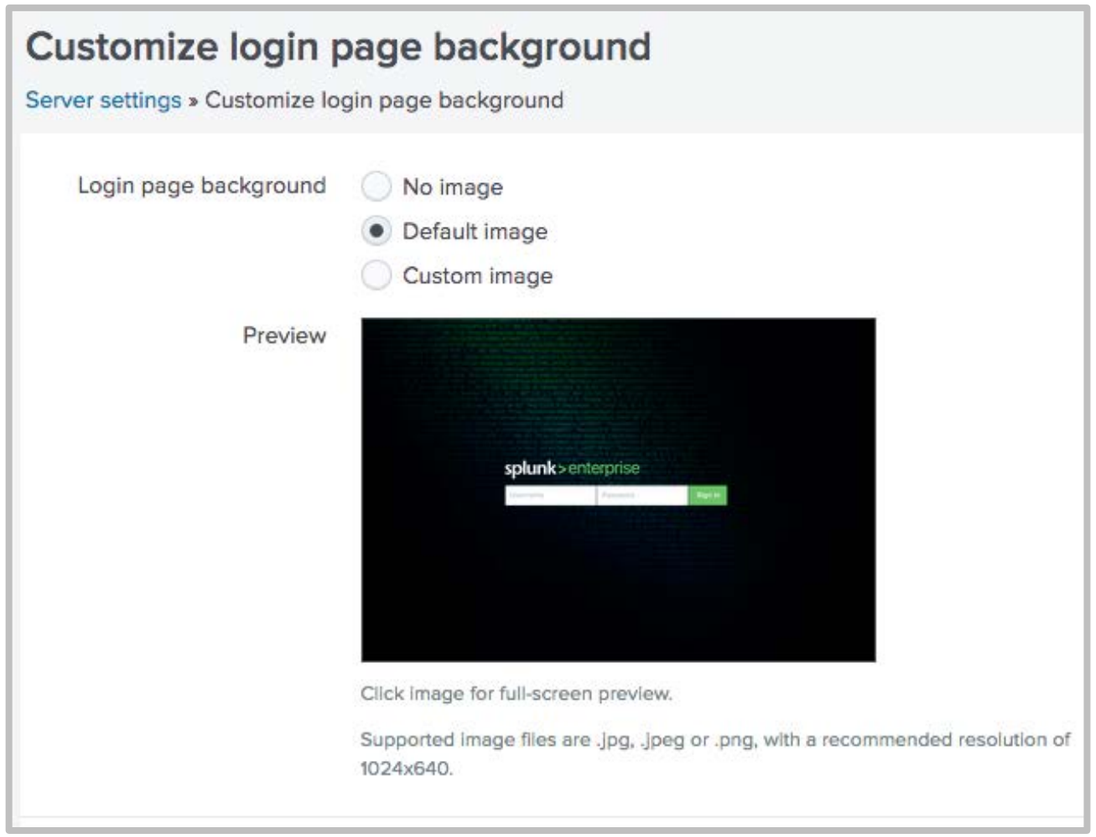
Describing General Settings – Index/KV Store

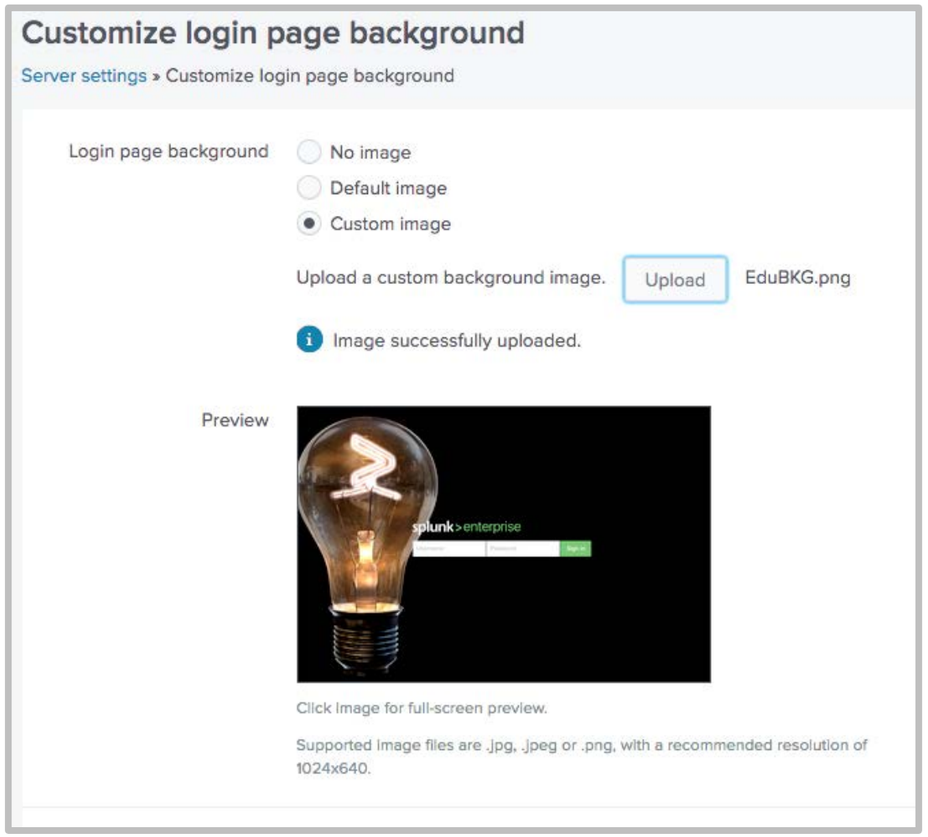
10. Default host name which is the default value for the host field for inputs forwarded (indexed) from this server
11. Identifies the path to the existing indexes (read-only in UI)
12. Sets the minimum free disk space setting the datastore location can fall before Splunk stops indexing
13. Defines the port used by the KV Store to communicate with splunkd



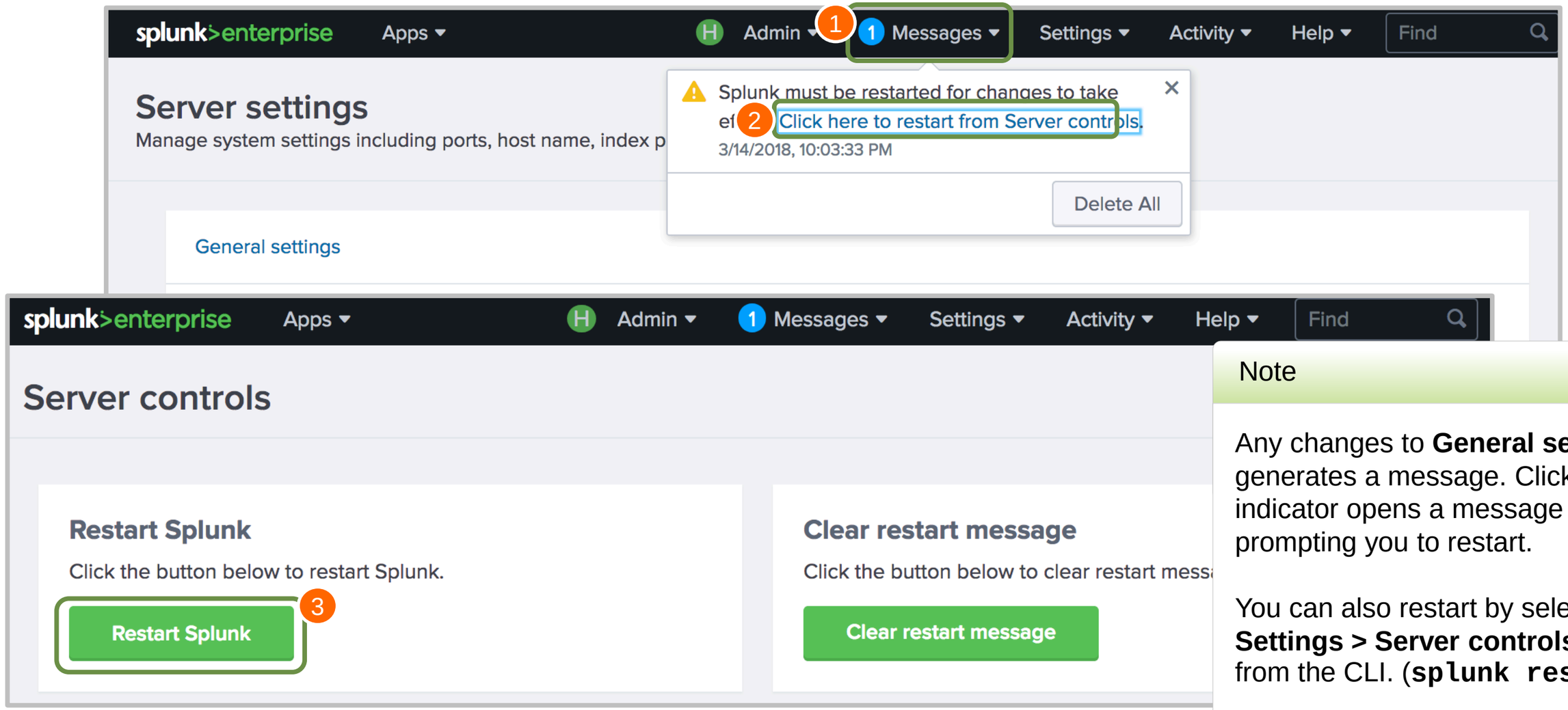
Customizing Login Background

Select **Server settings > Login background** to customize the login page





Restarting the Server from Splunk Web



Note

Any changes to **General settings** generates a message. Clicking the indicator opens a message prompting you to restart.

You can also restart by selecting **Settings > Server controls** or from the CLI. (**`splunk restart`**)

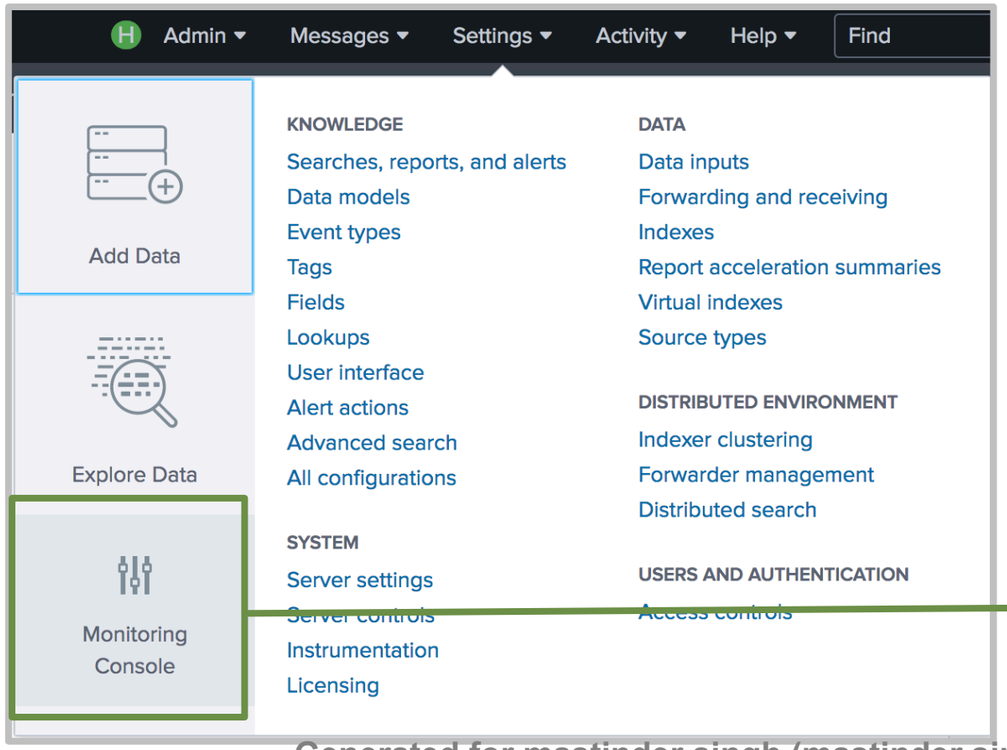
The Splunk Command Line Interface (CLI)

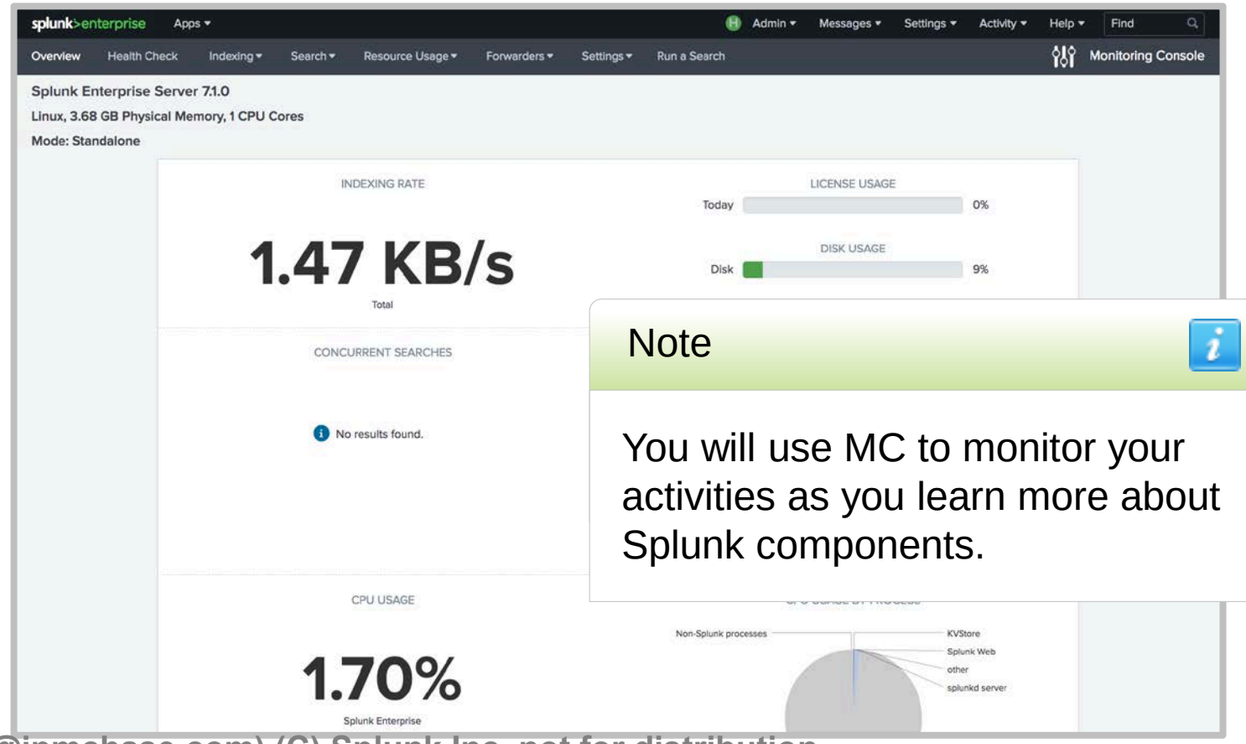
- **`splunk`** is an executable command in the **`bin`** directory
  - Same syntax is used on all supported platforms

Command	Operation
`splunk help`	Display a usage summary
`splunk help <object>`	Display the details of a specific object
`splunk [start | stop | restart]`	Manages the Splunk processes
`splunk start –-accept-license`	Automatically accept the license without prompt
`splunk status`	Display the Splunk process status
`splunk show splunkd-port`	Show the port that the **splunkd** listens on
`splunk show web-port`	Show the port that Splunk Web listens on
`splunk show servername`	Show the servername of this instance
`splunk show default-hostname`	Show the default host name used for all data inputs

Monitoring Console (MC)

- Splunk collects a lot of data about itself
- MC is a Splunk admin-only app used to monitor and investigate Splunk performance, resource usage, and more



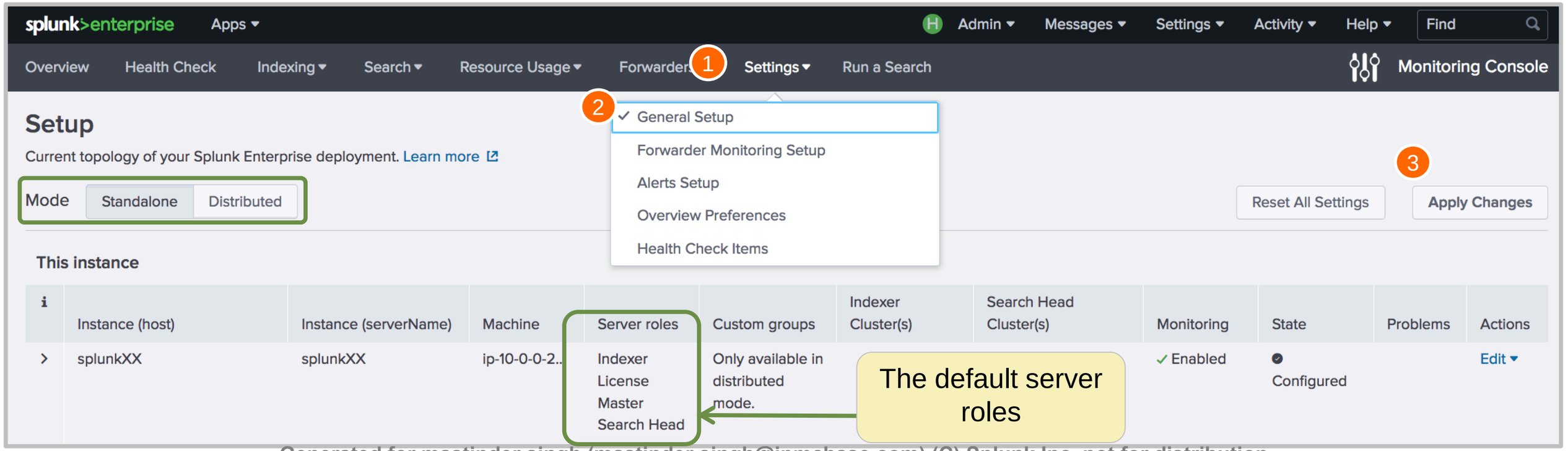


Note

You will use MC to monitor your activities as you learn more about Splunk components.

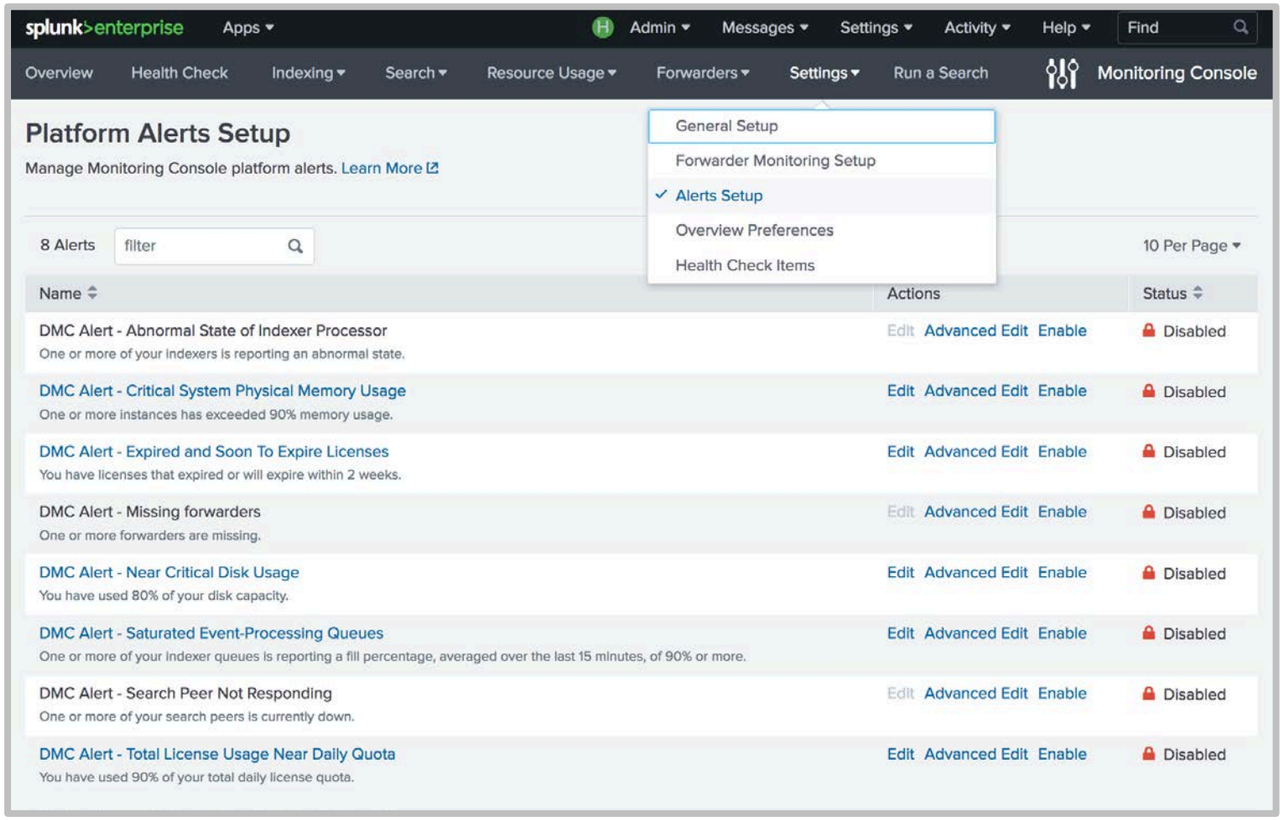
Enabling MC in Standalone Mode

- MC runs un-configured in standalone mode by default
- To enable, click **Settings > General Setup > Apply Changes**
  - You must **Apply Changes** to initialize the MC and after any change



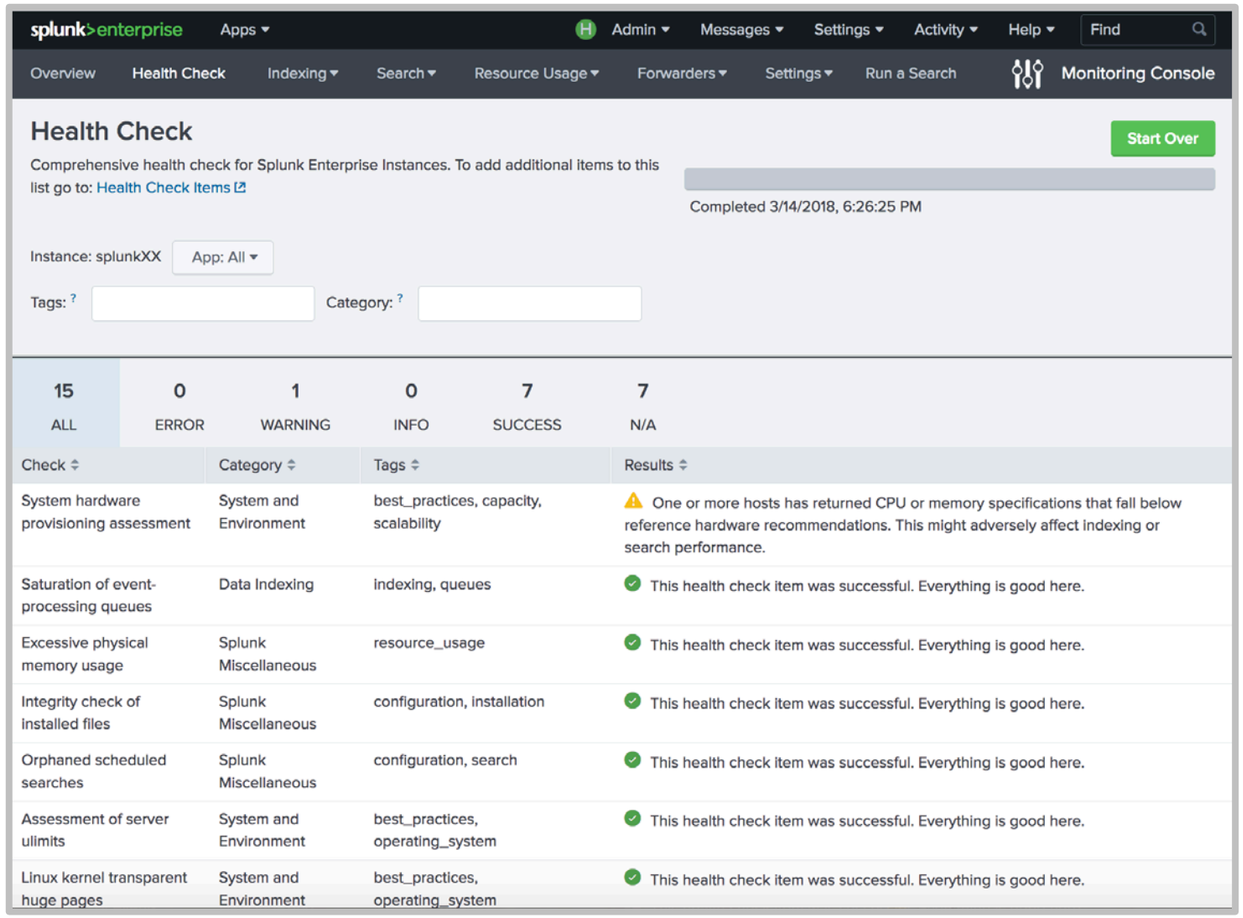
Enabling MC Platform Alerts

- Effective operation of your Splunk environment is timely identification and notification of critical conditions
  - Any item over 80% mark can't be good
- MC **Alerts Setup** provides a number of preconfigured platform alerts
  - Platform alerts are disabled by default
  - Tweak parameters such as alert schedule, suppression time, and alert actions



MC Health Check Items

- In addition to platform alerts, MC comes with preconfigured health checks
- Each health check is an ad hoc search that runs sequentially
  - **Monitoring Console > Health Check**
- Health checks can be disabled, modified, created, and exported
  - **Settings > Health Check Items**



More Resources

- Splunk Documentation: http://docs.splunk.com/Documentation
- Splunk App Repository: https://splunkbase.splunk.com/
- Splunk Answers: http://answers.splunk.com/
- Splunk Blogs: https://www.splunk.com/blog/
- Splunk Wiki: http://wiki.splunk.com/
- Splunk User Groups: https://usergroups.splunk.com/

Lab Exercise 1 – Configure Splunk

Time: 15 minutes

Tasks:

- Log into Splunk Web
- Change Splunk server name
- Restart Splunk
- Enable MC
- Use CLI to confirm the status and changes

Module 2: License Management

Module Objectives

- Identify license types
- Describe license violations
- Add and remove licenses

Splunk License Types

- **Enterprise trial license**
  - Downloads with product
  - Features same as Enterprise except for 500mb per day limit
  - Only valid for 60 days, after which one of the other 3 license types must be activated
  - ***Sales trial license*** is a trial Enterprise license of varying size and duration
- **Enterprise license**
  - Purchased from Splunk
  - Full functionality for indexing, search head, deployment server, etc.
  - Sets the daily indexing volume
  - No-enforcement license, allows users to keep searching even if you are in a license violation period

Splunk License Types (cont.)

- **Free license**
  - Disables alerts, authentication, clustering, distributed search, summarization, and forwarding to non-Splunk servers
  - Allows 500mb/day of indexing and forwarding to other Splunk instances
- **Forwarder license**
  - Sets the server up as a heavy forwarder
  - Applies to non-indexing forwarders
  - Allows authentication, but no indexing
- Splunk license comparison:

https://www.splunk.com/en_us/products/splunk-enterprise/free-vs-enterprise.html

License Warnings and Violations

- If the indexing exceeds the allocated daily quota in a pool, an alert is raised in Messages (pool warning) on any page in Splunk Web
  - The daily license quota resets at midnight
- 5 or more warnings on an enforced Enterprise license or 3 warnings on a Free license, in a rolling 30-day period, is a *violation*
- Splunk Enterprise 6.5.0 and later will provide warnings but it will not disable search during the violation period
  - Prior versions of Splunk would disable search

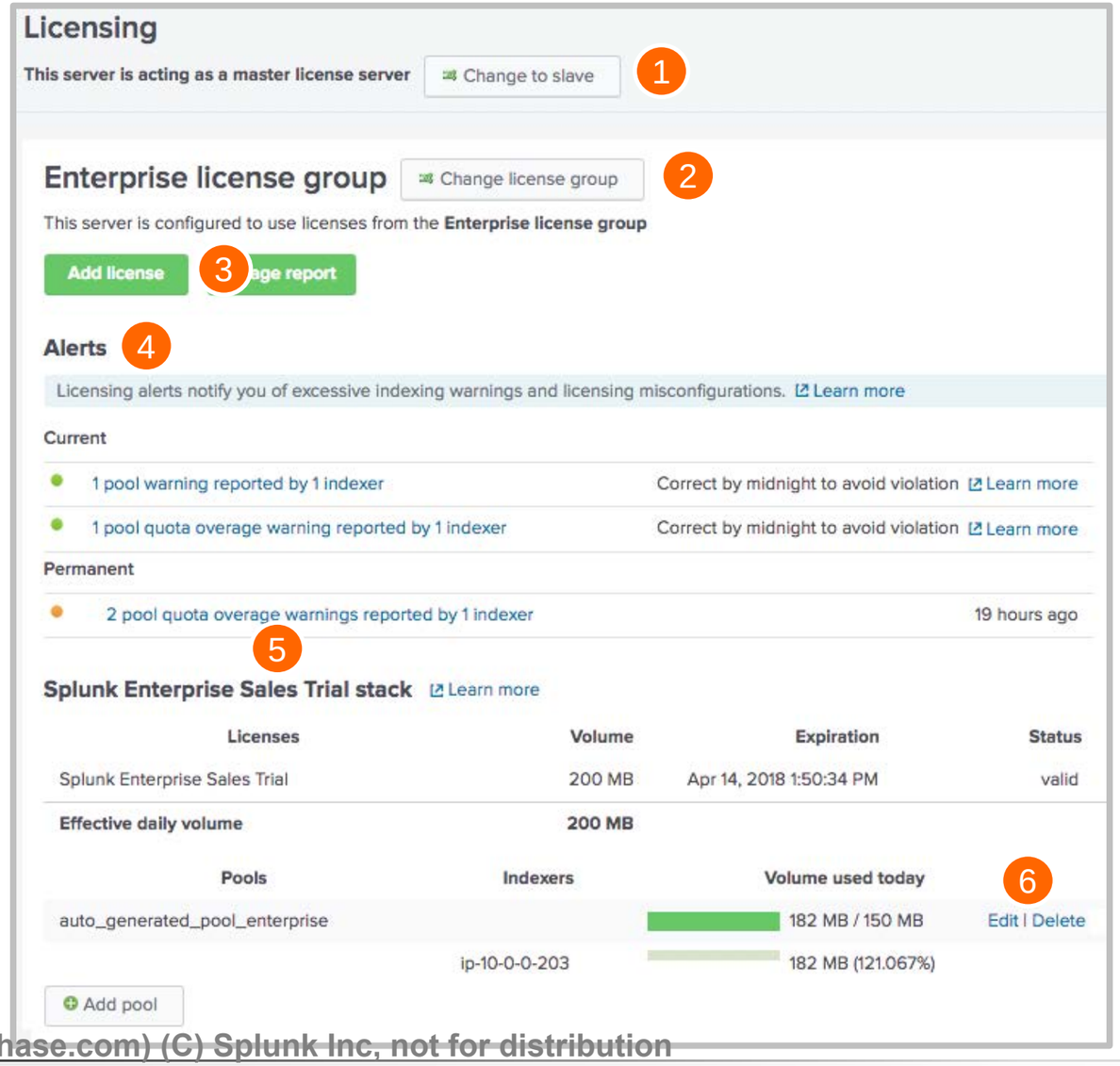
What Counts As Daily License Quota?

- All data from all sources that is indexed
  - It is the data (full size) that flows through the parsing pipeline, per day, per indexer
  - It is not the amount of storage used by the indexes
- What does not count against your license daily quota?
  - Replicated data (Index Clusters)
  - Summary indexes
  - Splunk internal logs (_internal, _audit, etc. indexes)
  - Structural components of an index (metadata, tsidx, etc.)
- Metrics data counts against a license at a fixed 150 bytes per metric event
  - Draws from the same license quota as event data

Managing Licenses

Select **Settings > Licensing**

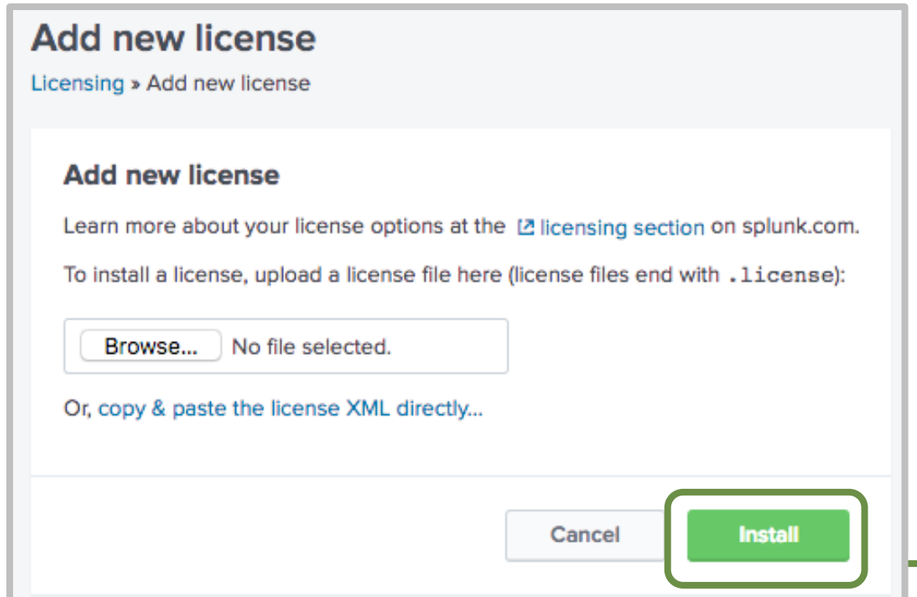
1. Designate the license server type
   – Master or slave
2. Change license group
3. Add a license
4. Check license alerts and violations
5. View stacks
6. Edit and add pools

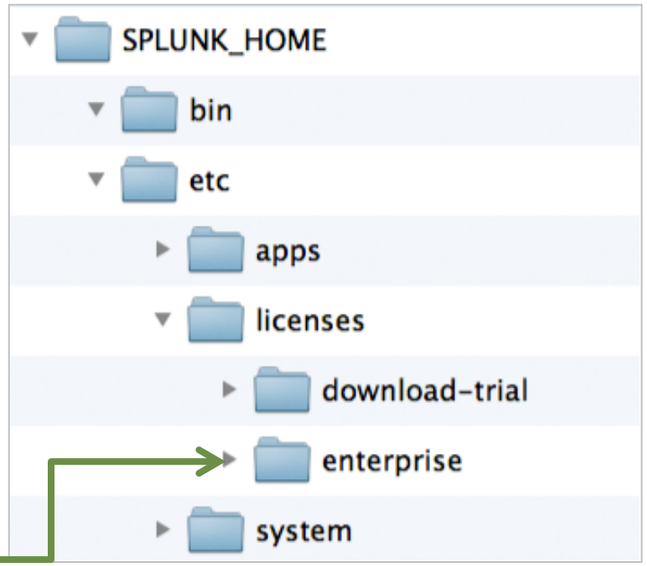


Adding a License

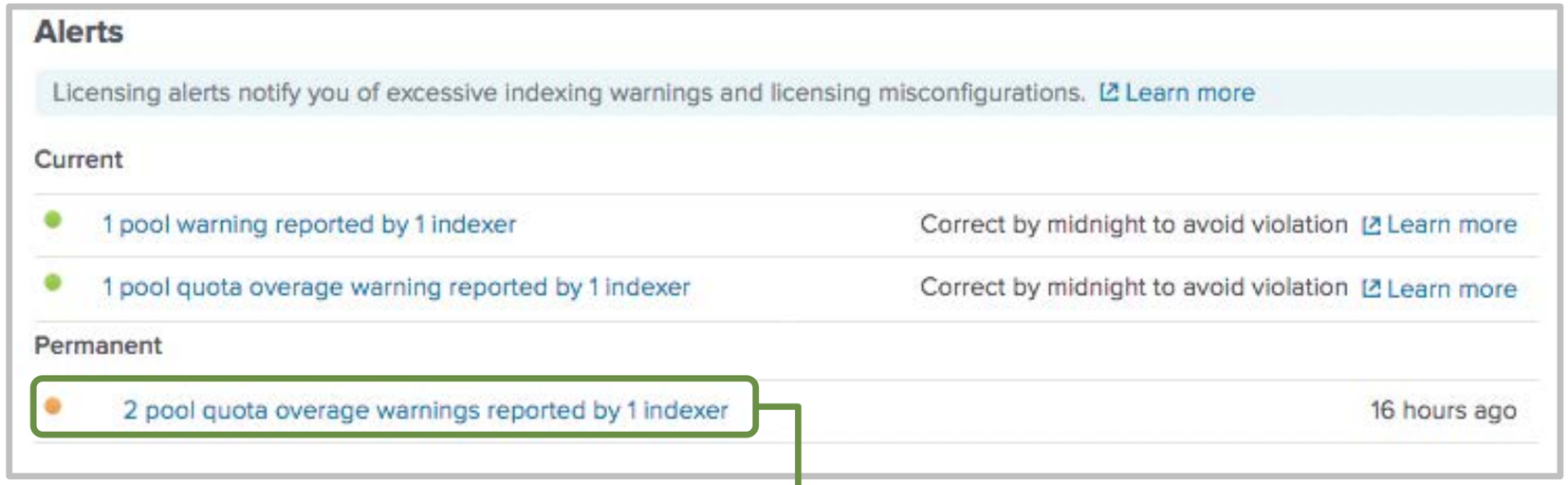
- Can use CLI or Splunk Web (upload or copy/paste)
  - License group change requires a restart
- Licenses are stored under **`SPLUNK_HOME/etc/licenses`**
- Multiple licenses of the same type are stacked (added together)

```
splunk add licenses <path_to_file>
```





Viewing Alerts



Pool quota overage alerts (3)

License alerts notify you of excessive indexing warnings and licensing misconfigurations. If you receive too many warnings, your indexer will be in violation of the license and you will not be able to search. Learn more

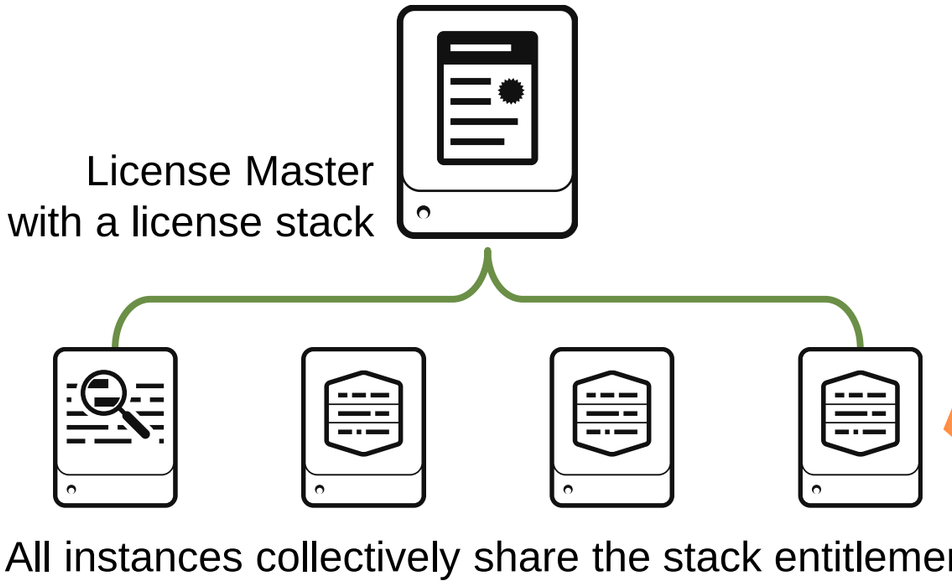
Severity	Time	Message	Indexer	Pool	Stack	Category
●	Correct by midnight to avoid violation Learn more	This pool is over poolsz=157286400 bytes, please correct before midnight		auto_generated_pool_enterprise	enterprise	pool_over_quota
●	Mar 30, 2018 12:00:00 AM (16 hours ago)	This pool has exceeded its configured poolsize=157286400 bytes. A warning has been recorded for all members	ip-10-0-0-203	auto_generated_pool_enterprise	enterprise	pool_over_quota
●	Mar 24, 2018 12:00:00 AM (6 days ago)	This pool has exceeded its configured poolsize=157286400 bytes. A warning has been recorded for all members	ip-10-0-0-203	auto_generated_pool_enterprise	enterprise	pool_over_quota

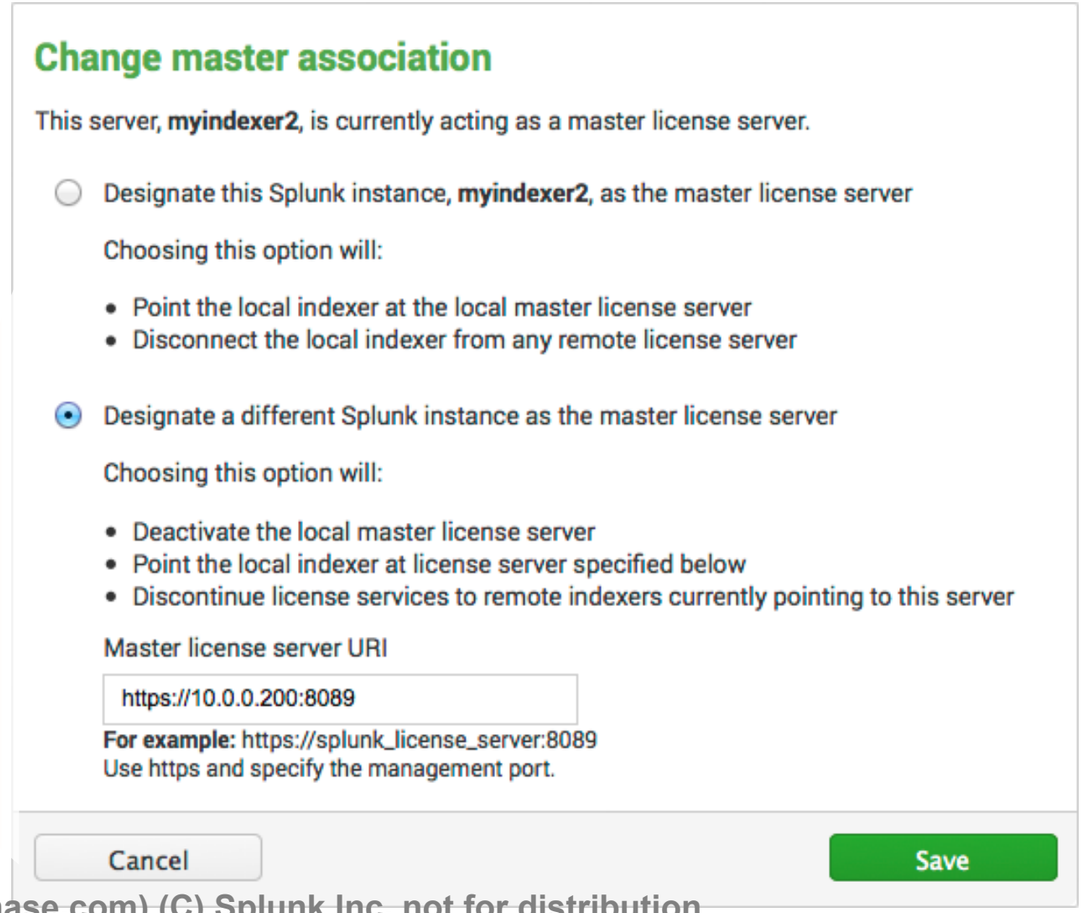
Show messages for all alert types

« return to overview

Change to Slave

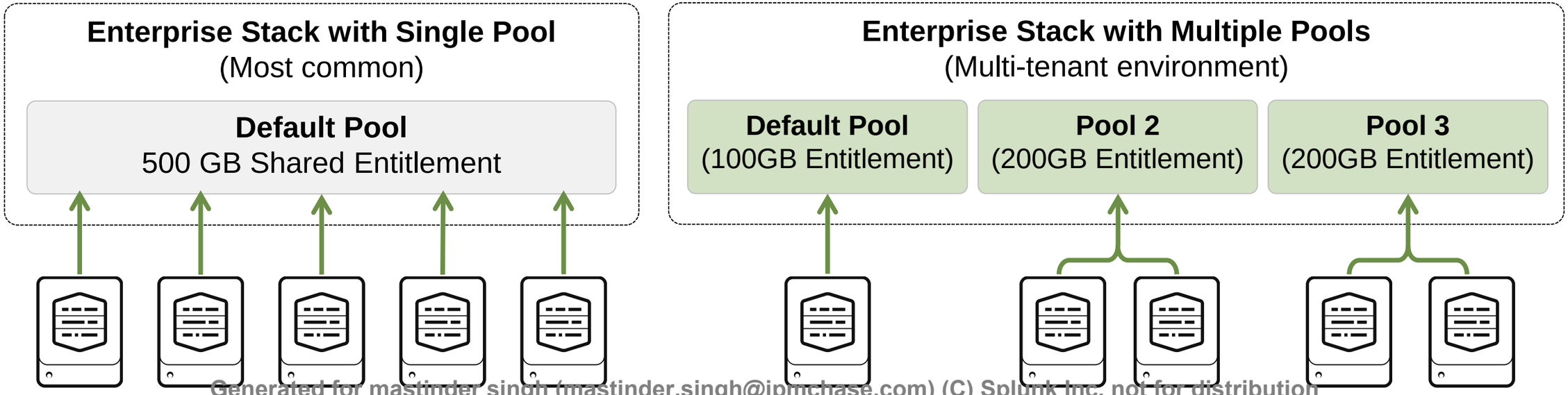
Change an instance to slave by entering the master license server URI





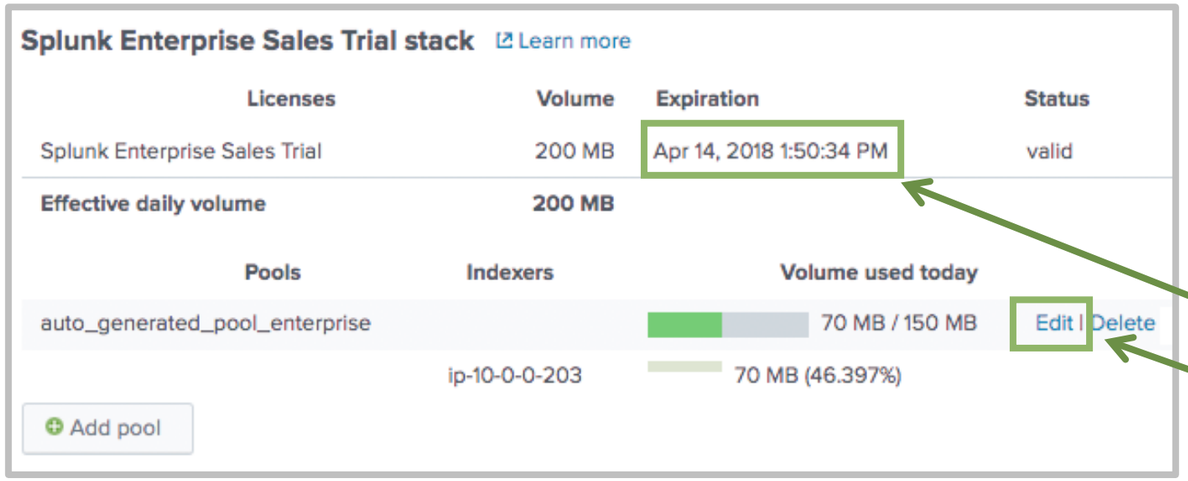
License Pooling

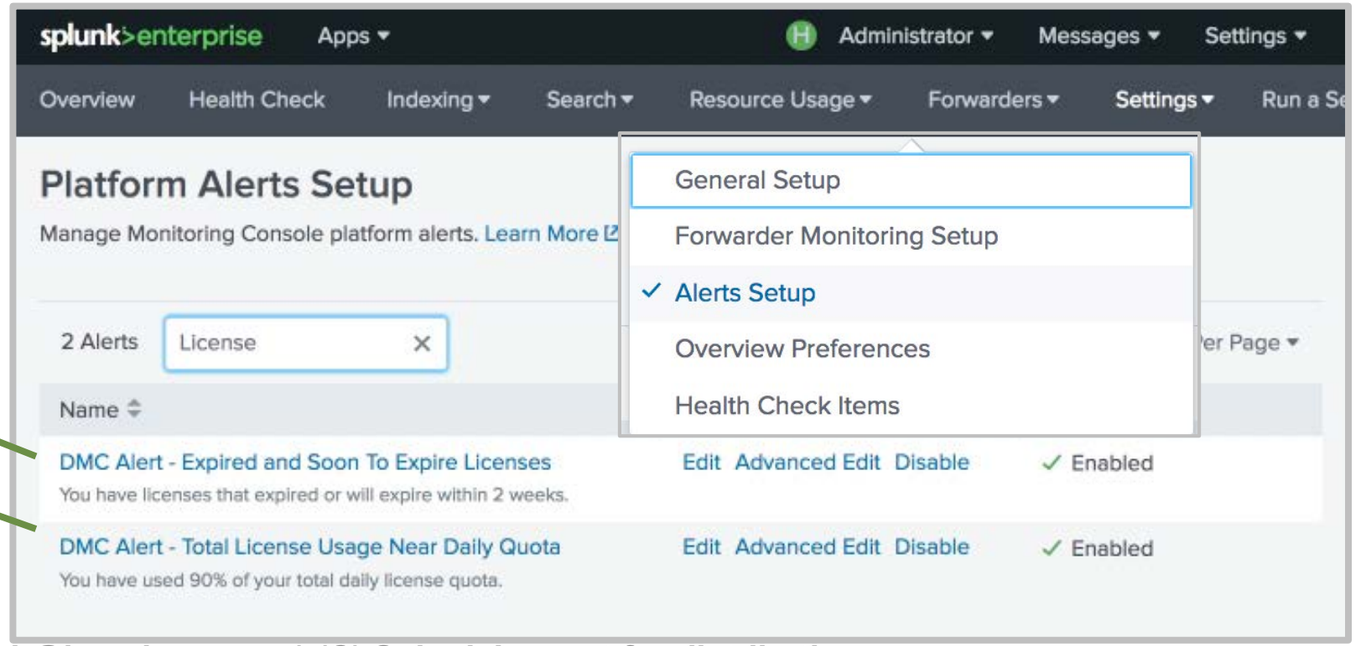
- **Pools** allow licenses to be subdivided and assigned to a group of indexers
  - Can be created for a given stack
  - Warnings and violations occur per pool
- Example: Master has a stack for a total of 500GB



Managing License Warnings

- DO NOT ignore license warnings
- Proactively monitor the consumption of your Splunk license
  - MC provides a couple of alerts
  - If possible, give yourself latitude by rearranging license pools





Lab Exercise 2 – Splunk License Management

Time: 10 minutes

Tasks:

- Add licenses
- Modify the license pool
- Enable MC Alert

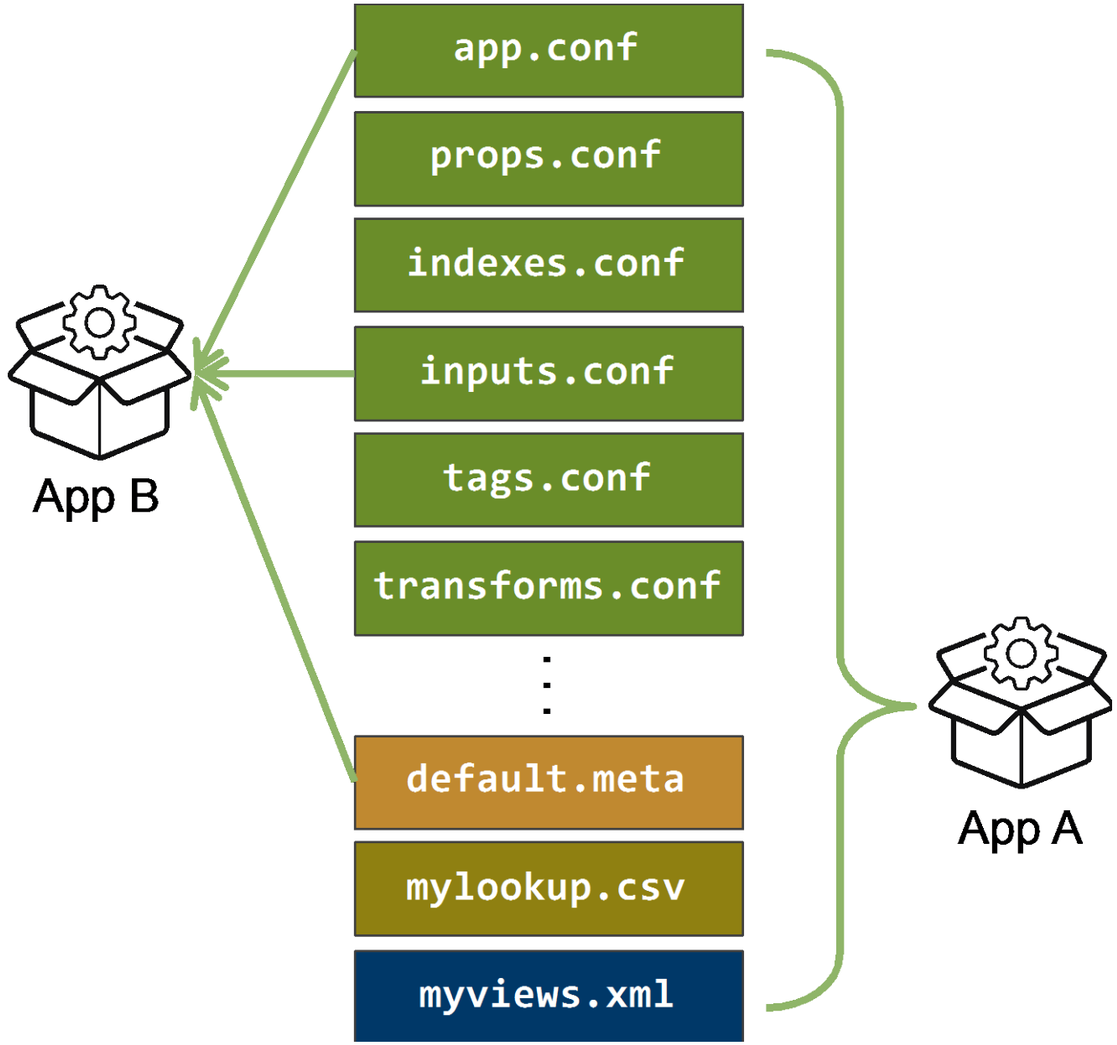
Module 3: Splunk Apps

Module Objectives

- Describe Splunk apps and add-ons
- Install an app on a Splunk instance
- Manage app accessibility and permissions

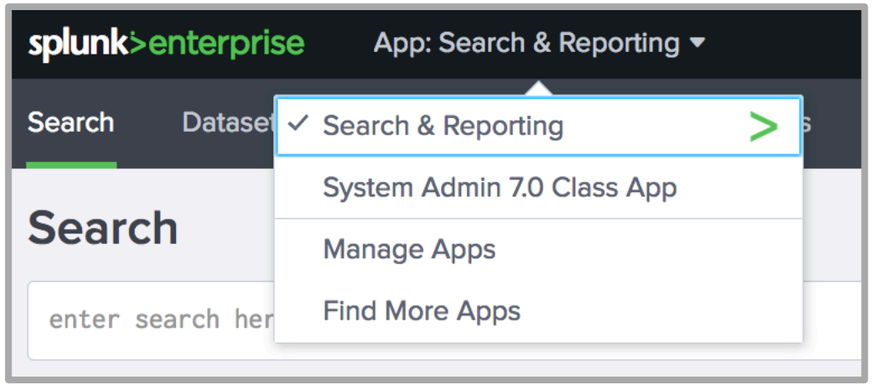
What is an App?

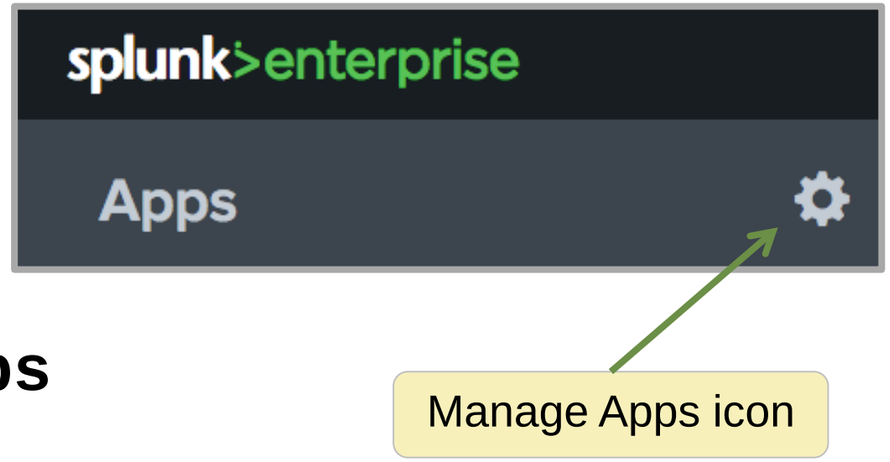
- An app is a collection of:
  - Configuration files
  - Scripts, web assets, etc.
- Most apps are focused on:
  - A specific type of data from a vendor, operating system, or industry
  - A specific business need
- Apps may be installed on any Splunk instance
- Splunk includes a number default apps



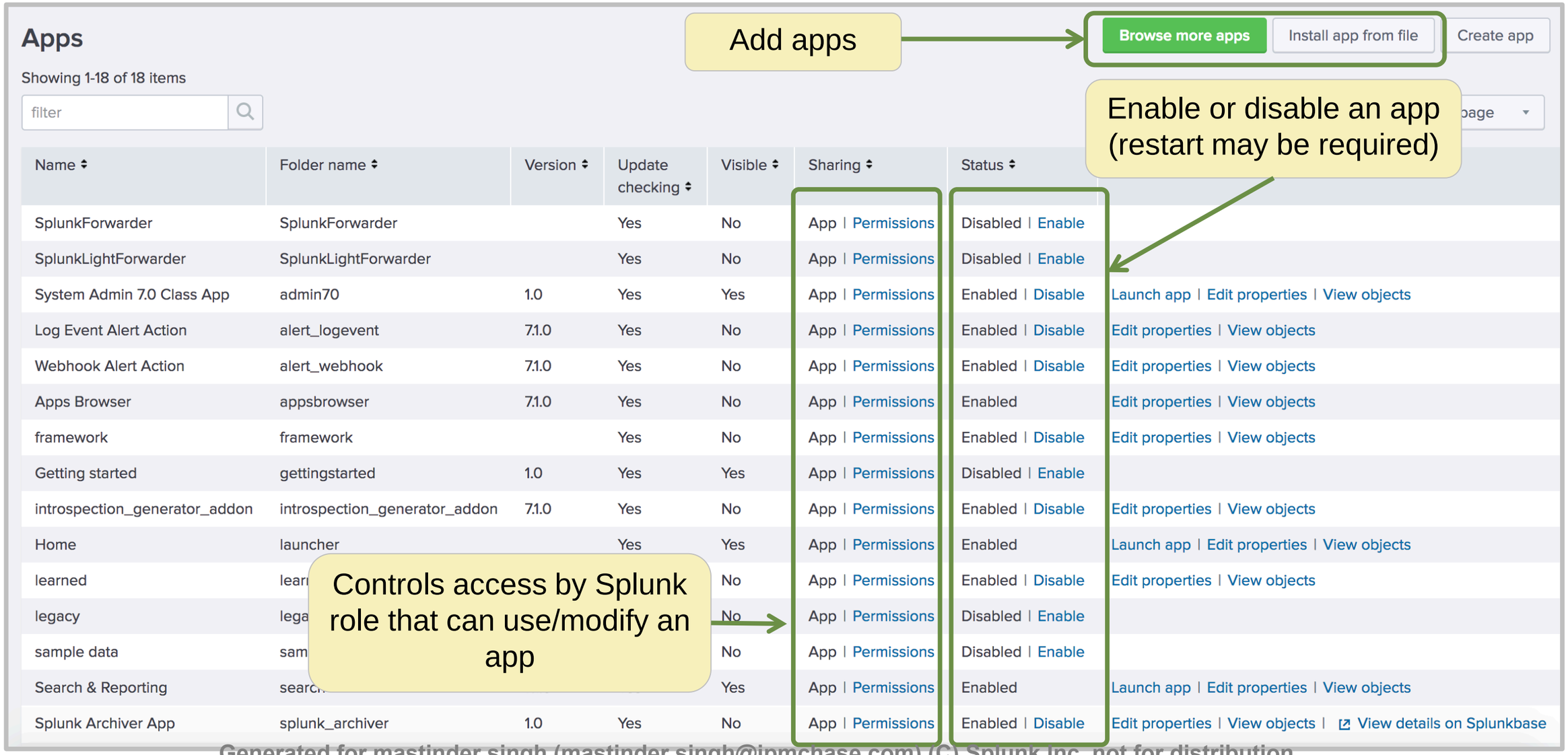
View All Installed Apps

- Within an app, use the dropdown menu and select **Apps: app name > Manage Apps**
- On the **Home** view (launcher app), click the Manage Apps icon
- Apps can be visible or hidden
  - Several apps are installed by default that are hidden or disabled
    - Internal apps used by Splunk should not be modified
    - Legacy apps
    - Sample apps
- Apps are installed under **`SPLUNK_HOME/etc/apps`**





Managing Apps



Apps

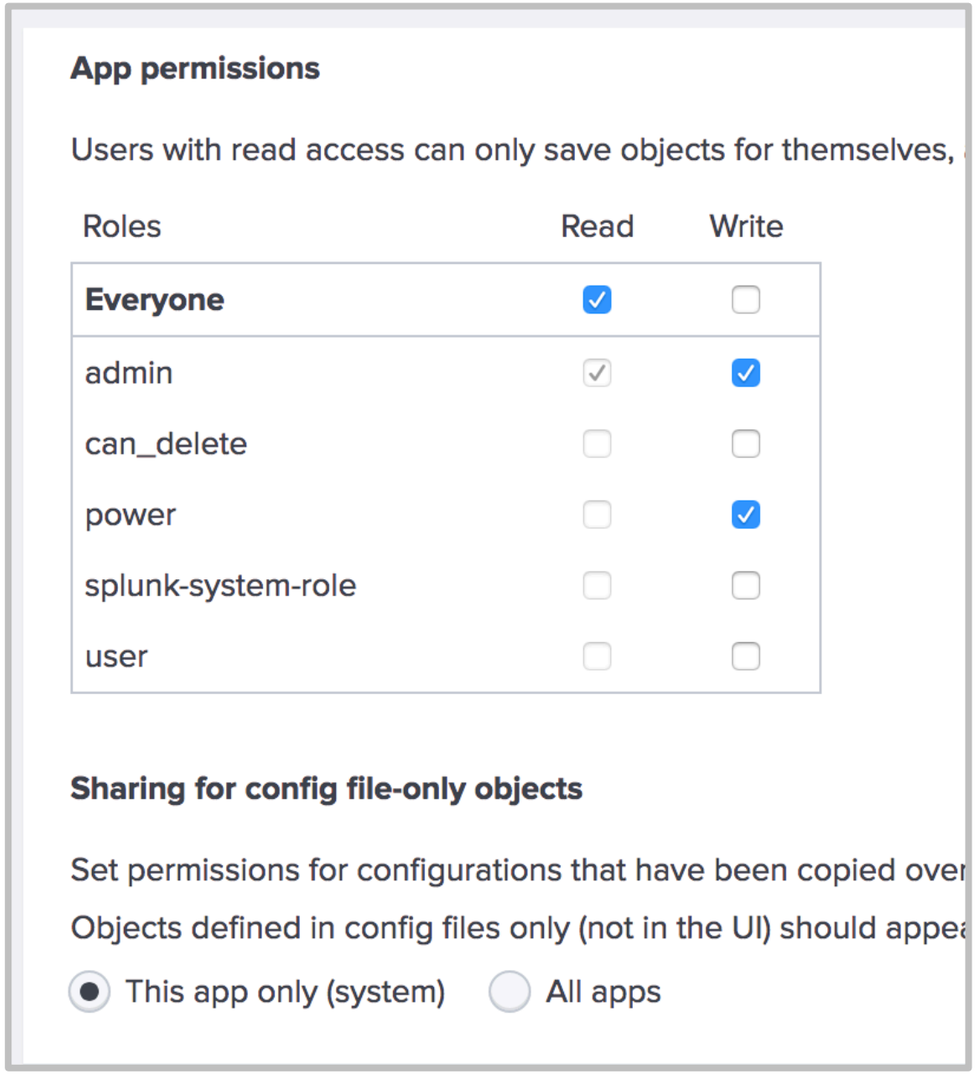
Showing 1-18 of 18 items

filter

Name	Folder name	Version	Update checking	Visible	Sharing	Status	
SplunkForwarder	SplunkForwarder		Yes	No	App | Permissions	Disabled | Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App | Permissions	Disabled | Enable	
System Admin 7.0 Class App	admin70	1.0	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit properties | View objects
Log Event Alert Action	alert_logevent	7.1.0	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Webhook Alert Action	alert_webhook	7.1.0	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Apps Browser	appsbrowser	7.1.0	Yes	No	App | Permissions	Enabled	Edit properties | View objects
framework	framework		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Getting started	gettingstarted	1.0	Yes	Yes	App | Permissions	Disabled | Enable	
introspection_generator_addon	introspection_generator_addon	7.1.0	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects
Home	launcher		Yes	Yes	App | Permissions	Enabled	Launch app | Edit properties | View objects
learned	learn			No	App | Permissions	Enabled | Disable	Edit properties | View objects
legacy	lega			No	App | Permissions	Disabled | Enable	
sample data	sam			No	App | Permissions	Disabled | Enable	
Search & Reporting	search			Yes	App | Permissions	Enabled	Launch app | Edit properties | View objects
Splunk Archiver App	splunk_archiver	1.0	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objects | View details on Splunkbase

App Permissions

- A user's role with **read** permission can see the app and use it
- A user's role with **write** permission can add/delete/modify knowledge objects used in the app
  - By default, the **user** role does not have write permissions within the **search** app



Installing an App from Splunkbase

- From the **Apps** page, click **Browse more apps**
- Or, click **Apps > Find More Apps**
  - Splunk Web will access **splunkbase.splunk.com**
  - Search for the app you want to install
  - Select **Install** (most apps are free)
    - You must provide your **splunk.com** user ID and password
    - The app is installed into a sub-directory below **`SPLUNK_HOME/etc/apps`**
    - Some apps require a restart
- Or, go directly to **splunkbase.splunk.com** and download the app as a file to your local computer

Note

Anyone can sign up for a user account in Splunk.com.

A support contract is not required.

Installing an App From a File

- Download the app from splunkbase
  - The file format may be: **`.tar.gz`**, **`.tgz`**, **`.zip`**, or **`.spl`** file
- Install the app:
  - From Splunk Web, click **Install app from file**
  - Or, use CLI
    `splunk install app` ***`path-to-appfile`***
  - Or extract the app in the proper location
    `cd SPLUNK_HOME/etc/apps`
    `tar –xf` ***`path-to-appfile`***
- Apps may require a splunkd restart
- Configure the app according to its documentation

Apps on Forwarders?

- Universal forwarders don't have a web interface, but they can still benefit from an app
- An add-on is a subset of an app
  - Usually contains data collection but no GUI components (reports or dashboards)
- To install an add-on or app on a forwarder
  - Install the app using the CLI on the forwarder
  - Or, use a deployment server to deploy the app

Deleting an App

- When you delete an app, all of its related configuration files and scripts are deleted from a Splunk server
  - User's private app artifacts remain untouched
- To delete an app:
  - **`splunk remove app <app_folder>`**
  - Or, navigate to **`SPLUNK_HOME/etc/apps`** and delete the app's folder and all its contents
  - Restart the Splunk server
- It can be reinstalled later
- Safer to disable it or move the app's files to another location

Lab Exercise 3 – Install an App

- **Time:** 10 minutes
- **Tasks:**
- Download an app
- Install the app
- Change the app’s permissions
- Verify if the app's dashboard displays reports

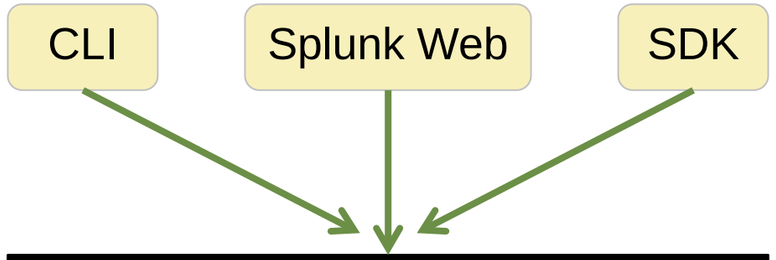
Module 4: Splunk Configuration Files

Module Objectives

- Describe Splunk configuration directory structure
- Understand configuration layering process
  - Index-time process
  - Search-time process
- Use `btool` to examine configuration settings

Splunk Configuration Files

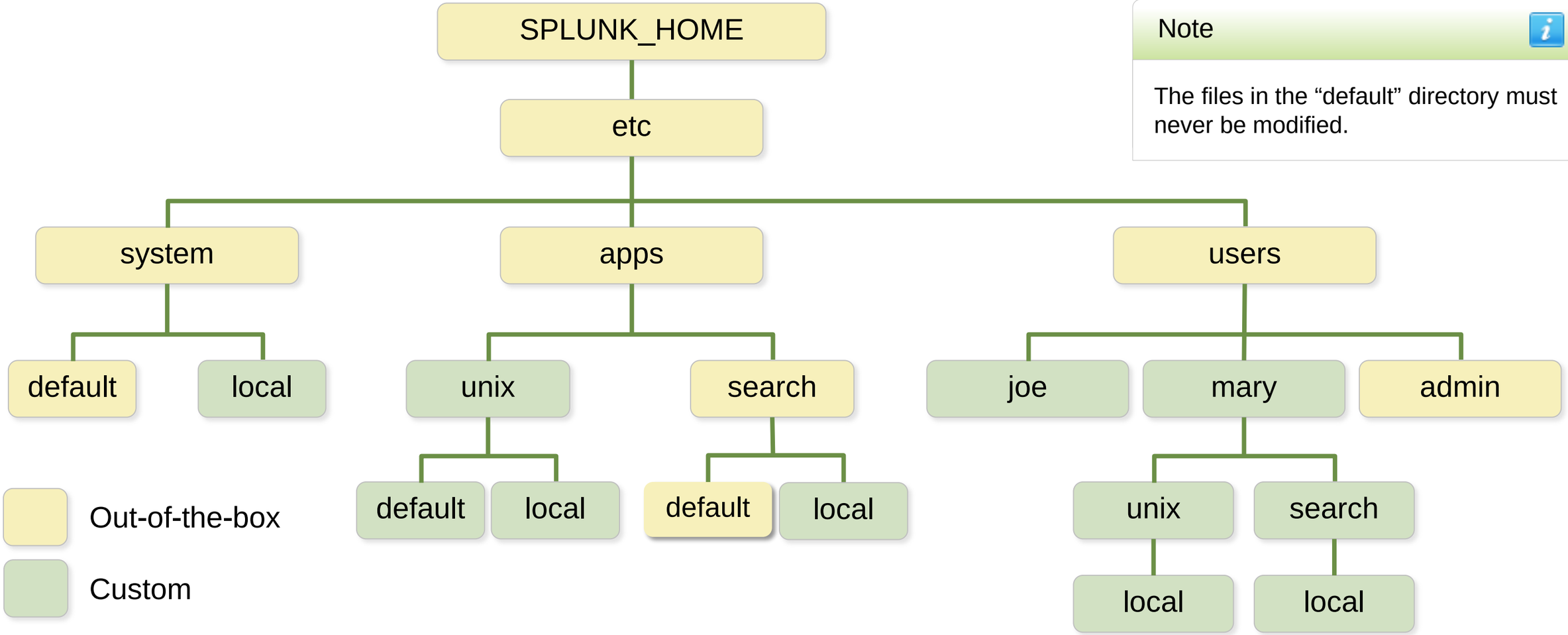
- Each configuration file governs a particular aspect of Splunk functionality
- Configuration changes are saved in **.conf** files under **SPLUNK_HOME/etc/**
  - **.conf** files are text files using a stanza and name/value (attribute) format
  - The syntax is case-sensitive
- You can change settings using Splunk Web, CLI, SDK, app install, and/or direct edit
- All **.conf** files have documentation and examples:
  - **SPLUNK_HOME/etc/system/README**
    - ***.conf.spec**
    - ***.conf.example**
    - Splunk documentation: docs.splunk.com




```
[default]
host=www

[monitor:///var/log/httpd]
sourcetype = access_common
ignoreOlderThan = 7d
index = web
```

inputs.conf

Configuration Directories



Note

The files in the “default” directory must never be modified.

http://docs.splunk.com/Documentation/Splunk/latest/Admin/Listofconfigurationfiles

Default vs. Local Configuration

- Splunk ships with default **`.conf`** files
  - Stored in the **`default`** directories
- Only modify configurations to files in a **`local`** directory
- Avoid storing configurations in **`SPLUNK_HOME/etc/system`**
  - Manage your configurations in the **Searching and Reporting** app's local directory (**`SPLUNK_HOME/etc/apps/search/local`**) unless the configuration is only for a specific app

Shipped with Splunk or the app
- Overwritten on update
- Do **not** modify

Your specific configuration changes
- Preserved on update

Index Time vs. Search Time

Index time	Global context	User-independent and background tasks such as inputs, parsing, indexing, etc.
Search time	App/User context	User-related activity, such as searching

- The priority of layered configurations are based on the context

  For example:

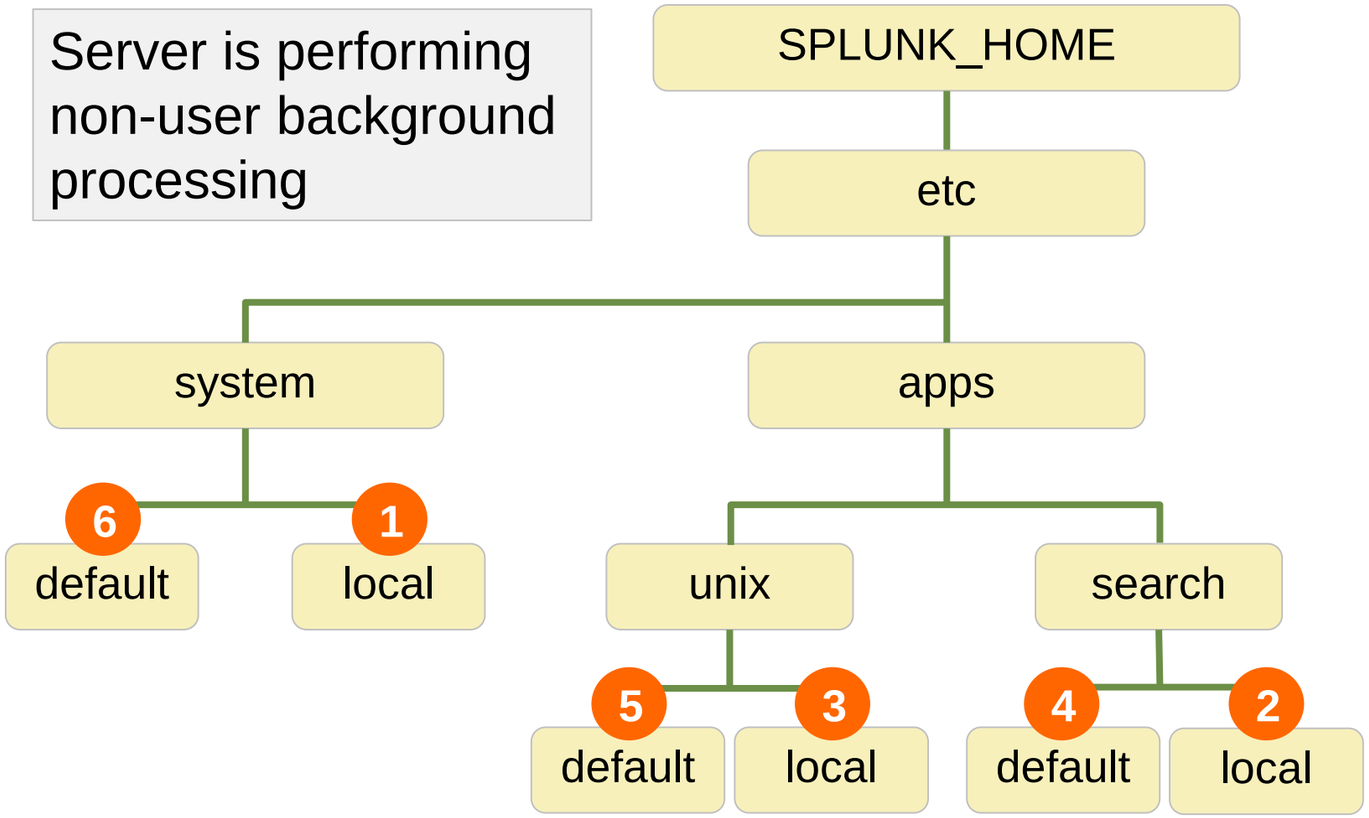
  - **Global context**: a network input to collect syslog data
  - **App/User context**: Mary's private report in the Search app

- For a list of configuration files and their context, go to:

  docs.splunk.com/Documentation/Splunk/latest/Admin/Wheretofindtheconfigurationfiles

Index Time Precedence Order

Server is performing non-user background processing



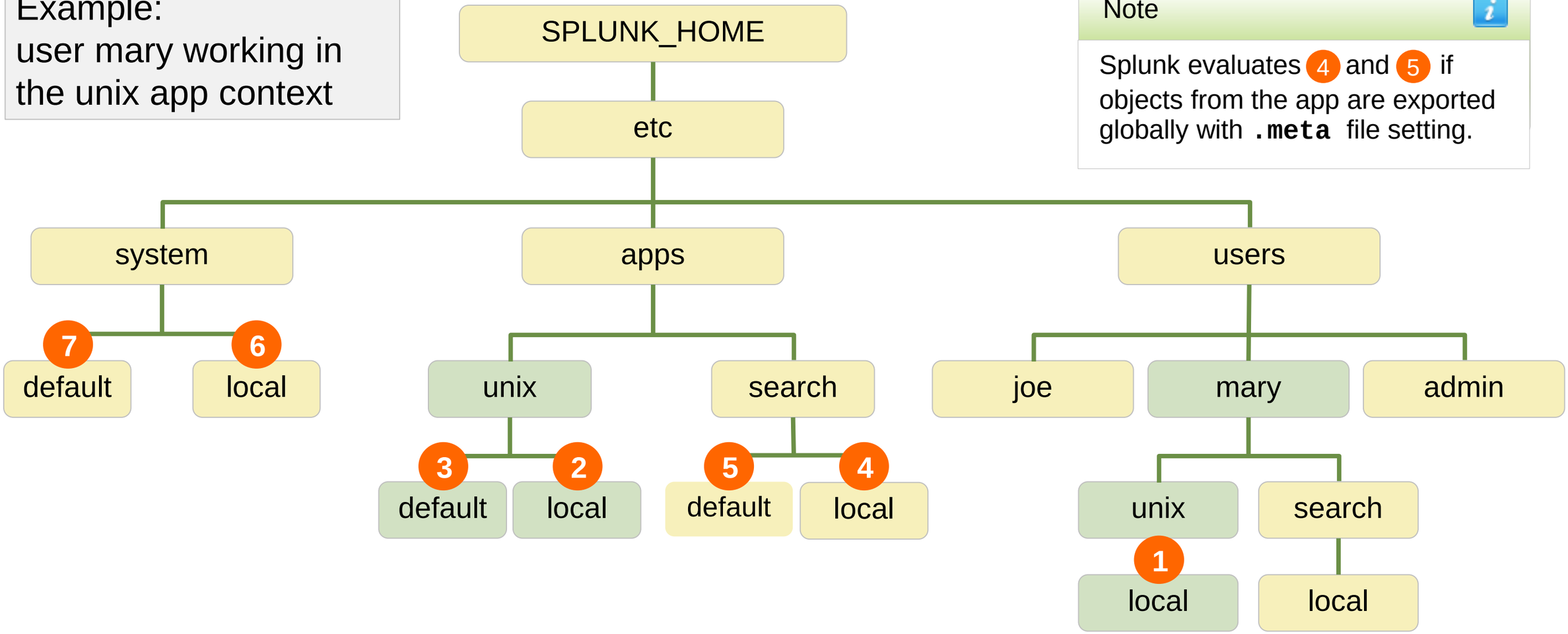
1. etc/system/local
2. etc/apps/search/local
3. etc/apps/unix/local
4. etc/apps/search/default
5. etc/apps/unix/default
6. etc/system/default

Note

If two or more apps at the same level of precedence have conflicts between them, the conflicts are resolved in ASCII order by app directory name.

Search Time Precedence Order

Example:
user mary working in the unix app context



Note

Splunk evaluates 4 and 5 if objects from the app are exported globally with `.meta` file setting.

Index Time Merging of Configurations

- When Splunk starts, configuration files are merged together into a single run-time model for each file type
  - Regardless of the number of **`inputs.conf`** files in various apps or the system path, only one master inputs configuration model exists in memory at runtime
- If there are no duplicate stanzas or common settings between the files, the result is the union of all files
- If there are conflicts, the setting with the highest precedence is used
  - Remember that **`local`** always takes precedence over **`default`**

Example of Merging (No Conflict)

SPLUNK_HOME/etc/system/local/example.conf

```
[a]
x=1
y=2

[b]
j=1
k=2
```

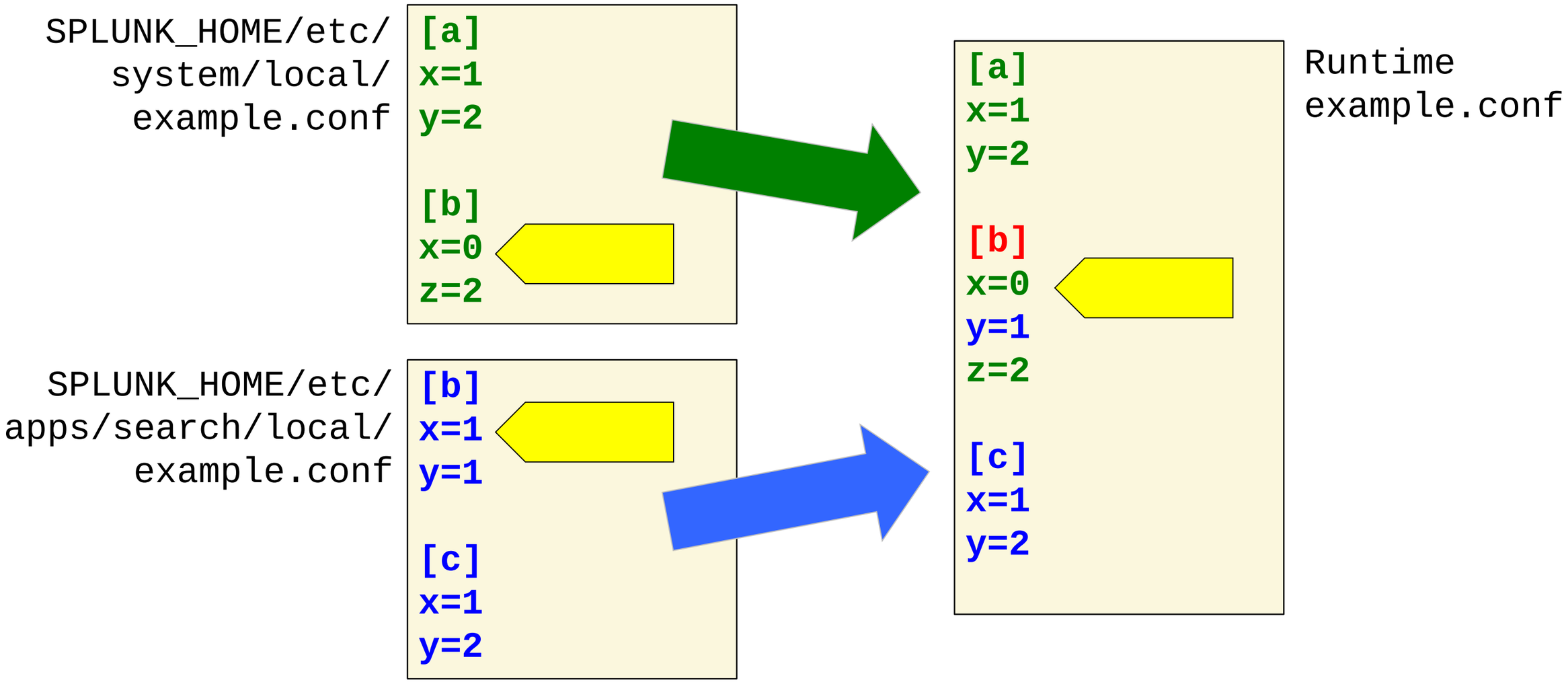
SPLUNK_HOME/etc/apps/search/local/example.conf

```
[b]
p=1
q=1

[c]
s=1
t=2
```

Runtime example.conf

```
[a]
x=1
y=2

[b]
j=1
k=2
p=1
q=1

[c]
s=1
t=2
```

Example of Merging (Conflict)



Configuration Validation Command - **btool**

- **splunk btool** *conf-name* **list** [*options*]
  - Shows on-disk configuration for requested file
  - Run **splunk btool check** each time Splunk starts
  - Useful for checking the configuration scope and permission rules
    - Use **--debug** to display the exact **.conf** file location
    - Add **--user= <*user*> --app=<*app*>** to see the user/app context layering
- Examples:
  - **splunk help btool**
  - **splunk btool check**
  - **splunk btool inputs list**
  - **splunk btool inputs list monitor:///var/log**
  - **splunk btool inputs list monitor:///var/log --debug**

docs.splunk.com/Documentation/Splunk/latest/Troubleshooting/Usebtooltotroubleshootconfigurations

`btool` Example

Scenario: What are the **`/var/log/secure.log`** input configurations and where are they specified?

```
> splunk btool inputs list monitor:///var/log/secure.log --debug

  etc/apps/search/local/inputs.conf     [monitor:///var/log/secure.log]
  etc/system/local/inputs.conf          host = myIndexer
  etc/system/default/inputs.conf        index = default
  etc/apps/search/local/inputs.conf     sourcetype = linux_secure
```

`etc/system/local/inputs.conf`

```
[monitor:///var/log/secure.log]
host=myIndexer
```

`etc/apps/search/local/inputs.conf`

```
[monitor:///var/log/secure.log]
sourcetype=linux_secure
host=webserver
```

Overriding Defaults

- There are default settings in **SPLUNK_HOME/etc/system/default** and **SPLUNK_HOME/etc/apps/search/default**
- The correct method to override these settings is to do so in the **local** directory at the same scope
  - Only add the items you are overriding — do not make a copy of the entire configuration file
- Example:
  - To disable a default attribute **TRANSFORMS for [syslog]:**

```
# etc/system/default/props.conf
[syslog]
TRANSFORMS = syslog-host
REPORT-syslog = syslog-extractions
...
```

```
# etc/system/local/props.conf
[syslog]
TRANSFORMS =
```

Reloading Configuration Files After Edit

- Changes made using Splunk Web or the CLI may not require restart
  - A message appears if restart is required (i.e. changing server settings)
- Changes made by editing **`.conf`** files are not automatically detected
- To force reload, go to **http://servername:webport/debug/refresh**
  - Reloads many of the configurations, including `inputs.conf`, but not all
- To reload all configurations, restart Splunk
  - Splunk Web: **Settings** > **Server controls** > **Restart Splunk**
  - CLI: **`splunk restart`**

Lab Exercise 4 – Examine User Configuration Files

- **Time**: 25 – 30 minutes
- **Tasks**:
- Run the same search as different users
- Check the search results and compare
- Use the **btool** command to investigate configurations

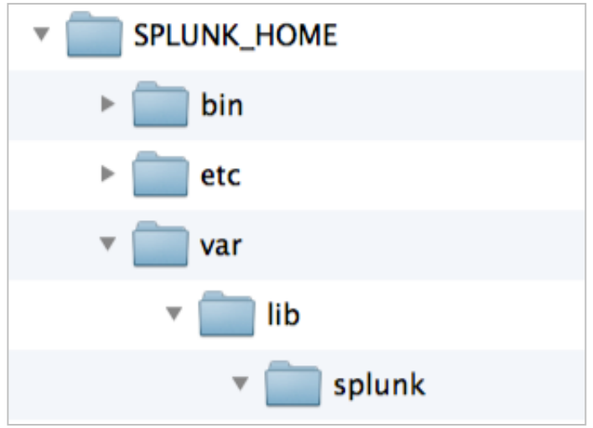
Module 5: Splunk Indexes

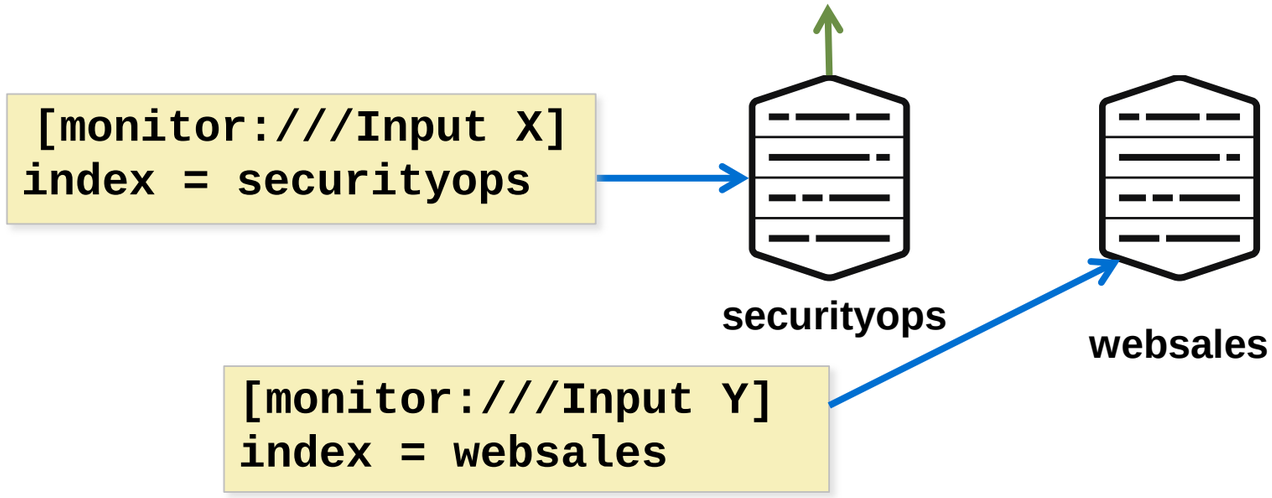
Module Objectives

- Learn how Splunk indexes function
- Understand the types of index buckets
- Create new indexes
- Explain the advantages of using multiple indexes
- Monitor indexes with MC

What are Indexes?

- Splunk stores the input data as events in indexes
  - **SPLUNK_HOME/var/lib/splunk**
  - Set in **Settings > Server Settings > General Settings**
  - Can override on a per-index basis
- The System Admin can:
  - Create new indexes
  - Control which indexes users can access
- Splunk users can specify the index to search
- Splunk ships with some indexes already installed





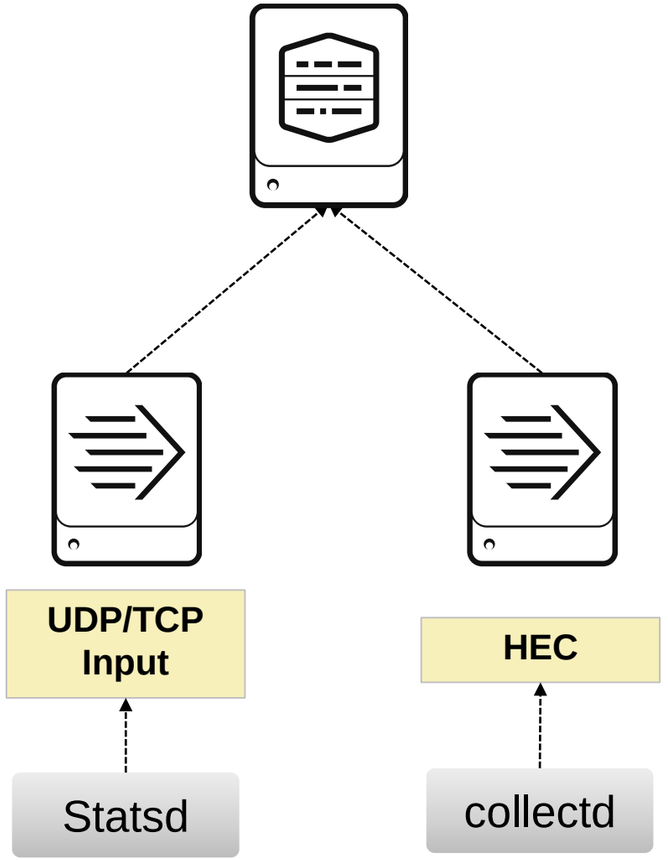
Preconfigured Indexes

Splunk ships with several indexes preconfigured

- **_internal** – Splunk indexes its own logs and metrics from its processing here
- **_audit** – Splunk stores its audit trails and other optional auditing information
- **_introspection** – tracks system performance and Splunk resource usage data
- **_thefishbucket** – contains checkpoint information for file monitoring inputs
- **summary** – default index for summary indexing system
- **main** – default index for inputs, located in the **`defaultdb`** directory

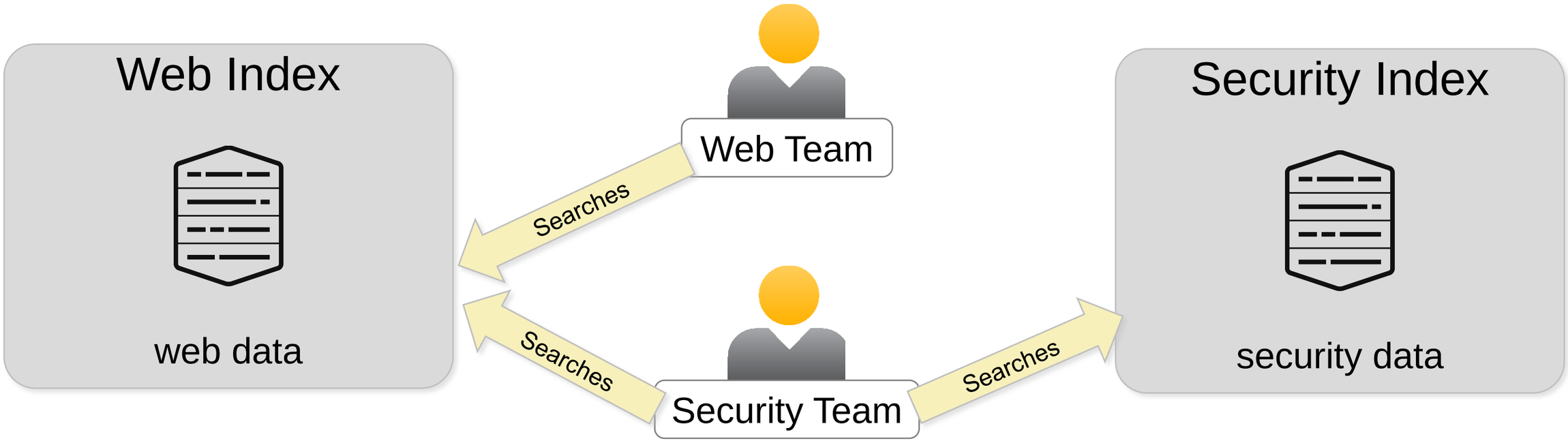
Metrics Indexing

- Starting with 7.0, Splunk supports metrics indexes
  - Special index format for metrics and certain types of log collection
- Supports the following protocols
  - The StatsD extension over UDP/TCP
  - Plain StatsD extension with dimensions over UDP/TCP
  - Collectd over HTTPs using HTTP Event Collector (HEC)
- Event-based indexes are not the same as metrics-based indexes
  - An event index cannot be converted into a metrics index (or vice-versa)



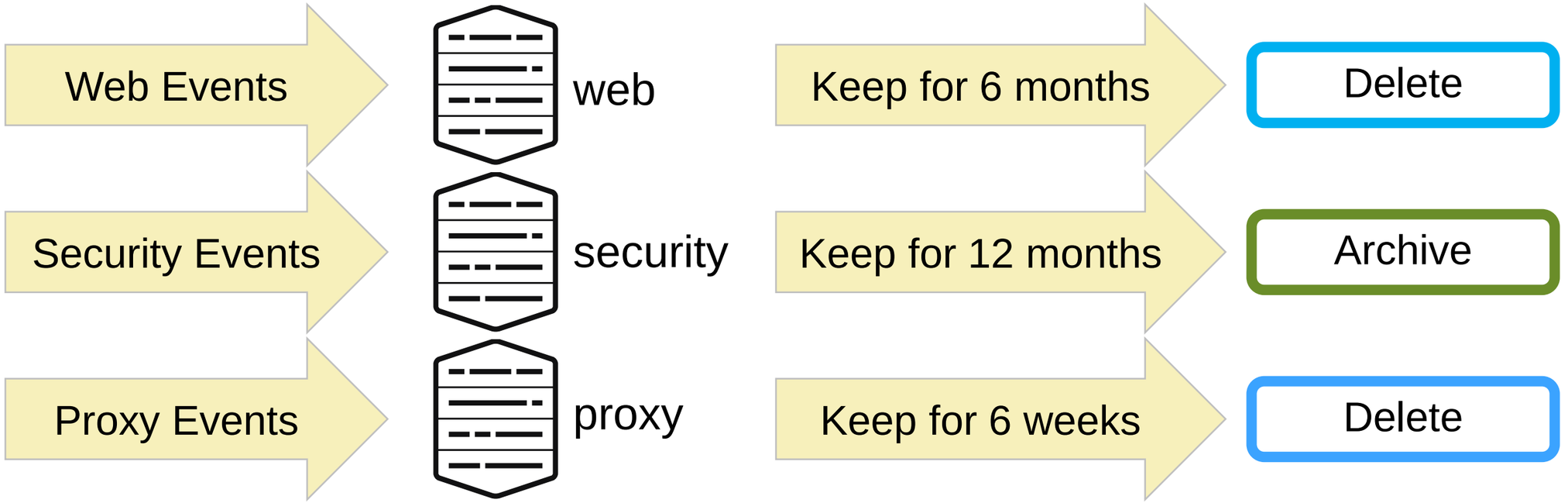
Why Create Indexes?

Access control – segregate events into separate indexes to limit access by Splunk role



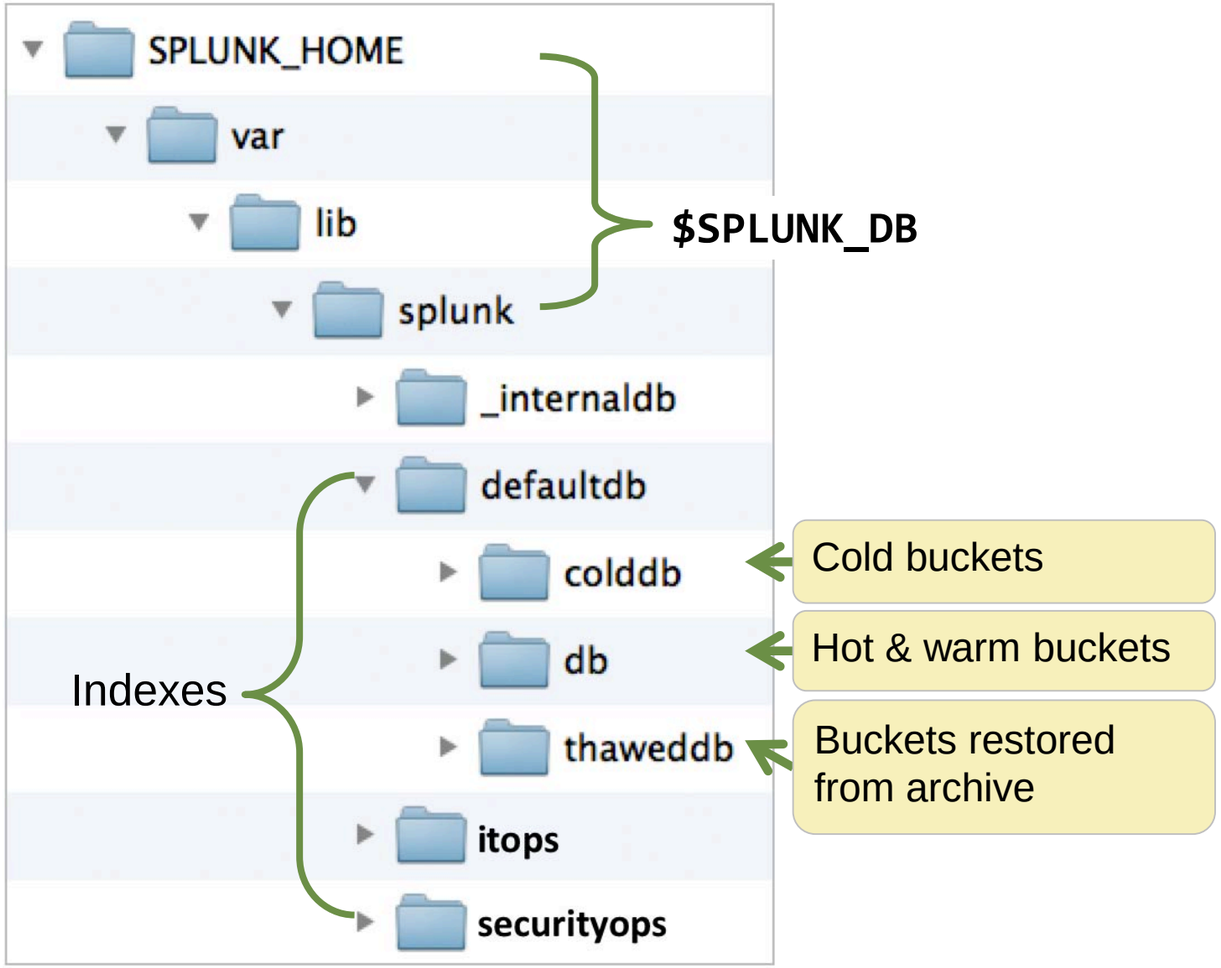
Why Create Indexes? (cont.)

- Retention
  - Policy is set per index
  - Separate events into different indexes based on desired retention time



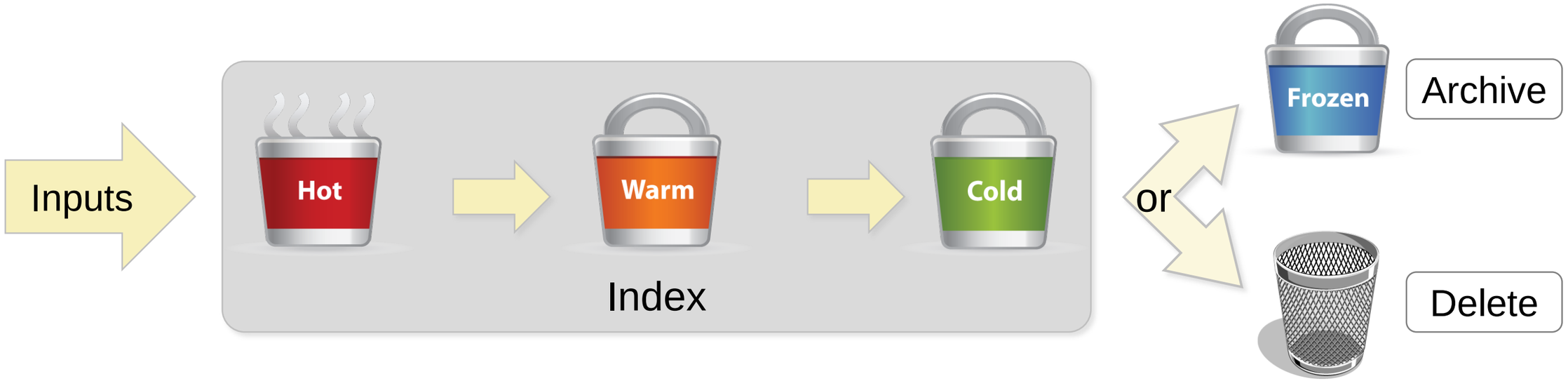
Buckets

- An index stores events in buckets
- A bucket is a directory containing a set of rawdata and indexing data
- Buckets have a maximum data size and a time span
  - Both can be configured



wiki.splunk.com/Deploy:UnderstandingBuckets

Data Flow Through an Index



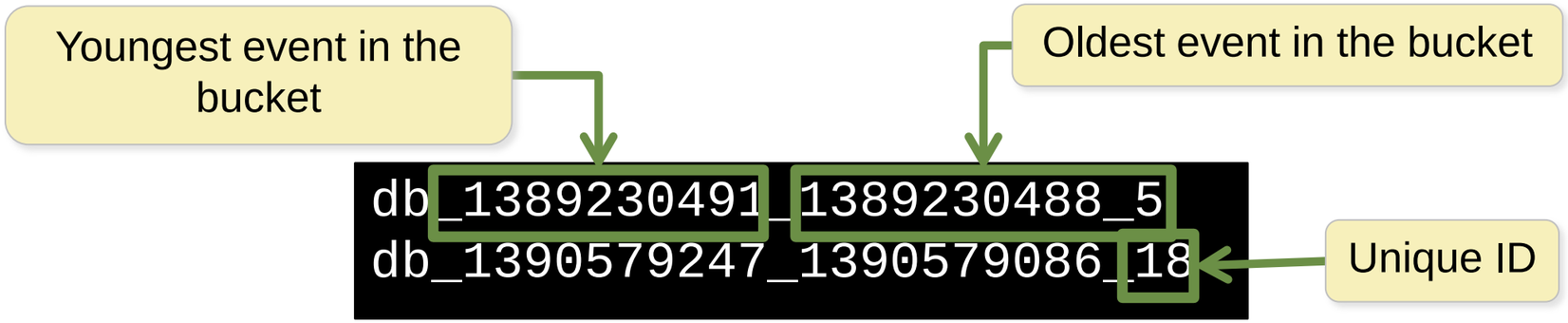
- **Hot**: Newest buckets – open for writes (readable)
- **Warm**: Recent data, buckets are closed (read only)
- **Cold**: Oldest data still in the index (read only)
- **Frozen**: Deletion is the default action. If a frozen path is defined, then the bucket's raw data is archived – not searchable

Hot Buckets

- After data is read and parsed, it goes through the license meter and the resulting event is written into a hot bucket
- When hot buckets reach their max size or time span, they are closed and converted to warm status
  - Hot buckets also roll to warm automatically when the indexer is restarted or 24 hours with no events written
  - Hot and warm buckets are stored in the **db** directory for the index
  - Hot buckets are renamed when rolled to warm

Warm and Cold Bucket Names

- Warm bucket names identify the time range of the events contained in that bucket
- When a warm bucket rolls to cold, the entire bucket is moved, maintaining its name
- At search time, Splunk scans the time range on a bucket name to determine whether or not to open the bucket and search its events



Note

When clustering is used, index replication adds further identifiers to the bucket name.

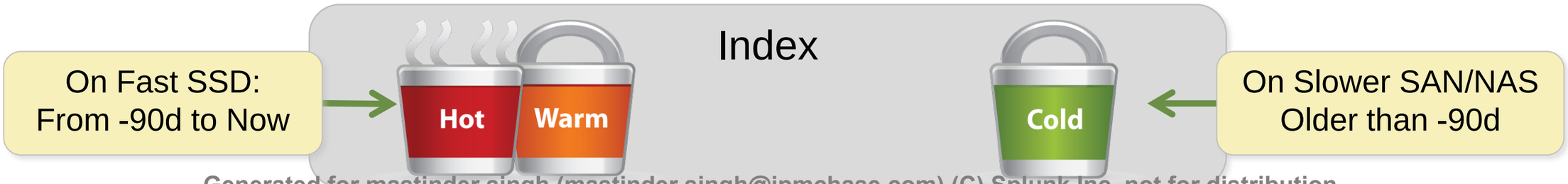
Freezing: Data Expiration

- The oldest bucket is deleted from an index when:
  - The index's maximum size is reached
  - The bucket's age exceeds the retention time limit
    - All the events in the bucket have expired
- Splunk will never exceed the maximum overall size of an index
  - Buckets may be deleted even if they have not reached the time limit
- You can optionally configure the frozen path
  - Splunk moves the bucket's raw data to this location before deletion
  - Frozen buckets are not searchable
- Frozen data can be brought back (thawed) into Splunk if needed

Buckets on Different Storage Systems

- **Best Practice:** Use a high performance file system to store indexes
  - The bucket time span and storage type can affect search performance
- You can use multiple storage systems for buckets
  - Specify separate volumes for hot/warm and cold buckets during index creation
  - Hot and warm buckets should be on the fastest storage
  - Cold buckets can be located on a slower, less expensive storage (or SAN/NAS)

wiki.splunk.com/Deploy:BucketRotationAndRetention



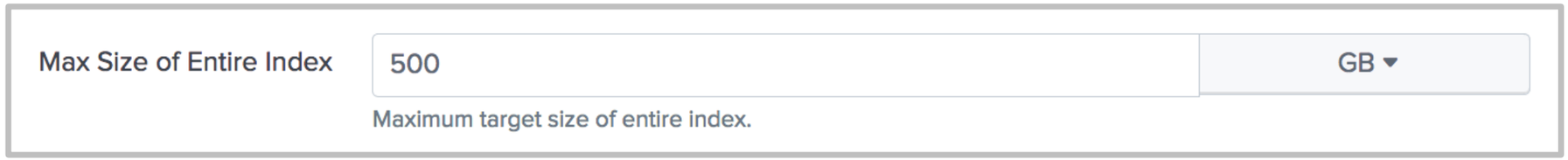
Estimating Index Growth Rate

- Splunk compresses the event's raw data as it is indexed
  - Indexing components are added to each bucket
    - If events have many searchable terms, the index components are larger
    - If the data contains fewer searchable terms and less variety, the index is smaller
- **Best practice**: get a good growth estimate
  - Input your data in a test/dev environment over a sample period
    - If possible, index more than one bucket of events
  - Examine the size of the index's **db** directory compared to the input
    - MC: **Indexing > Indexes and Volumes > Index Detail: Instance**

http://docs.splunk.com/Documentation/Splunk/latest/Capacity/Estimateyourstoragerequirements

Calculating Index Storage

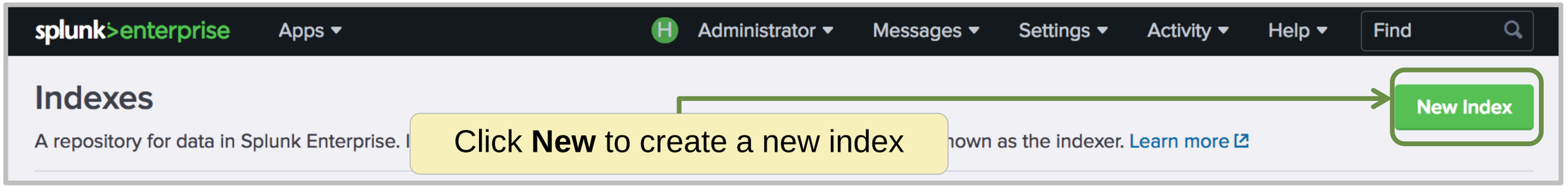
- Limiting size on disk is the most common method of controlling index growth



- Allocate disk space to meet data retention needs
  - Daily Rate * Compression Factor * Retention Period (in days) + Padding
- Example: **5** GB/day of security data searchable for **6** months (with compression factor of **.5**)
  - **900** GB (5 GB x 180 days) * **.5** (CF) + **50** GB (padding) = **500** GB
  - On average, data moves to frozen in this index after ~6 months

Adding an Index

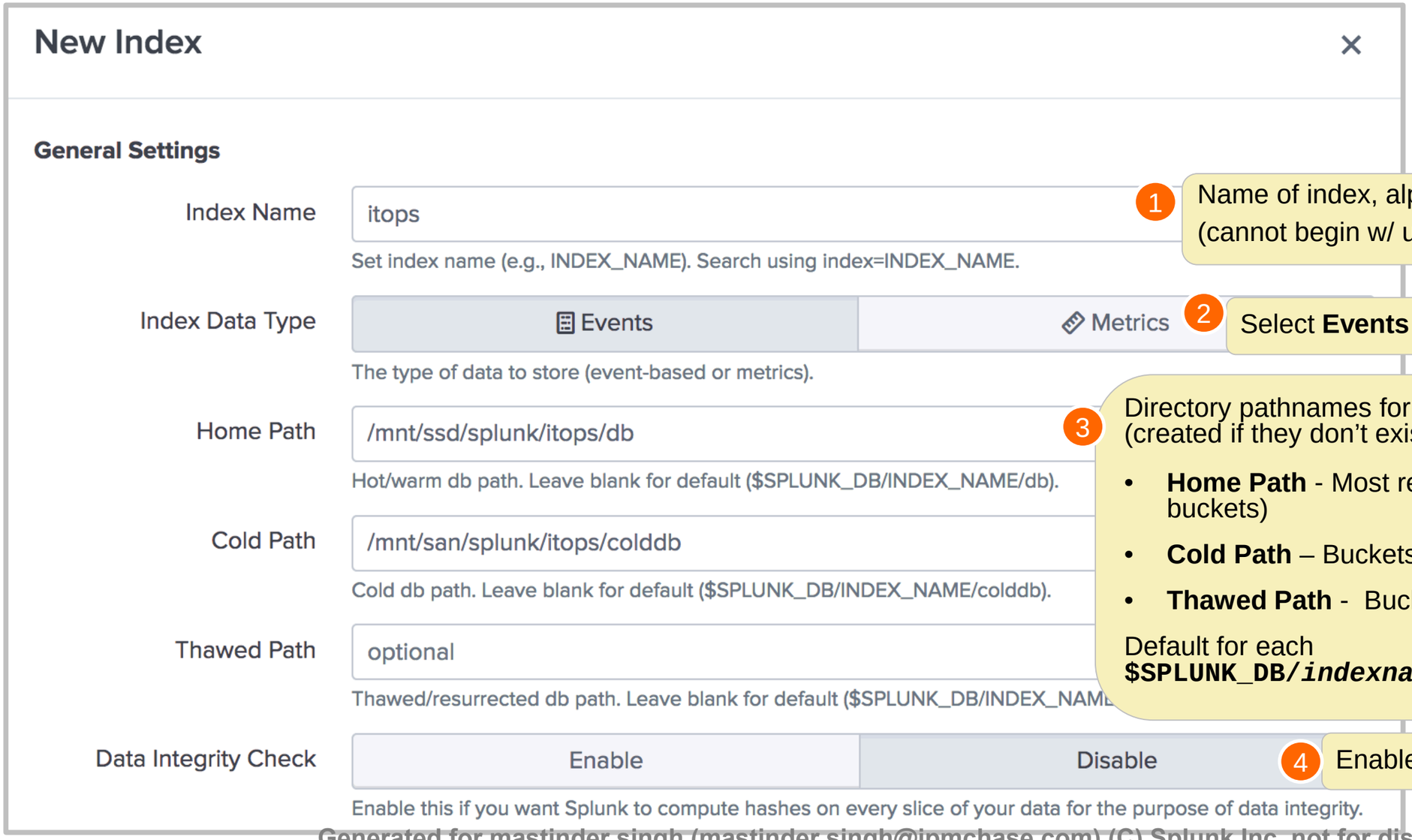
- Splunk Admins can create indexes from Splunk Web or CLI
  - Splunk Web
    - **Settings > Indexes > New Index**



  - CLI
    - **`splunk add index <index_name>`**

http://docs.splunk.com/Documentation/Splunk/latest/Indexer/Setupmultipleindexes

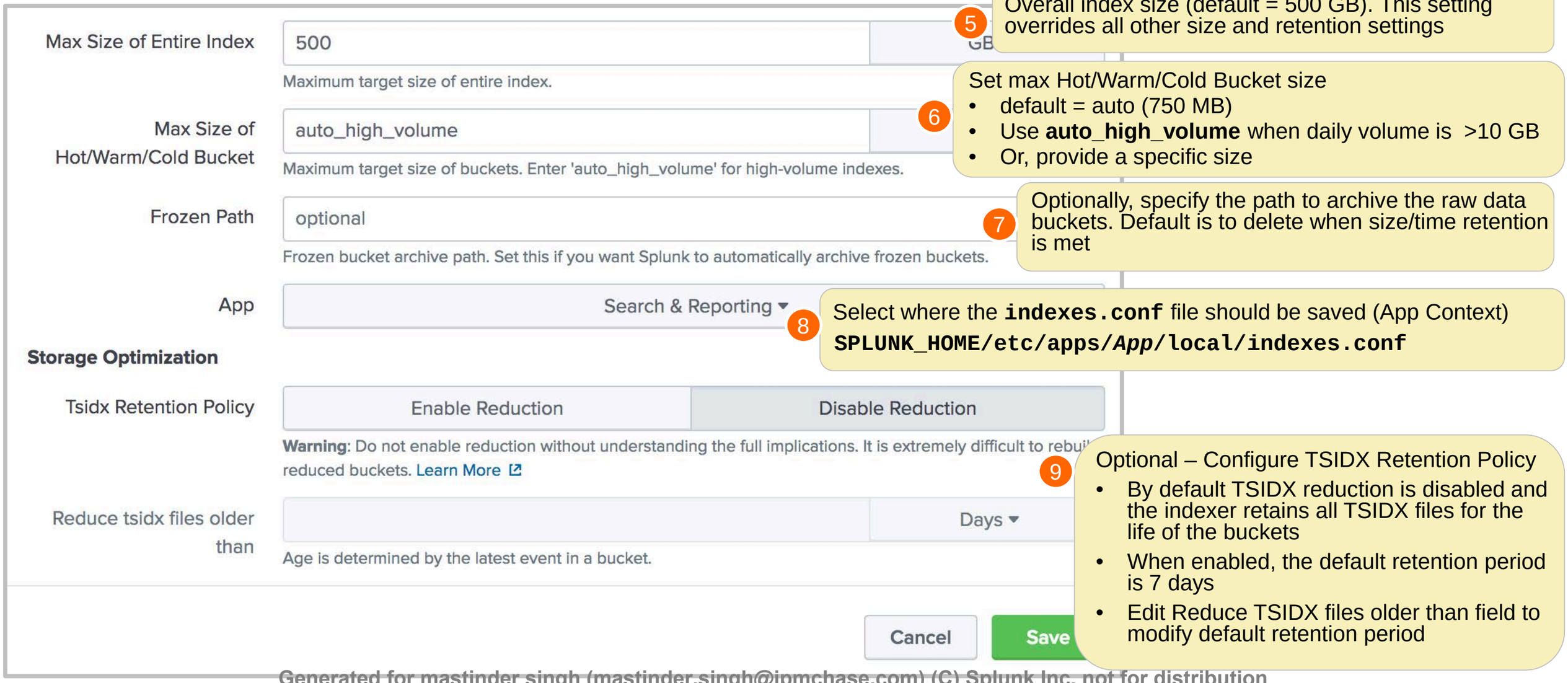
Adding an Index With Splunk Web



1. Name of index, alphanumeric, hyphens, underscores (cannot begin w/ underscore "_")
2. Select **Events** (default) or **Metrics**
3. Directory pathnames for index location (created if they don't exist)
   - **Home Path** - Most recent buckets (hot and Warm buckets)
   - **Cold Path** – Buckets aged out of hot/warm (cold buckets)
   - **Thawed Path** - Buckets copied in from archive

   Default for each **`$SPLUNK_DB/`*`indexname`*`/[db|colddb|thaweddb]`**
4. Enable data integrity check (optional)

Adding an Index With Splunk Web (cont.)



5 Overall index size (default = 500 GB). This setting overrides all other size and retention settings

6 Set max Hot/Warm/Cold Bucket size
- default = auto (750 MB)
- Use **auto_high_volume** when daily volume is >10 GB
- Or, provide a specific size

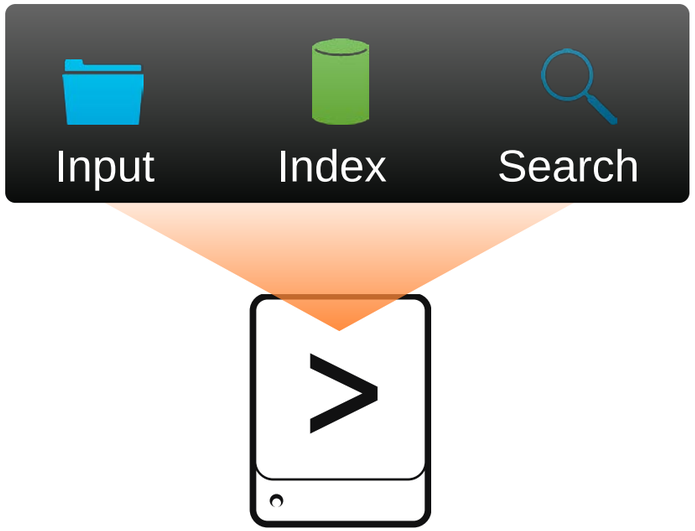
7 Optionally, specify the path to archive the raw data buckets. Default is to delete when size/time retention is met

8 Select where the **`indexes.conf`** file should be saved (App Context)
`SPLUNK_HOME/etc/apps/App/local/indexes.conf`

9 Optional – Configure TSIDX Retention Policy
- By default TSIDX reduction is disabled and the indexer retains all TSIDX files for the life of the buckets
- When enabled, the default retention period is 7 days
- Edit Reduce TSIDX files older than field to modify default retention period

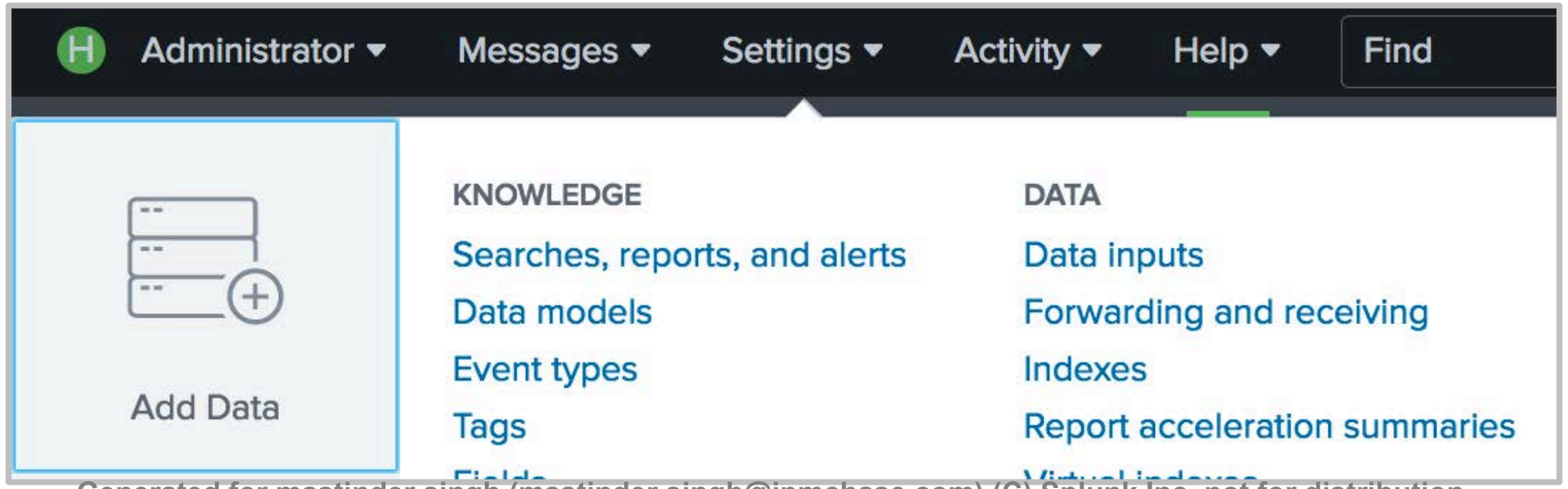
Input Staging (Index Testing)

- Production data is usually on a remote system and is not on the indexer
  - Normally data comes from one or more Splunk forwarders
- For testing, you can use Splunk Web to sample a log file on a test server
- Use **Add Data** to do this on the test server
  - Check to see if **sourcetype** and other settings are applied correctly
  - If not, delete the test data, change your test configuration, and try again

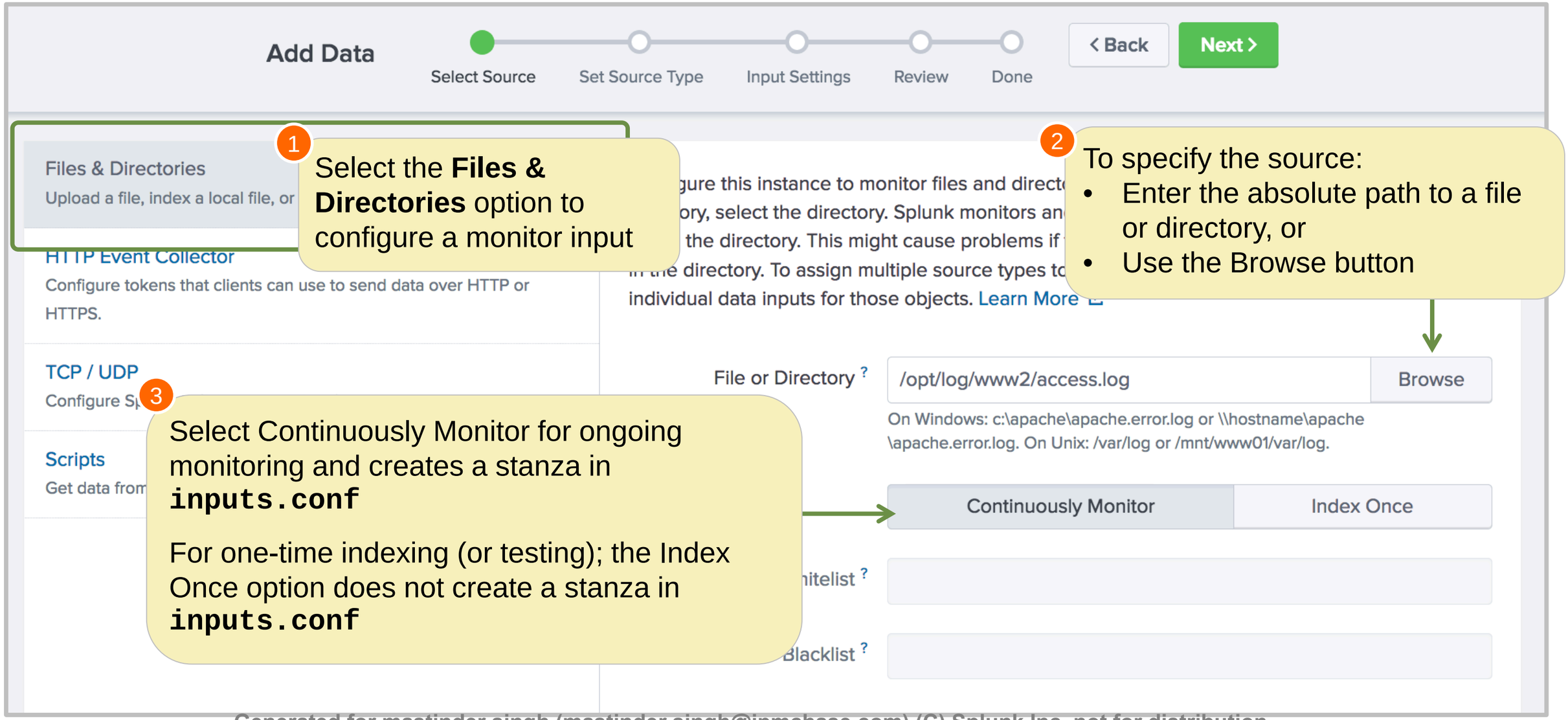


Adding an Input with Splunk Web

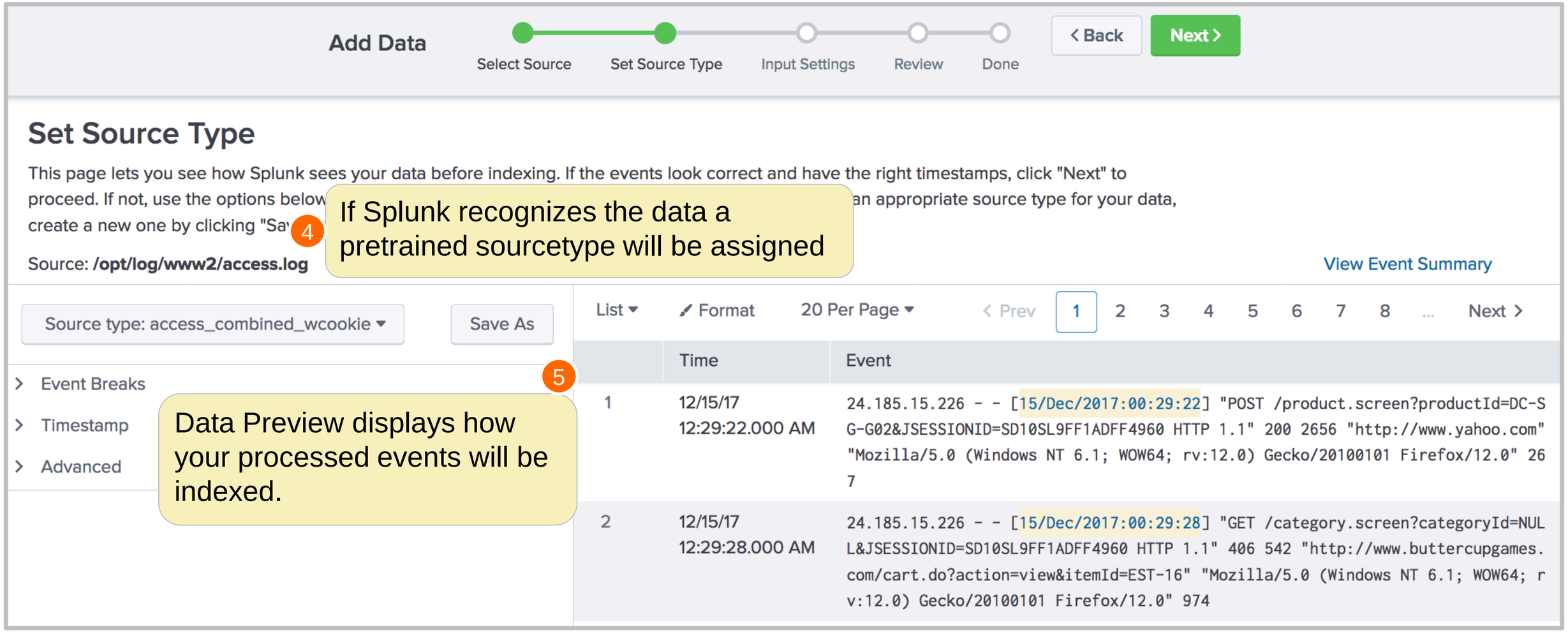
- Splunk admins have a number of ways to start the **Add Data** page
  - Click the **Add Data** icon
    - On the admin's **Home** page
    - On the **Settings** panel
  - Select **Settings** > **Data inputs** > **Add new**



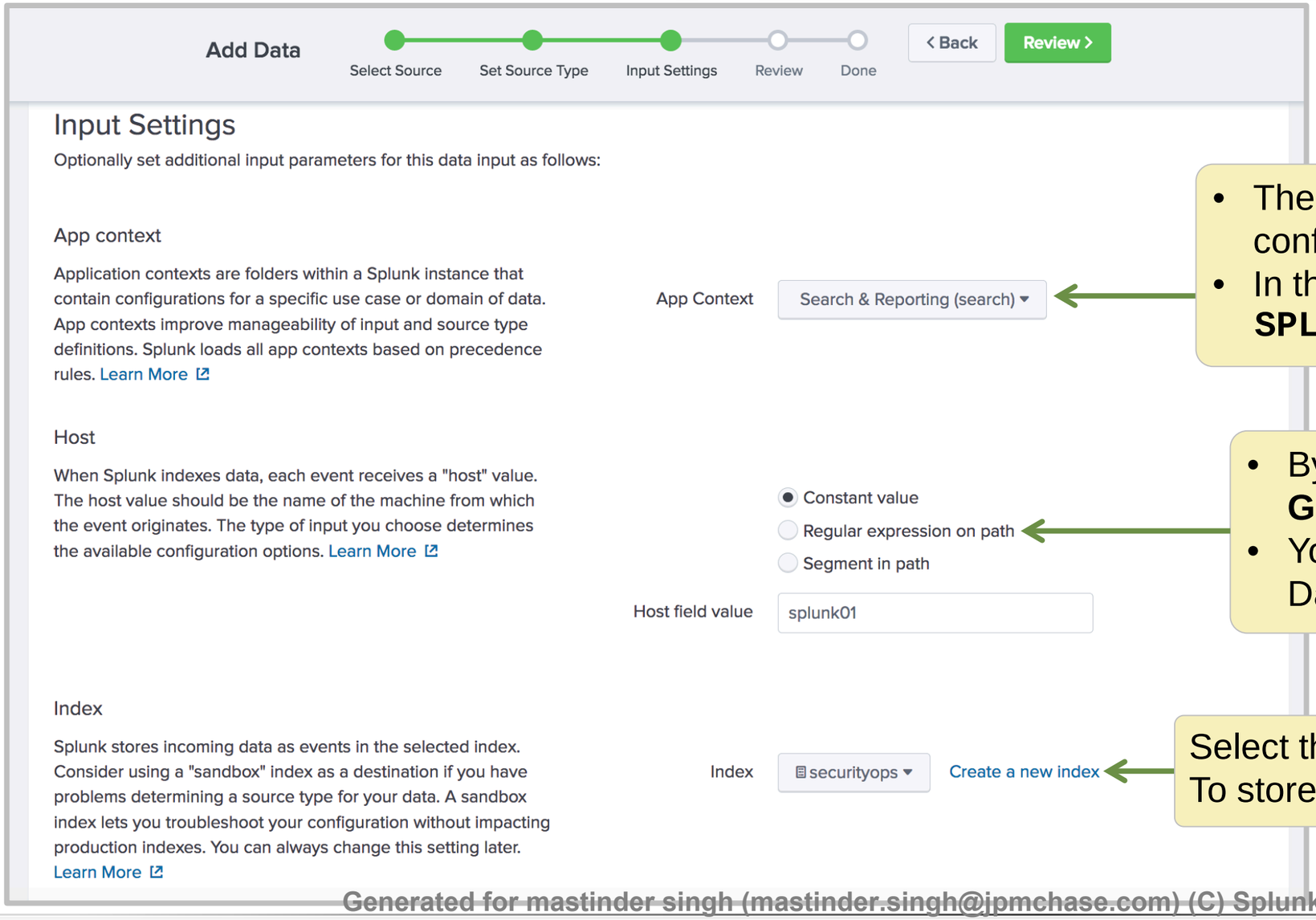
Select Source



Set Source Type (Data Preview)



Input Settings



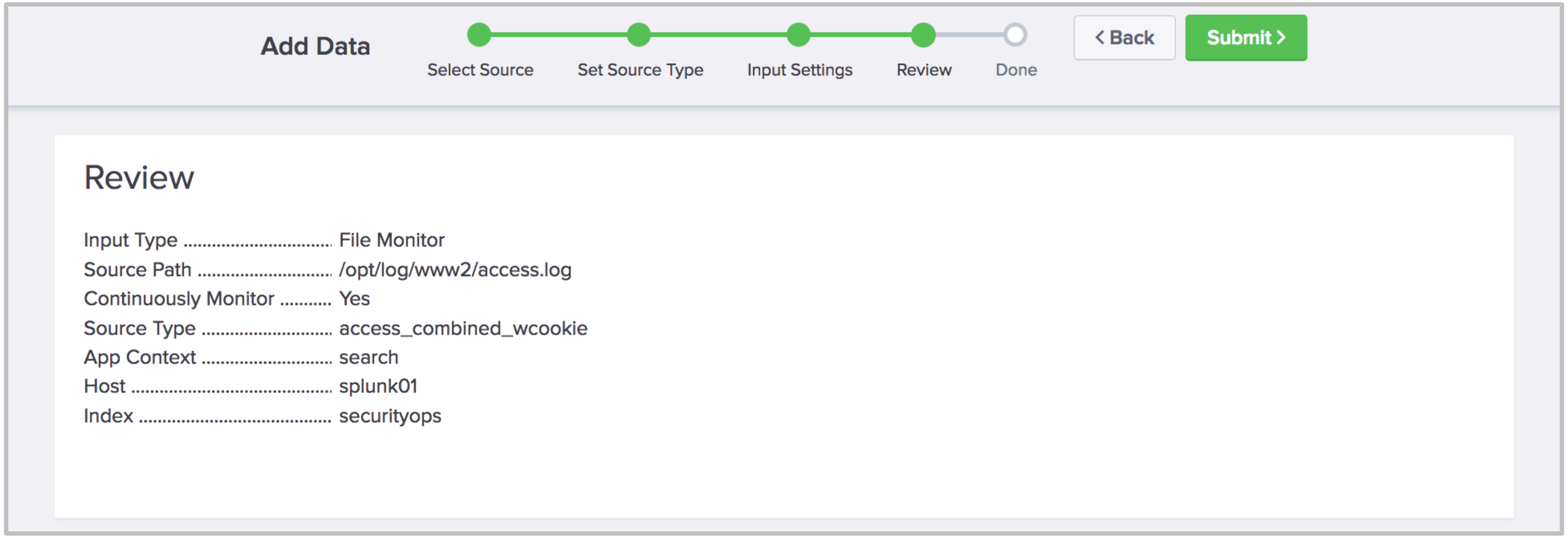
- The app context determines where your input configuration is saved
- In this example, it will be saved in: **`SPLUNK_HOME/etc/apps/search/local`**

- By default, the default host name in **General settings** is used
- You will learn about other options in the Data Administration class

Select the index where this input should be stored
To store in a new index, first create the new index

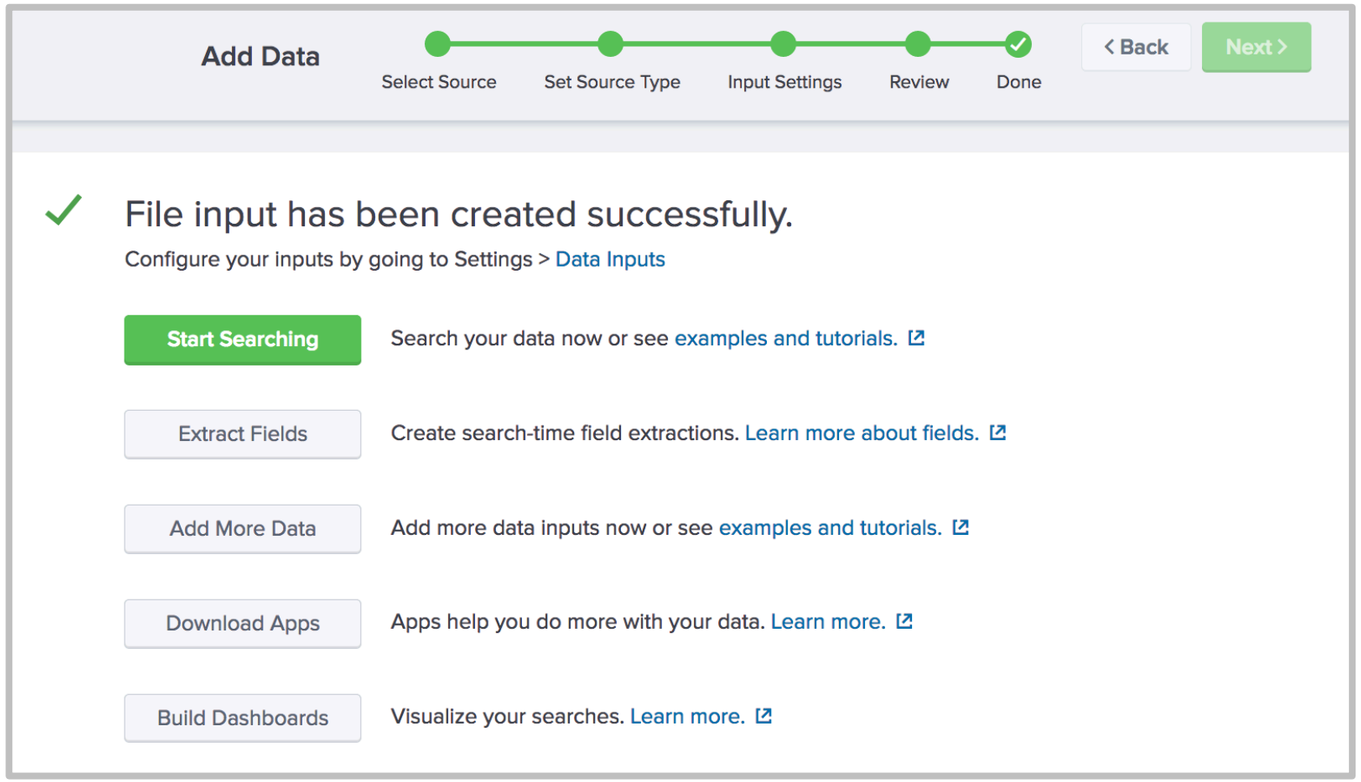
Review

Review the input configuration summary and click **Submit** to finalize



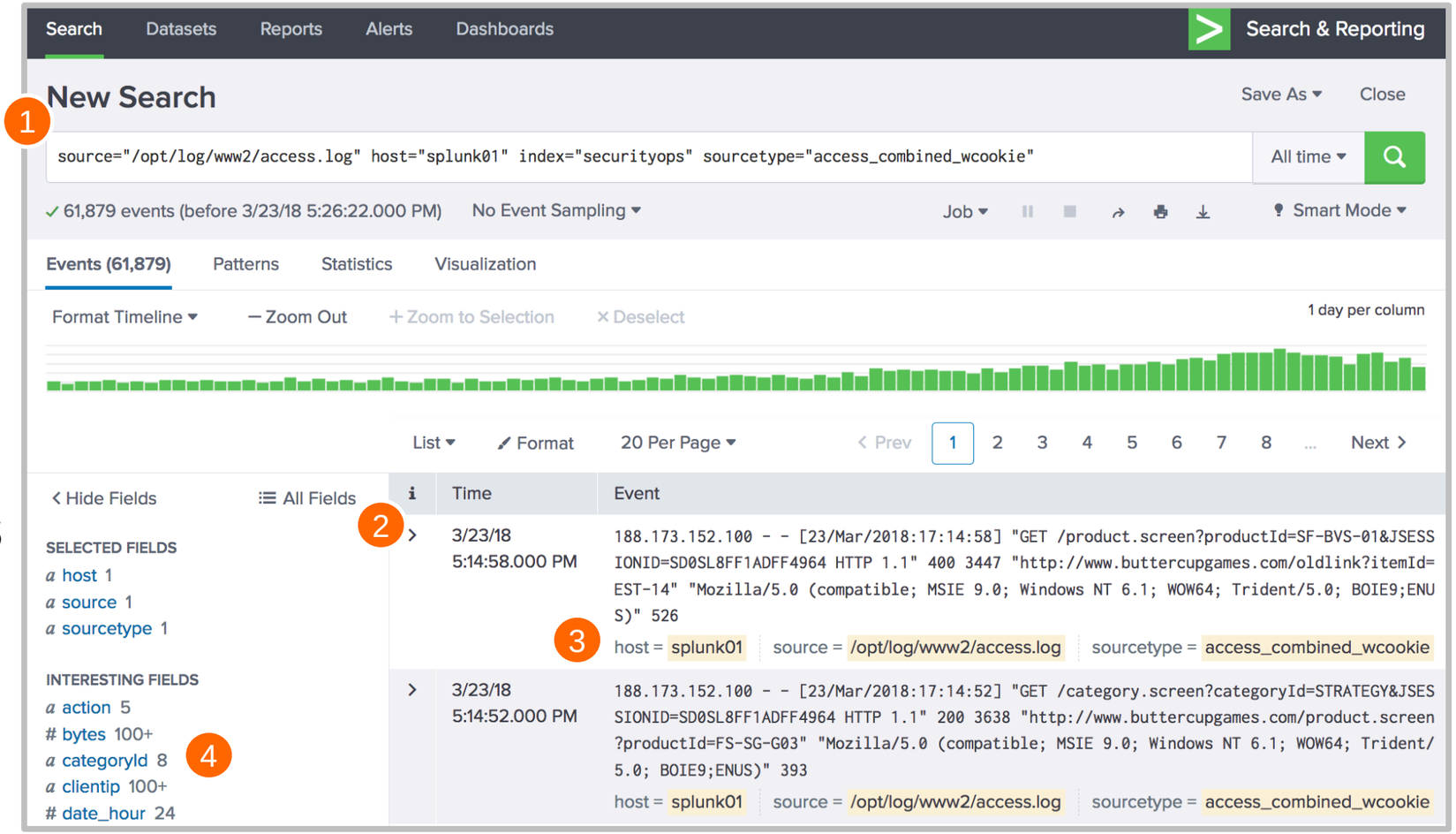
What Happens Next?

- Indexed events are available for immediate search
  - However, it may take a minute for Splunk to *start* indexing the data
- You are given other options to do more with your data
- The input configuration is saved in:
  `etc/apps/<app>/local/inputs.conf`



Verify your Input

1. Click **Start Searching** or search for **`index=<test_idx>`**
2. Verify the event timestamps
3. Confirm the **`host`**, **`source`**, and **`sourcetype`** field values
4. Check the auto-extracted field names



Lab Exercise 5 – Add Indexes

- **Time:** 5 - 10 minutes
- **Tasks:**
- Create two new indexes: **`securityops`** and **`itops`**
- Add a file monitor input to send events to the **`securityops`** index

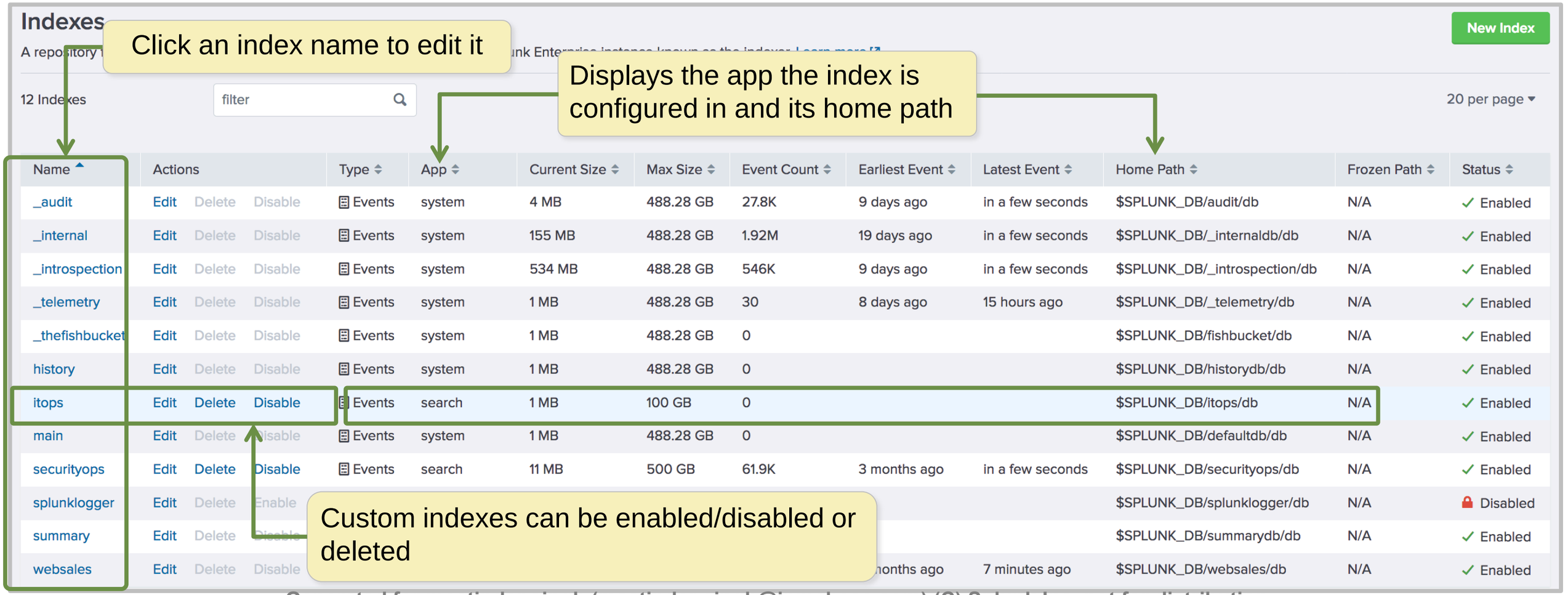
Module 6: Splunk Index Management

Module Objectives

- Manage indexes with Splunk Web
- Describe **`indexes.conf`** options
- Customize index retention policies
- Back up indexes
- Delete events from an index
- Restore frozen buckets

Managing Indexes with Splunk Web

Select **Settings > Indexes**



Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Frozen Path	Status
_audit	Edit Delete Disable	Events	system	4 MB	488.28 GB	27.8K	9 days ago	in a few seconds	$SPLUNK_DB/audit/db	N/A	Enabled
_internal	Edit Delete Disable	Events	system	155 MB	488.28 GB	1.92M	19 days ago	in a few seconds	$SPLUNK_DB/_internaldb/db	N/A	Enabled
_introspection	Edit Delete Disable	Events	system	534 MB	488.28 GB	546K	9 days ago	in a few seconds	$SPLUNK_DB/_introspection/db	N/A	Enabled
_telemetry	Edit Delete Disable	Events	system	1 MB	488.28 GB	30	8 days ago	15 hours ago	$SPLUNK_DB/_telemetry/db	N/A	Enabled
_thefishbucket	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			$SPLUNK_DB/fishbucket/db	N/A	Enabled
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			$SPLUNK_DB/historydb/db	N/A	Enabled
itops	Edit Delete Disable	Events	search	1 MB	100 GB	0			$SPLUNK_DB/itops/db	N/A	Enabled
main	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			$SPLUNK_DB/defaultdb/db	N/A	Enabled
securityops	Edit Delete Disable	Events	search	11 MB	500 GB	61.9K	3 months ago	in a few seconds	$SPLUNK_DB/securityops/db	N/A	Enabled
splunklogger	Edit Delete Enable								$SPLUNK_DB/splunklogger/db	N/A	Disabled
summary	Edit Delete Disable								$SPLUNK_DB/summarydb/db	N/A	Enabled
websales	Edit Delete Disable						months ago	7 minutes ago	$SPLUNK_DB/websales/db	N/A	Enabled

Index Data Integrity Check

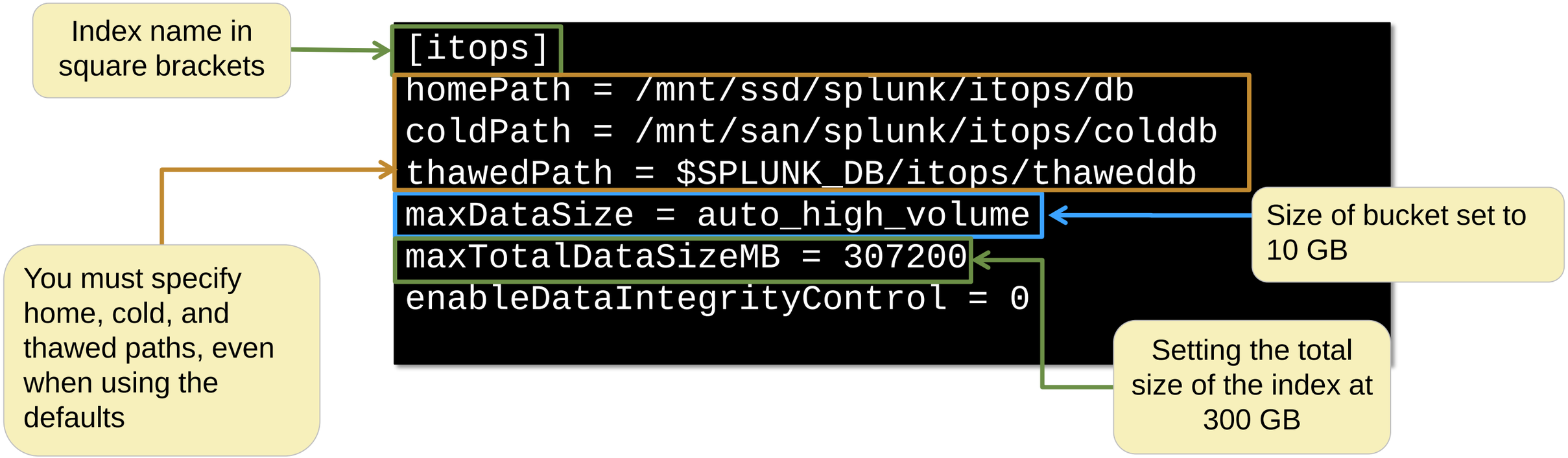
- Provides an ability to validate that data has not been tampered with after indexing

  docs.splunk.com/Documentation/Splunk/latest/Security/Dataintegritycontrol

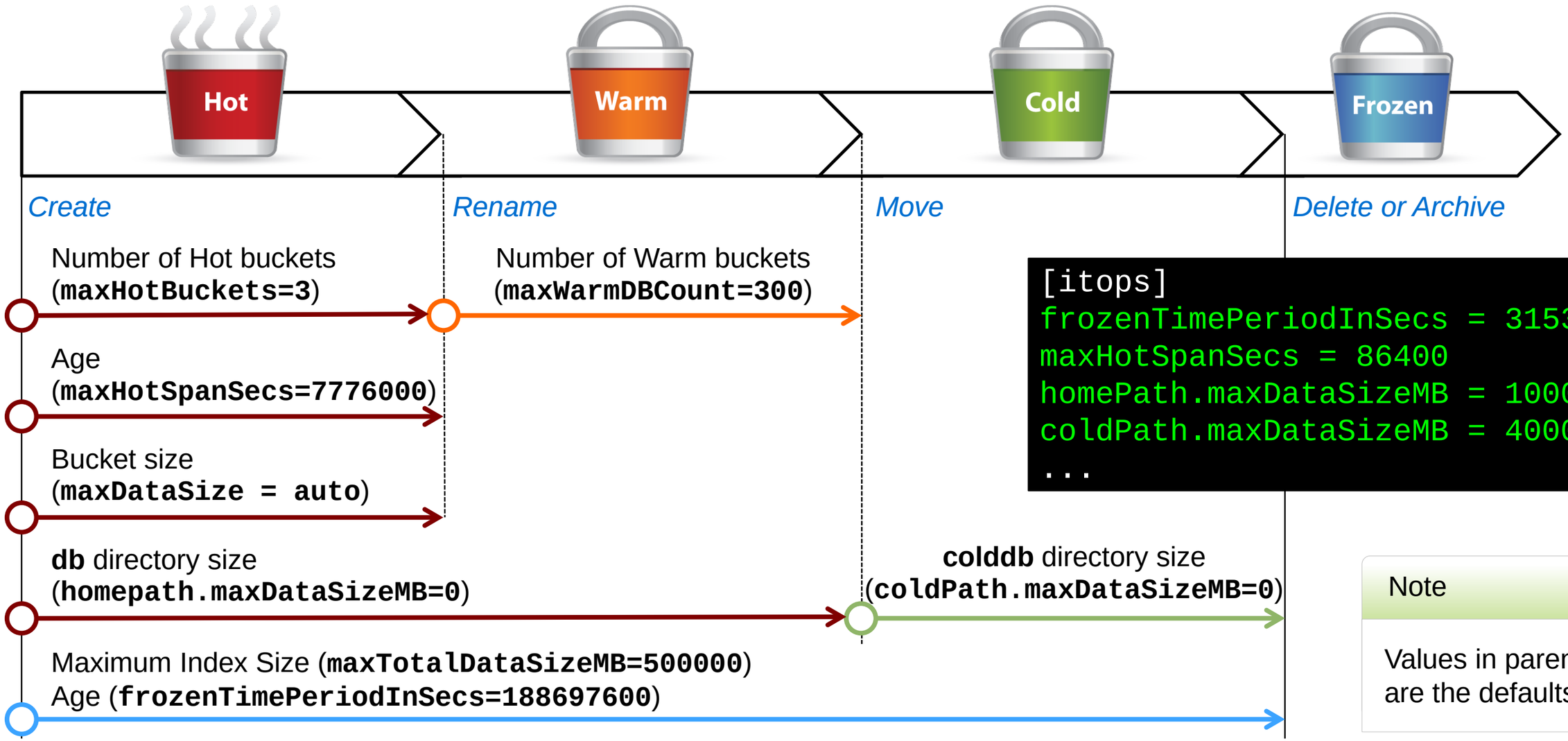
- When enabled, produces calculated hash files for auditing and legal purposes
  - Works on index level (including clustering)
  - Does not protect in-flight data from forwarders
  - To prevent data loss, use the indexer acknowledgment capability (`useACK`)
- To verify the integrity of an index/bucket:
  - **`splunk check-integrity -bucketPath [bucket_path] [verbose]`**
  - **`splunk check-integrity -index [index] [verbose]`**
- To re-generate hash files:
  - **`splunk generate-hash-files [-bucketPath|-index] [bucket_path|index]`**

indexes.conf

The index stanza is created in **`local/indexes.conf`** of the selected app



indexes.conf Options



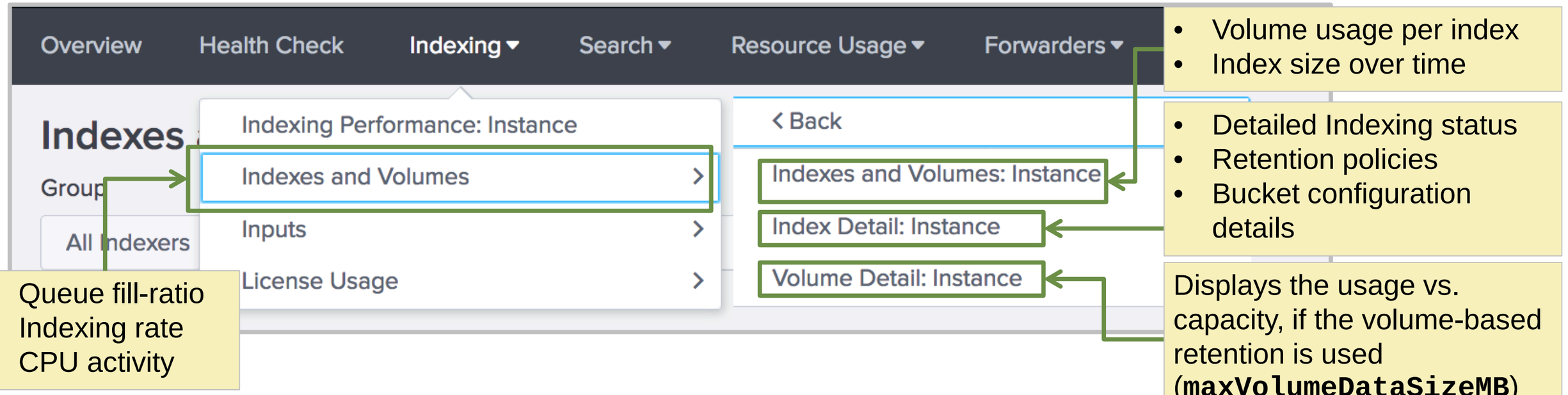

```
[itops]
frozenTimePeriodInSecs = 31536000
maxHotSpanSecs = 86400
homePath.maxDataSizeMB = 100000
coldPath.maxDataSizeMB = 400000
...
```

Note

Values in parentheses are the defaults.

Viewing Indexing Activity and Health

- **Monitoring Console**
  - Provides comprehensive indexing activity details
  - **Snapshot** shows averages over the previous 15 minutes
  - **Historical** exposes trending and possible decaying health



Customizing Index Retention Policies

- To set more advanced/specific options, edit the stanza in **`indexes.conf`**
- New indexes default to 3 hot buckets at a time
  - If it is likely that an index will receive events that are not in time-sequence order, increase the number of available hot buckets
- High-volume indexes should have up to 10 hot buckets
  - Set with the **`maxHotBuckets`** key
- **Best practice** for high-volume indexes:
  - Examine and copy settings of **`main`** index stanza and adjust for your case

Warning

Incorrect retention settings can cause premature bucket rotation and even stop Splunk. It is advised to contact Splunk Professional Services before editing retention policies.

Strict Time-based Retention Policies

- Example: Purge HR data when it is more than 90 days old, but no sooner
- Issues to consider:
  - Splunk freezes entire buckets, not individual events
  - If a bucket spans more than one day, you can't meet the 90 day requirement
- Configuration option:

  `frozenTimePeriodInSecs = 7776000` (90 days)

  `maxHotSpanSecs = 86400` (24 hours)

Warning

These options satisfy the strict data retention policy but may negatively impact performance. Using small maxHotSpanSecs under indexer clustering is not recommended because it can produce many small buckets.

Monitor bucket size and the rate of accumulation (bucket count wise) closely after changing.

Volume Stanzas in indexes.conf

- Example: Prevent data bursts in one index from triggering indexing issues elsewhere in the same volume
- Issues to consider:
  - Splunk cannot determine the maximum size for non-local volumes
  - Hot/warm and cold buckets can be in different volumes
  - If the volume runs out of space, buckets roll to frozen before **`frozenTimePeriodInSecs`**
- Configuration Options: Use volume reference if a retention based on size is desired

```
[volume:fast]
path = /mnt/ssd/
maxVolumeDataSizeMB = 500000

[volume:slow]
path = /mnt/raid/
maxVolumeDataSizeMB = 4000000
```

```
[soc]
homePath = volume:fast/soc/db
homePath.maxDataSizeMB = 50000
coldPath = volume:slow/soc/colddb
coldPath.maxDataSizeMB = 200000
```

What to Back Up

- Indexed events – Splunk indexes
  - **SPLUNK_HOME/var/lib/splunk/**
  - Or the directories where you placed your indexes (see **indexes.conf** for details)
- The monitored source data files (optional)
- **SPLUNK_HOME/etc** for config and other important files
  - **apps**
  - **users**
  - **system/local**
  - **licenses**
  - **init.d**
  - **passwd**
  - and more

Backup Recommendation

- Use the incremental backup of your choice
  - Warm and cold buckets of your indexes
  - Configuration files
  - User files
- Hot buckets cannot be backed up without stopping Splunk
  - Use the snapshot capability of underlying file system to take a snapshot of hot, then back up the snapshot
  - Schedule multiple daily incremental backups of warm
    - Works best for high data volumes

Moving an Index

1. Stop Splunk
2. Copy the entire index directory to new location while preserving permissions and all subdirectories
   - *NIX: **`cp -rp <source> <target>`**
   - Windows: **`xcopy <source> <target> /s /e /v /o /k`** (or, robocopy)
3. If this is a global change, unset the **`SPLUNK_DB`** environment variable and update **`SPLUNK_HOME/etc/splunk-launch.conf`**
4. Edit **`indexes.conf`** to indicate the new location
5. Start Splunk
6. After testing and verifying new index, the old one can be deleted

Removing Indexed Events

- If you have unwanted events in an index
  - Splunk does not have an index editor
  - First, you should address your configuration to omit/modify future incoming events
- What are your options for events already in the index?
  - Let the events age-out normally (whole bucket ages out)
  - Use the **`delete`** command to make the unwanted events not show up in searches
  - Following options are NOT recommended in production:
    - Run **`splunk clean`** command to delete **ALL** events from the index
    - Delete the index

Deleting Events

- Create a native account with the **can_delete** role
  - Specifically set up for deletions
  - DO NOT give this capability to other roles
    - By default, the admin role does not have this ability
- Delete CANNOT be undone:
  - Log into Splunk Web as a user of the **can_delete** role
  - Create a specific search that identifies the data you want to delete
    - Double check that the search ONLY includes the events to delete
    - Pay special attention to which index you are using and the time range
  - After you are certain you've targeted only the data you want to delete, then pipe the **`delete`** command

Note

This is a "virtual" delete. Splunk marks the events as deleted and they never show in searches again. However, they continue to take up space on disk.

Cleaning Out an Index

- To flush indexed events and reset an index, use the CLI **`clean`** command
  - DATA WILL BE PERMANENTLY DESTROYED
  - Typically used on test/dev systems, not for production systems
- Command syntax:

  `splunk clean` `[eventdata|userdata|all] [-index name]`
    - **`eventdata`** – delete indexed events and metadata on each event
    - **`userdata`** – delete user accounts
    - **`all`** – everything - including users, saved searches, and alerts
  - ALWAYS SPECIFY AN INDEX TO AVOID TEARS

  WARNING! If no index is specified, the default is to clean (destroy) all indexed events from all indexes!

The Fishbucket – Re-indexing Data

- The **`fishbucket`** index stores the checkpoint information for monitor inputs
- To reset the individual input checkpoint, use the `btprobe` command:

```
splunk cmd btprobe –d SPLUNK_HOME/var/lib/splunk/
fishbucket/splunk_private_db --file <source> --reset
```

- Requires stopping the forwarder or indexer
- Other options:
  - **`splunk clean eventdata –index _thefishbucket`**
    - Force re-indexing of all file monitors in the indexer
    - Resetting the monitor checkpoint re-indexes the data and results in more license usage
  - **`rm -r ~/splunkforwarder/var/lib/splunk/fishbucket`**
    - Manually delete the **`fishbucket`** on forwarders

Restoring a Frozen Bucket

- To thaw a frozen bucket:
  - Copy the bucket directory from the frozen directory to the index's **`thaweddb`** directory
  - Stop Splunk
  - Run `splunk rebuild <path to thawed bucket directory>`
    - Does not count against license
  - Start Splunk
- Events in **`thaweddb`** are searchable along with other events
  - They will not be frozen, nor do they count against the index max size
  - Delete the thawed bucket directory when no longer needed and restart Splunk

Index Replication

- Splunk indexers can function as a **cluster**
  - Indexers in a cluster replicate buckets amongst themselves
- Index replication allows for rapid failure recovery
- Fully configurable replication allows you to balance speed of recovery and overall disk usage
- Index replication requires additional disk space
- Discussed in detail in **Splunk Cluster Administration** class
- Basic indexer cluster concepts:

  http://docs.splunk.com/Documentation/Splunk/latest/Indexer/Basicconcepts

Further Reading

- docs.splunk.com/Documentation/Splunk/latest/Indexer/HowSplunkstoresindexes
- docs.splunk.com/Documentation/Splunk/latest/Indexer/Setlimitsondiskusage
- docs.splunk.com/Documentation/Splunk/latest/Indexer/Automatearchiving
- wiki.splunk.com/Deploy:BucketRotationAndRetention

Lab Exercise 6 – Configure Retention Policies

- **Time**: 15 – 20 minutes
- **Tasks**:
- Configure a strict time-based retention policy for **`securityops`**
- Configure a volume-based retention policy for **`itops`**
- Use MC to monitor retention settings
- Create a local input to test

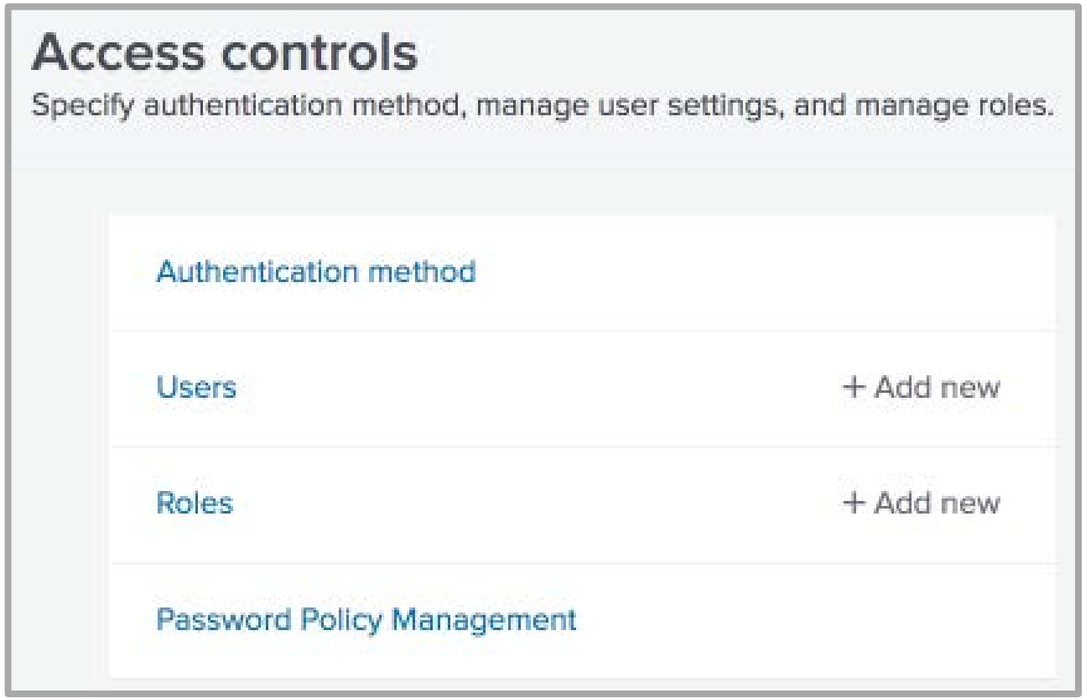
Module 7: Splunk User Management

Module Objectives

- Add Splunk users using native authentication
- Describe user roles in Splunk
- Create a custom role

Managing Users and Roles

- Users and roles define user privileges
- To have access to a Splunk instance, a user must have:
  - A Splunk user account
  - Assignment to one or more Splunk roles
- Click **Settings > Access controls**

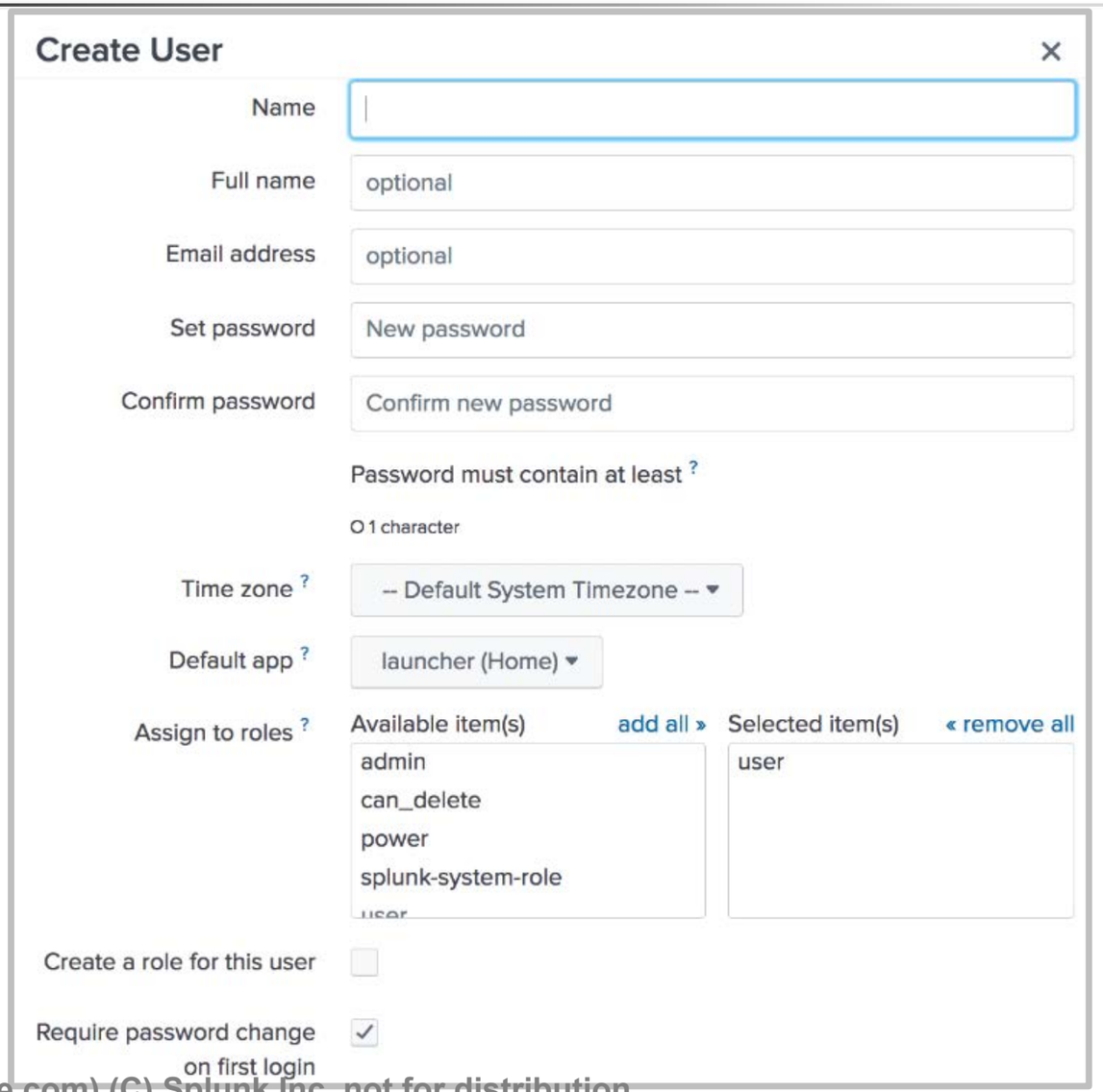


Adding Users in Splunk

- You can create user accounts directly in Splunk
  - Example: **`admin`** user
- Passwords are stored in **`SPLUNK_HOME/etc/passwd`**
- Use a blank password file to completely disable native authentication BUT
  - In all authentication scenarios, best practice is to keep a failsafe account here with a VERY strong password
- You can have a mix of Splunk and LDAP or other users
  - Splunk native authentication always takes precedence over others

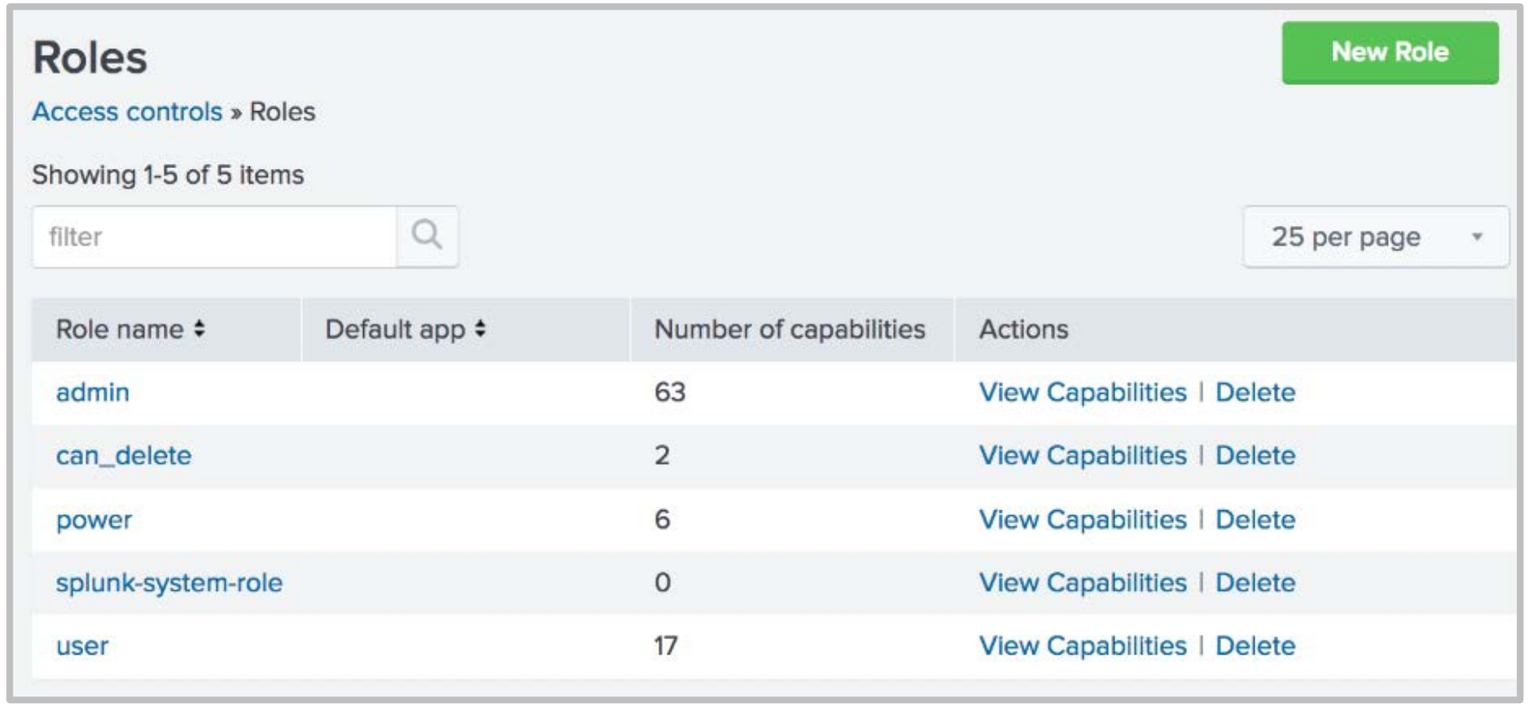
Adding Native Users

- Required:
  - Username and password
- Optional:
  - Full name and email address (defaults to none)
  - Time zone (defaults to search head time zone)
  - Default app (defaults to role default app, or home if no role default app)
  - Role(s)
    - Defaults to **user**
  - Change password on first login requirement
    - Defaults to enabled

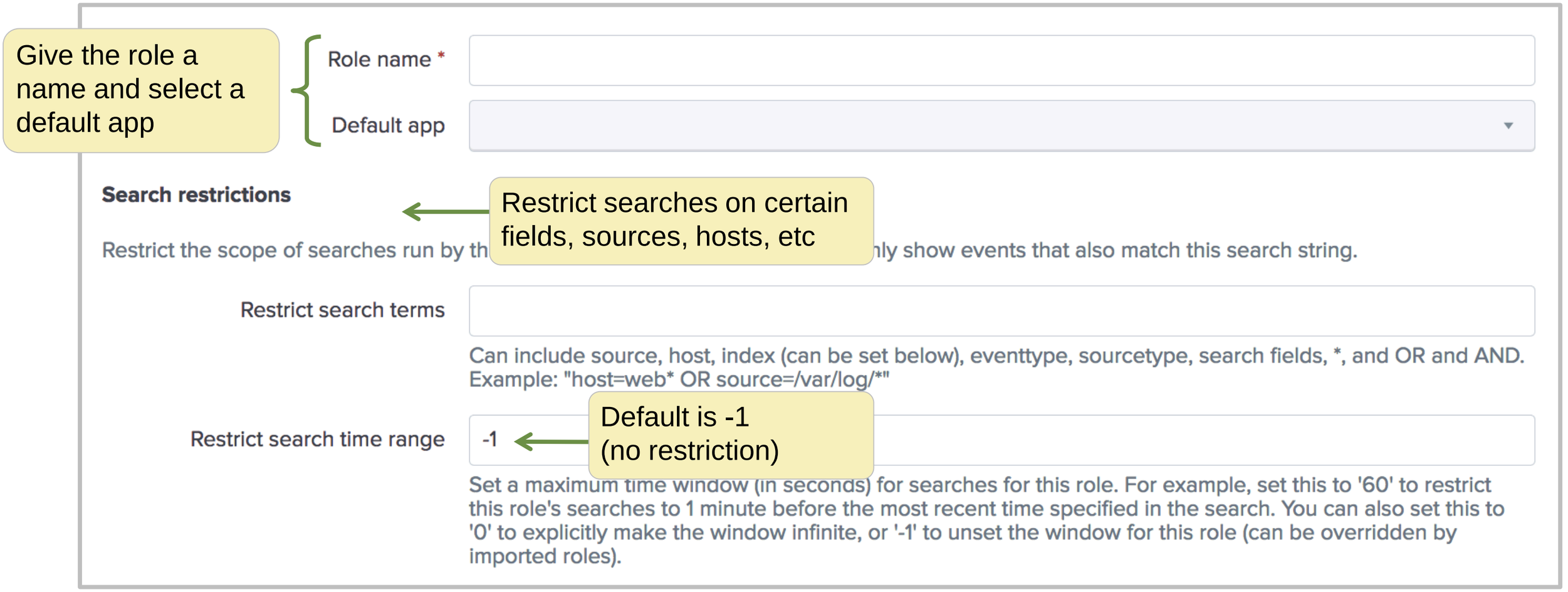


Identifying Roles

- Five built-in user roles:
  - **admin**, **power**, and **user**
    - Users can be assigned these roles
  - **`can_delete`**
  - **`splunk-system-role`**
    - Special role that allows system services to run without a defined user context
- Administrators can add custom user roles

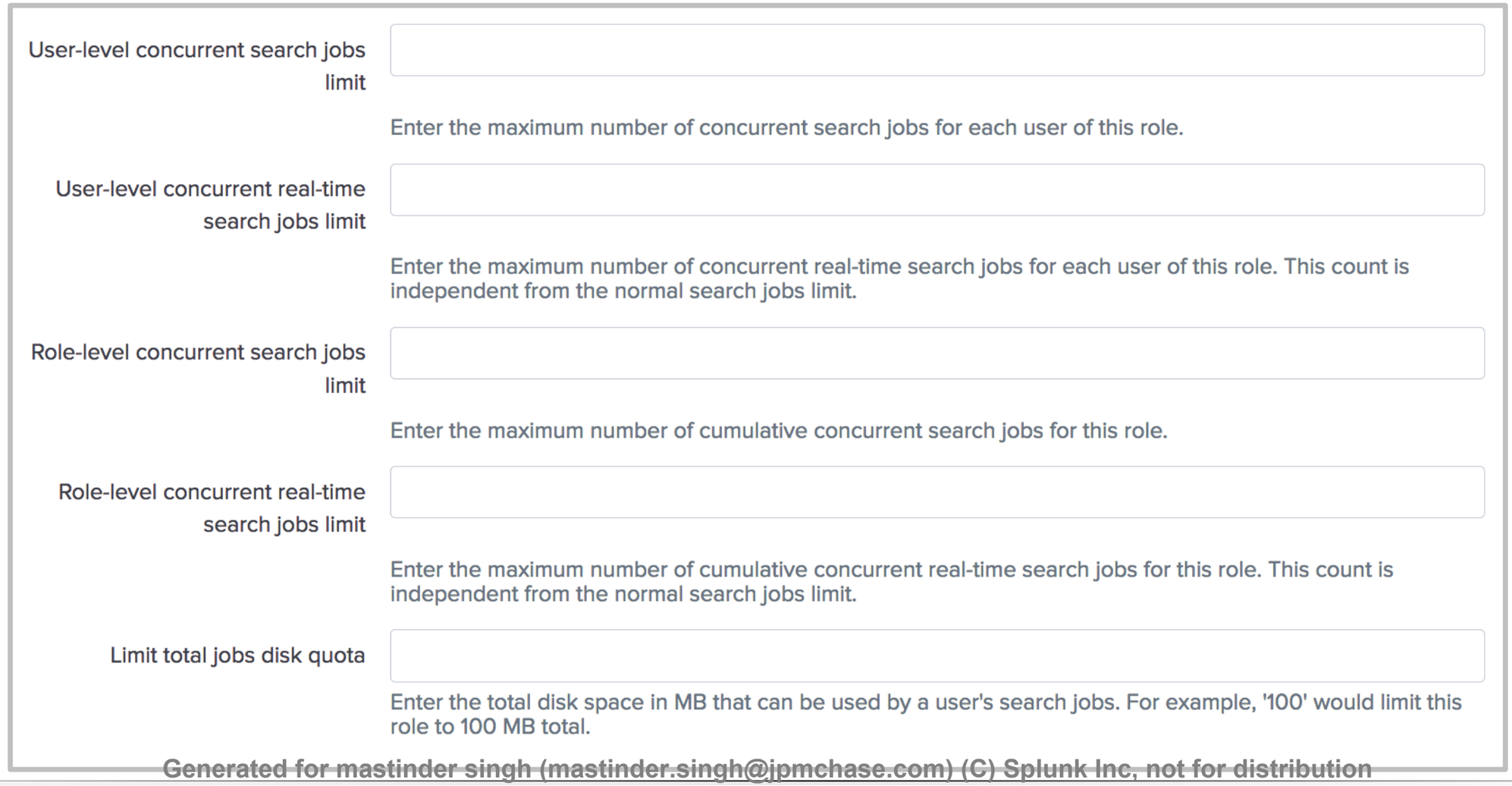


Defining Custom User Roles



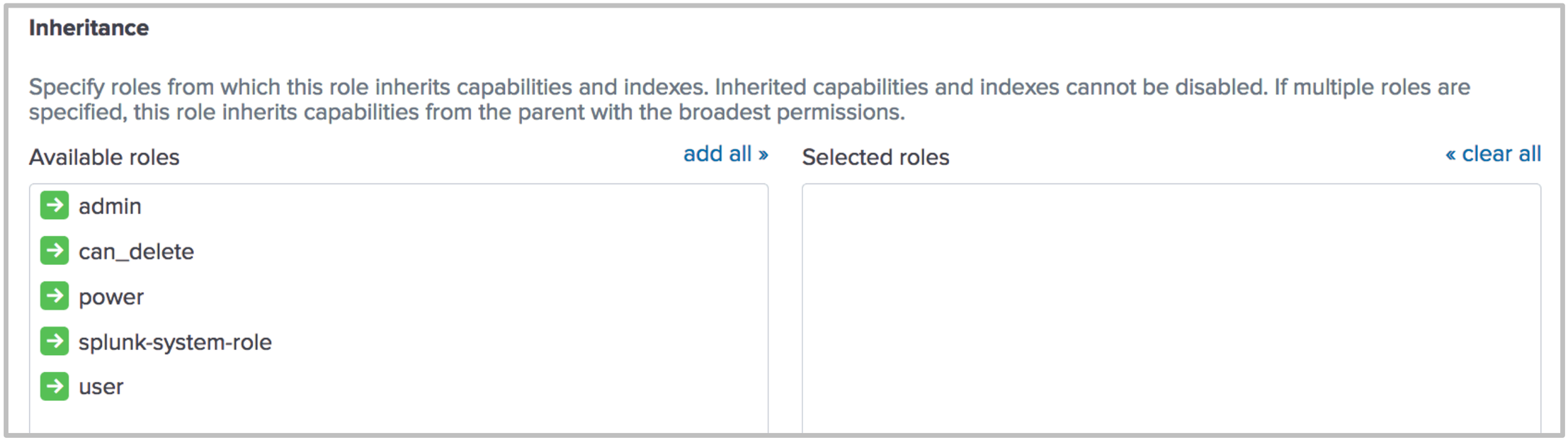
Defining Custom User Roles (cont.)

Optional user-level and role-level limits



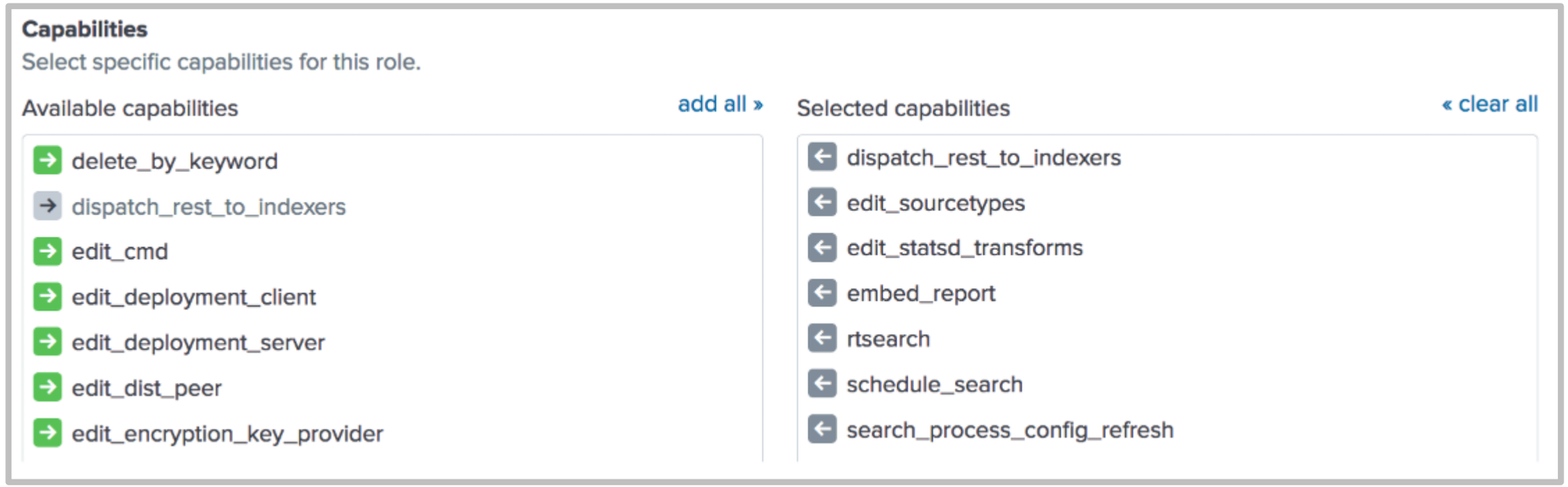
Describing Role Inheritance

- A new role can be based on one or more existing roles
- The new role inherits capabilities and index access
  - Inherited index access is not visible in the user interface
- You cannot disable inherited capabilities or access



Defining Role Capabilities

- Assign or remove capabilities
  docs.splunk.com/Documentation/Splunk/latest/Admin/authorizeconf



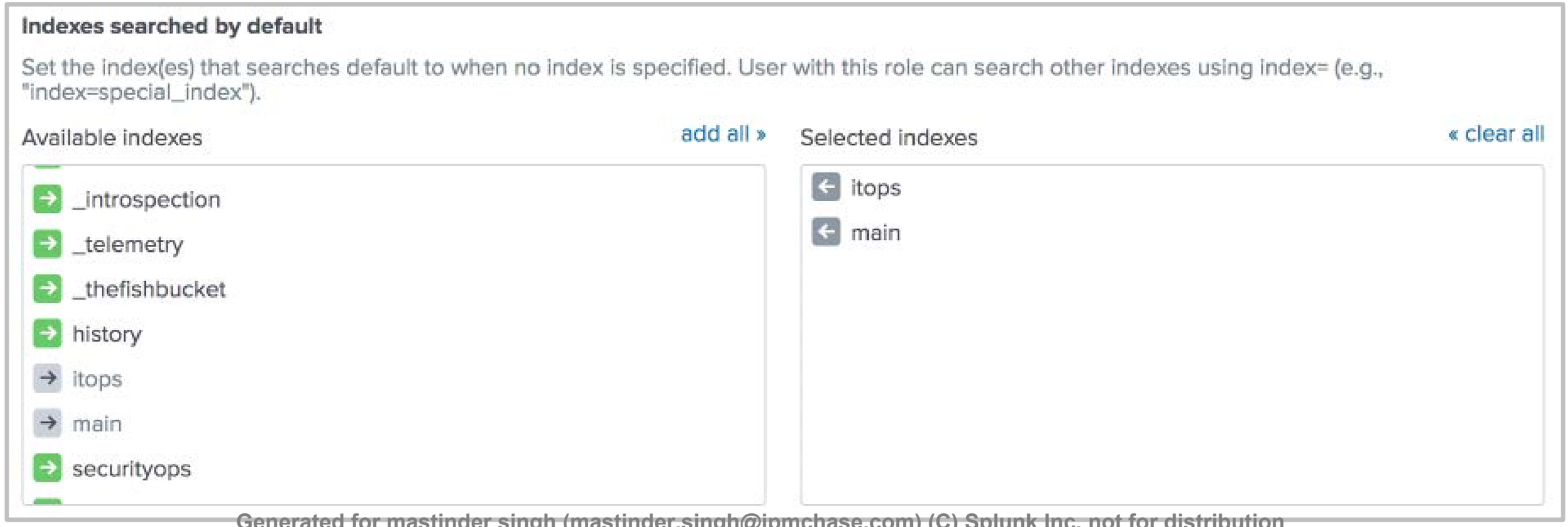
Inherited capabilities are visible in the **Imported capabilities** box

Implications of Inheritance

- If you create a new role that inherits from another role, such as **user**:
  - The new role has all the capabilities of the inherited role
  - The new role inherits the index settings (both default and allowed)
  - You cannot turn off capabilities or index access that was inherited from the original role
- If you want a role that is "like" **user** but with some capabilities turned off:
  1. Make a new role that does not inherit from any other role
  2. Turn on all of the same capabilities as in User, except those you want turned off
  3. Assign the appropriate indexes to the new role

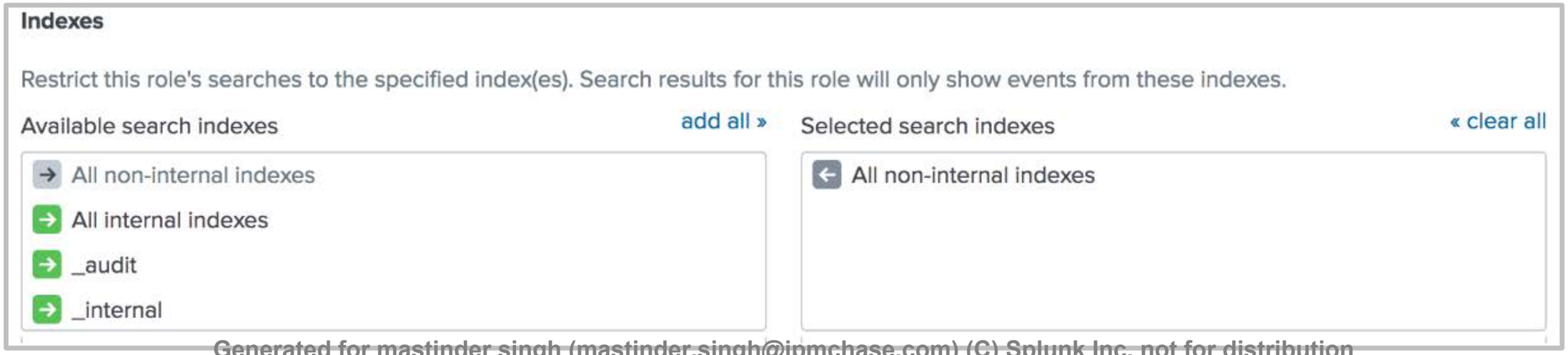
Role Index Search Options

- You can specify which indexes are searched if the user does not specify "**index=<index_name>**"
  - Usually, this should match the **Indexes** setting



Defining Role Index Access Options

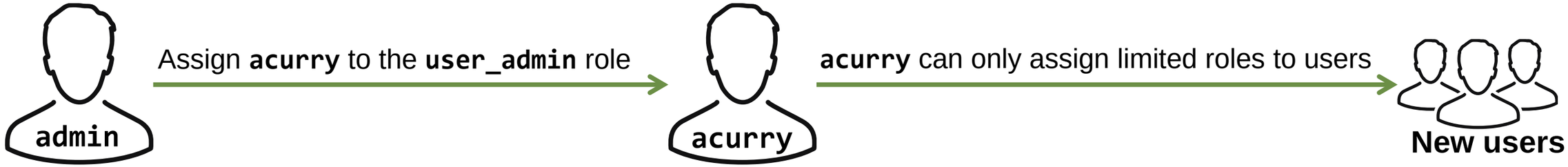
- Most important index setting
  - Controls which indexes the users in this role can access
  - If not selected, users cannot search or even see this index
- Inherited indexes are still available **even though they are not listed**
- The default is **All non-internal indexes**
  - Revisit access control each time a new index has been added



`edit_roles_grantable` Capability

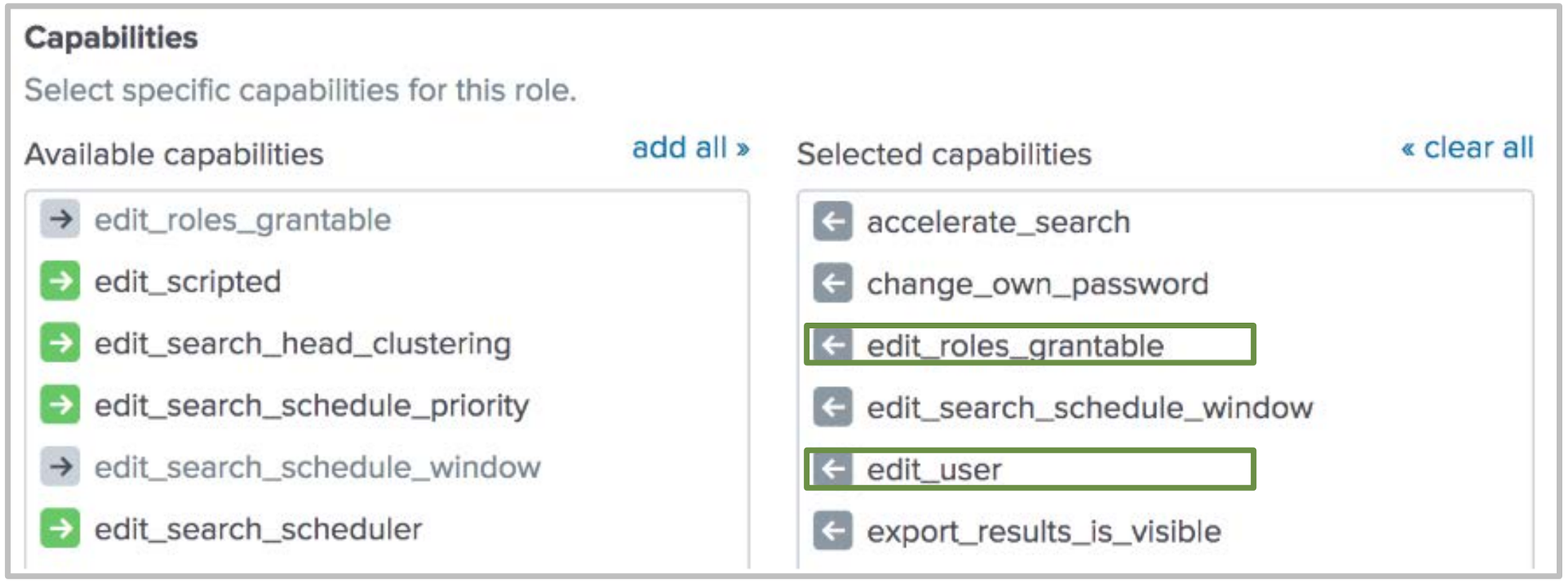
- Example: I want to separate and delegate administration tasks between sys-admins and data admins without granting full **`admin`** role
- Issues to consider:
  - With **`edit_roles`** and **`edit_user`** capabilities, users can promote themselves to full **`admin`** role
  - Want to restrict grantable capabilities only to the level sub-admins currently have
- Configuration option:
  - Add the **`edit_roles_grantable`** capability to the ***`sub-admin`*** role
    - Can only create roles with subset of the capabilities that the current user role has
    - Must use in conjunction with the **`edit_user`** capability

Example: edit_roles_grantable Capability



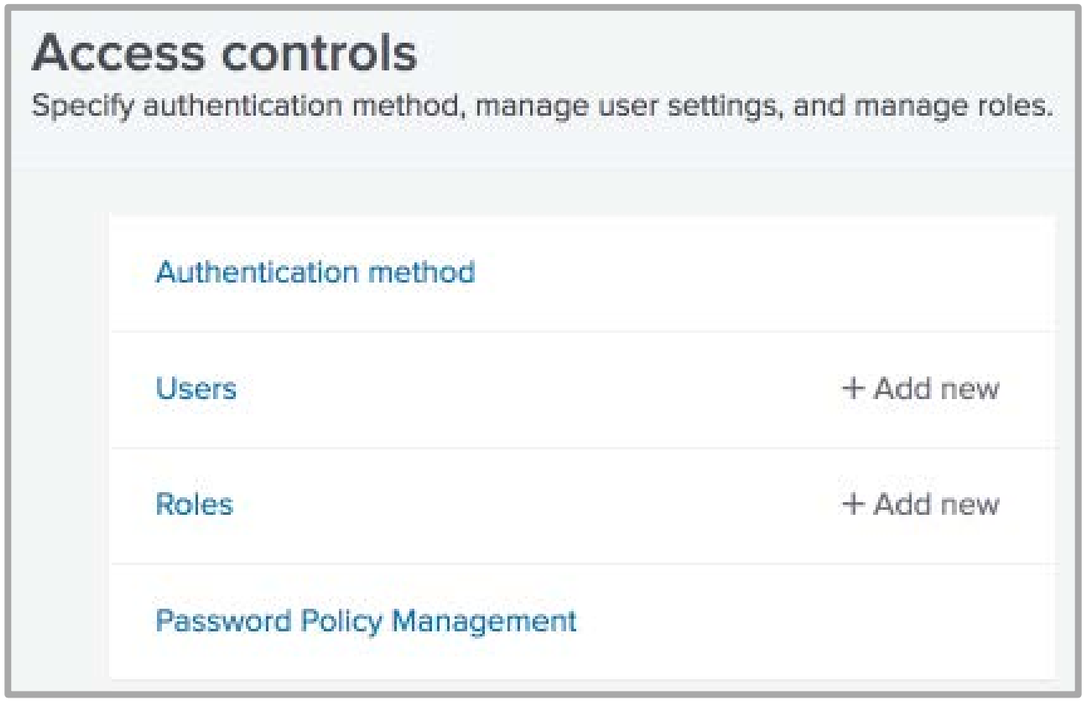
Add new role **user_admin**

- Inheritance:
  - **power**
  - **user**
- Capabilities:
  - **edit_roles_grantable**
  - **edit_user**



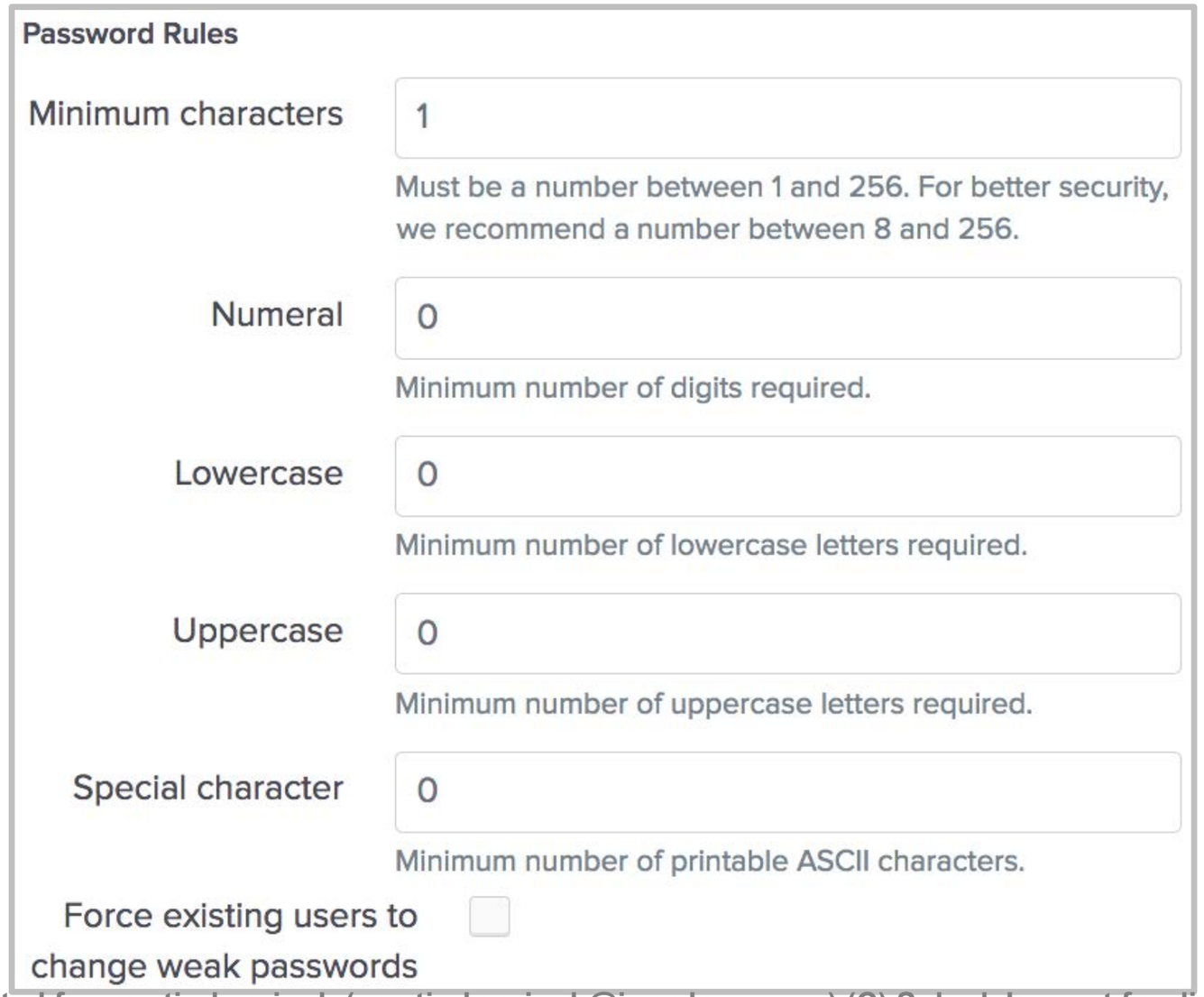
Password Policy Management

- Splunk 7.1 introduces password management options for administrators
  - Only applies to native Splunk users
    - Does not apply to SAML or LDAP passwords
  - Click **Settings > Access controls > Password Policy Management**
- Password best practices:

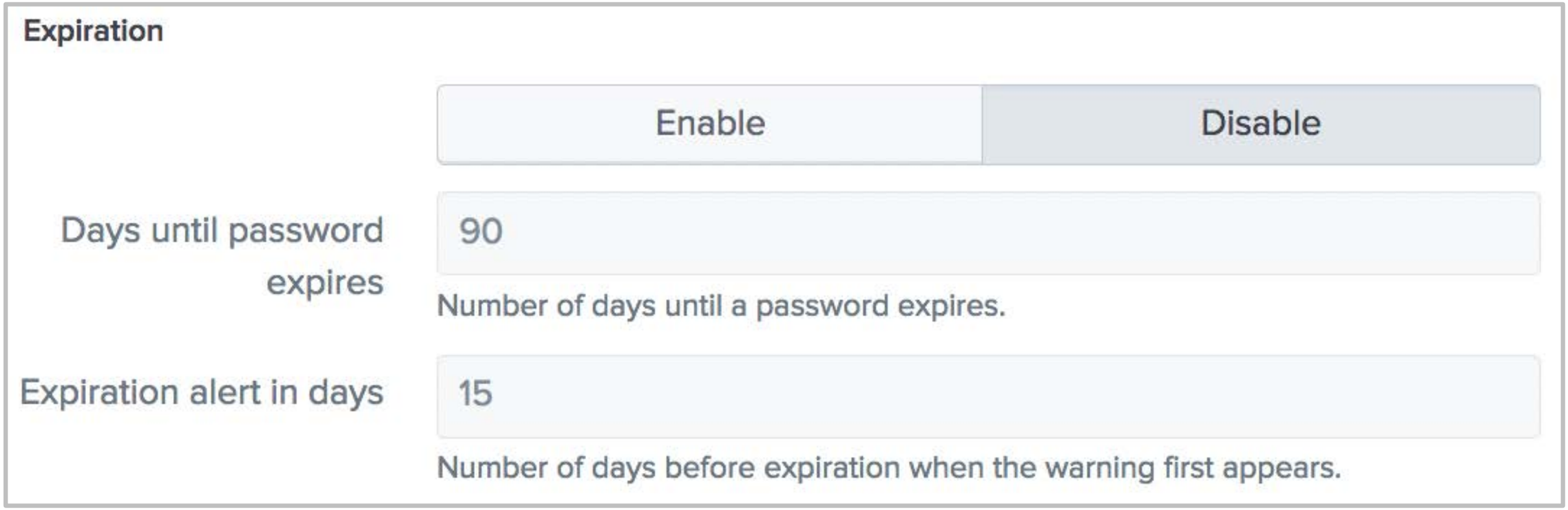


http://docs.splunk.com/Documentation/Splunk/7.1.0/Security/Passwordbestpracticesforadministrators

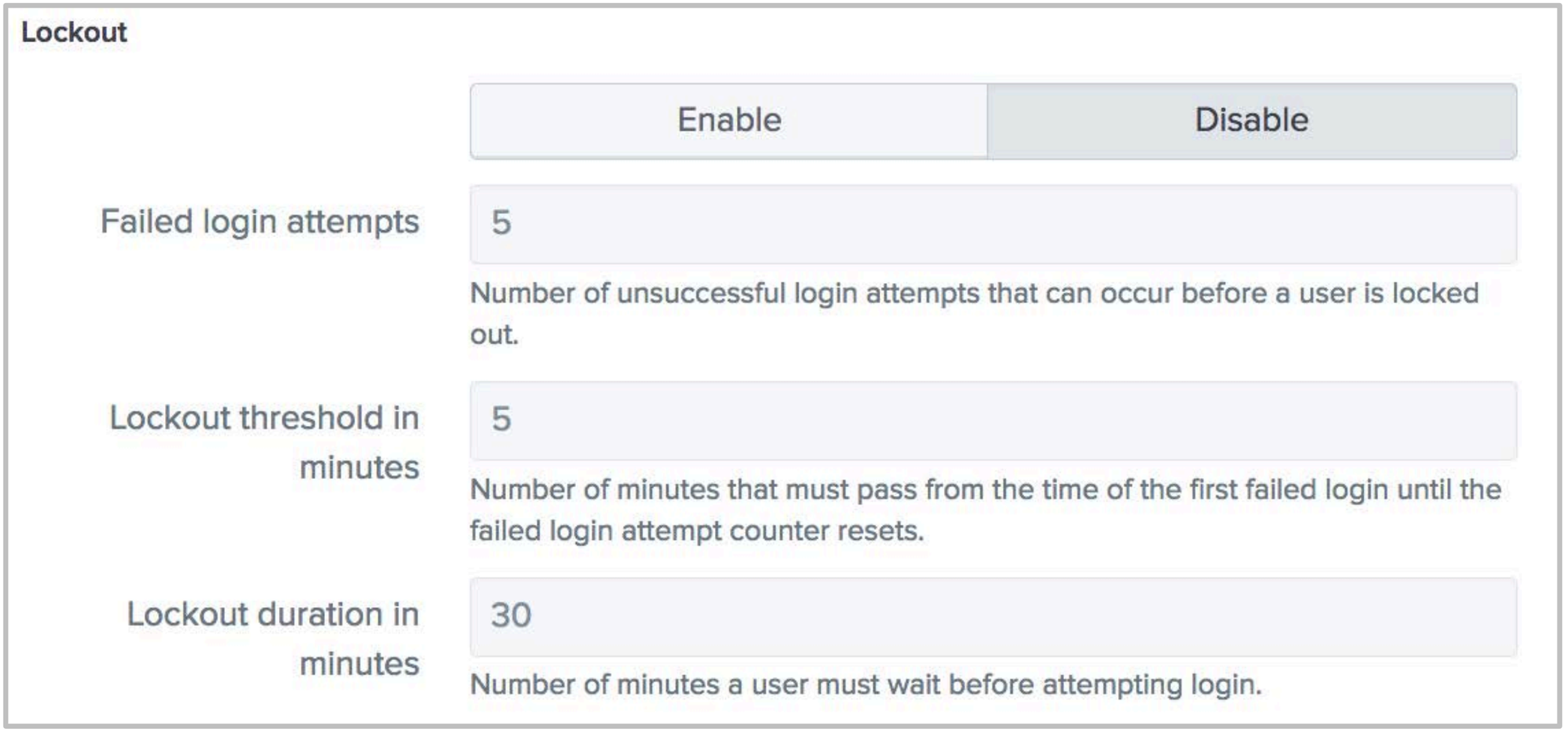
Password Rules



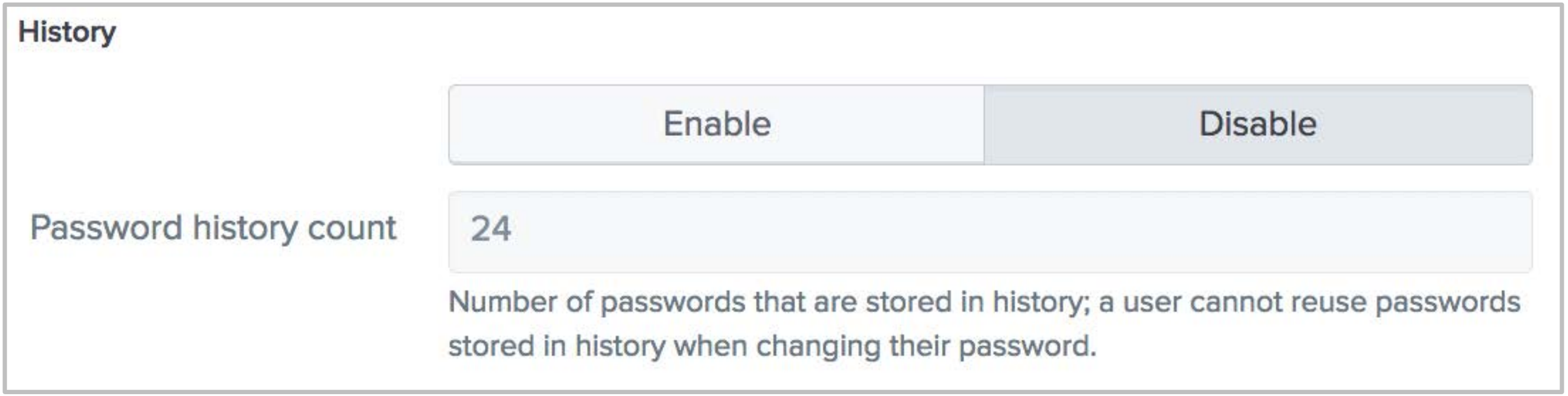
Password Expiration



Password Lockout

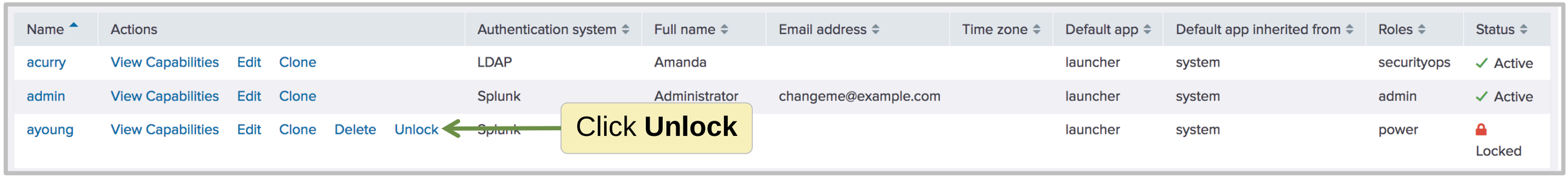


Password History



Unlocking Users

- Users that have been locked out or have forgotten their password, can be unlocked or reset in Splunk Web or CLI
  - Using Splunk Web, select **Settings > User**



  - Using CLI

```
splunk/bin/splunk edit user <lockeduser> -locked-out false
–auth <admin:password>
```

Admin Passwords

- An Admin password is **required** during installation and to start Splunk 7.1 for the first time
  - To create a password during startup

```
splunk/bin/splunk start --accept-license --answer-yes
--no-prompt --seed-passwd <ch@ngeM3>
```

  - To generate a random password during startup

```
splunk/bin/splunk start --accept-license --answer-yes
--no-prompt --gen-and-print-passwd
```

http://docs.splunk.com/Documentation/Splunk/latest/Security/Secureyouradminaccount

Lab Exercise 7 – Add Roles and Users

- **Time:** 10 minutes
- **Tasks:**
- Edit existing roles
- Create a new role and assign it to a user

Module 8: Splunk Authentication Management

Module Objectives

- Overview of integrating Splunk with LDAP
- Overview of integrating Splunk with SAML
- Overview of integrating Splunk with Multifactor Authentication

Splunk Authentication Options

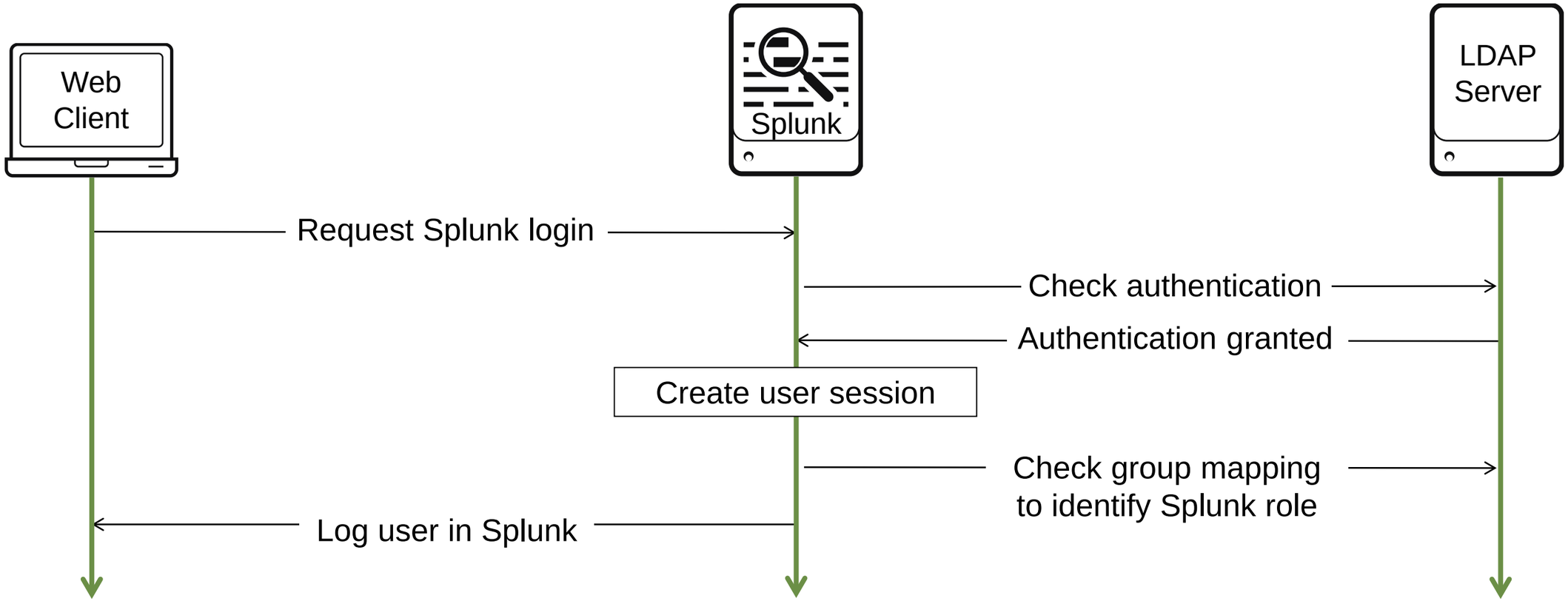
- User accounts can be defined as:
  - Native Splunk accounts
  - LDAP or Active Directory
  - SAML
  - Scripted access to PAM, RADIUS, or other user account systems
- Saves the settings in **`authentication.conf`**

Directory Server Integration

- **Best practice:** integrate Splunk with a directory server
  - Works with multiple LDAP servers, including OpenLDAP and Active Directory
  - You can configure from Splunk Web or CLI
- User accounts stored in directory server
  - Enforces LDAP user account and password policies
  - Users use the same user name and password in Splunk that they use elsewhere
  - LDAP groups must be mapped to Splunk roles
    - Or, this can be done manually in Splunk

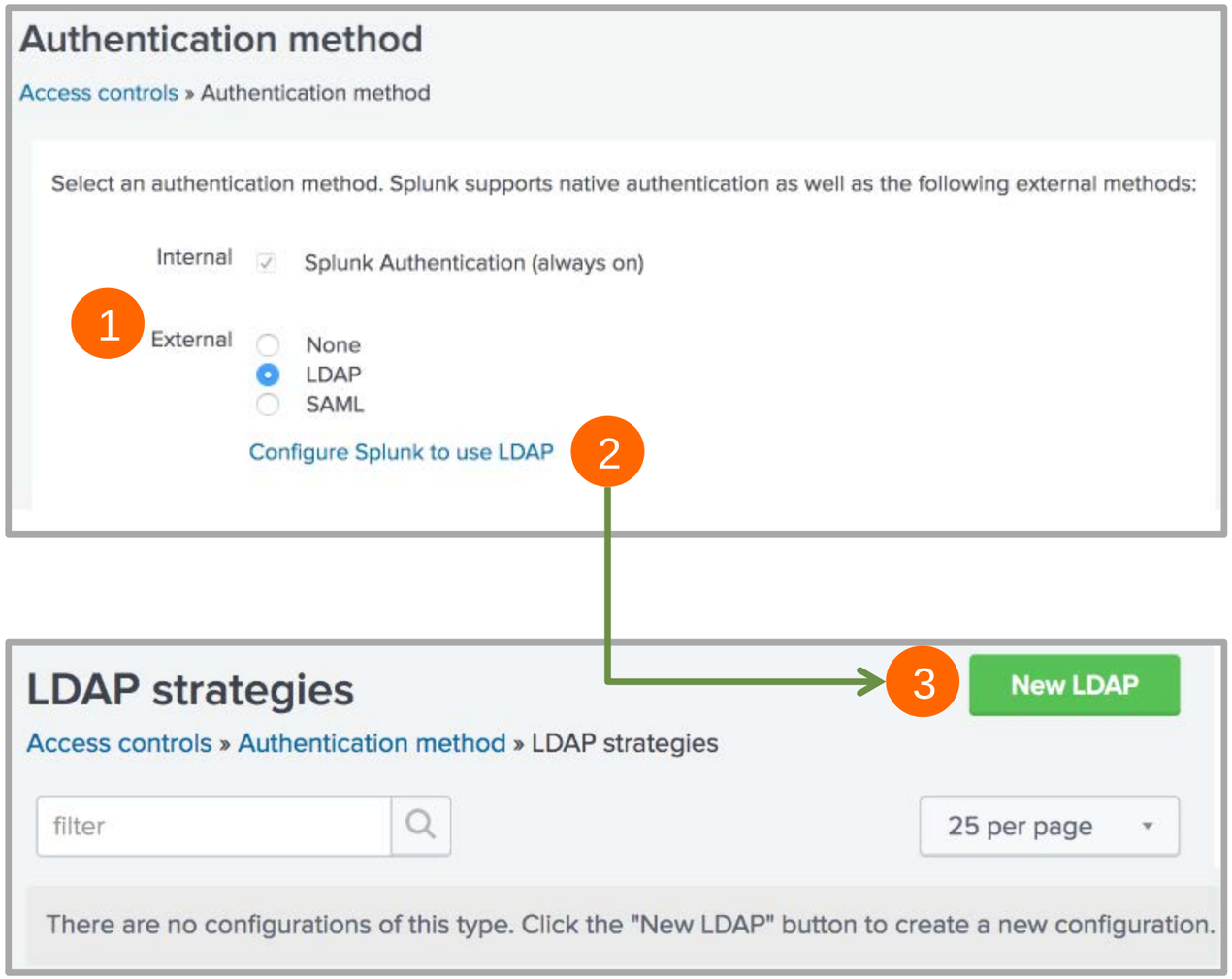
LDAP Authentication

LDAP maintains the user credentials - user ID and password, plus other information - centrally and handles all authentication



Creating an LDAP Strategy

1. Select **LDAP**
2. Click **Configure Splunk to use LDAP**
   - The list of current LDAP strategies displays
     - A strategy is a connection to one or more LDAP nodes on an LDAP server
   - Can define multiple LDAP servers
3. Click **New** to add a new LDAP strategy
   - Name the strategy and fill out the form

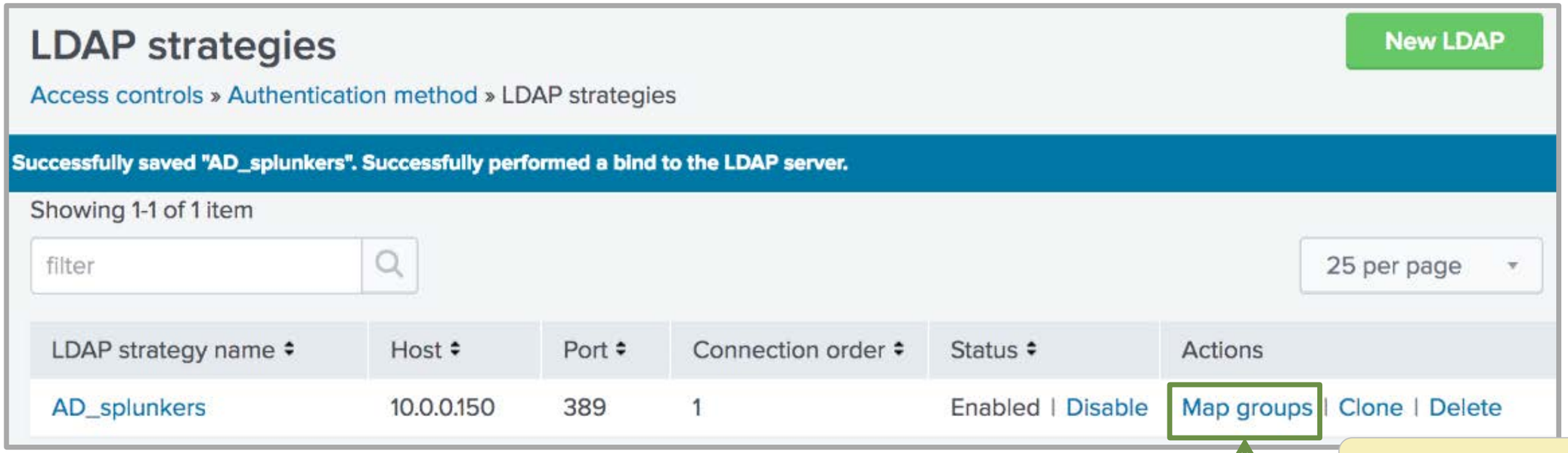


LDAP Strategy Settings

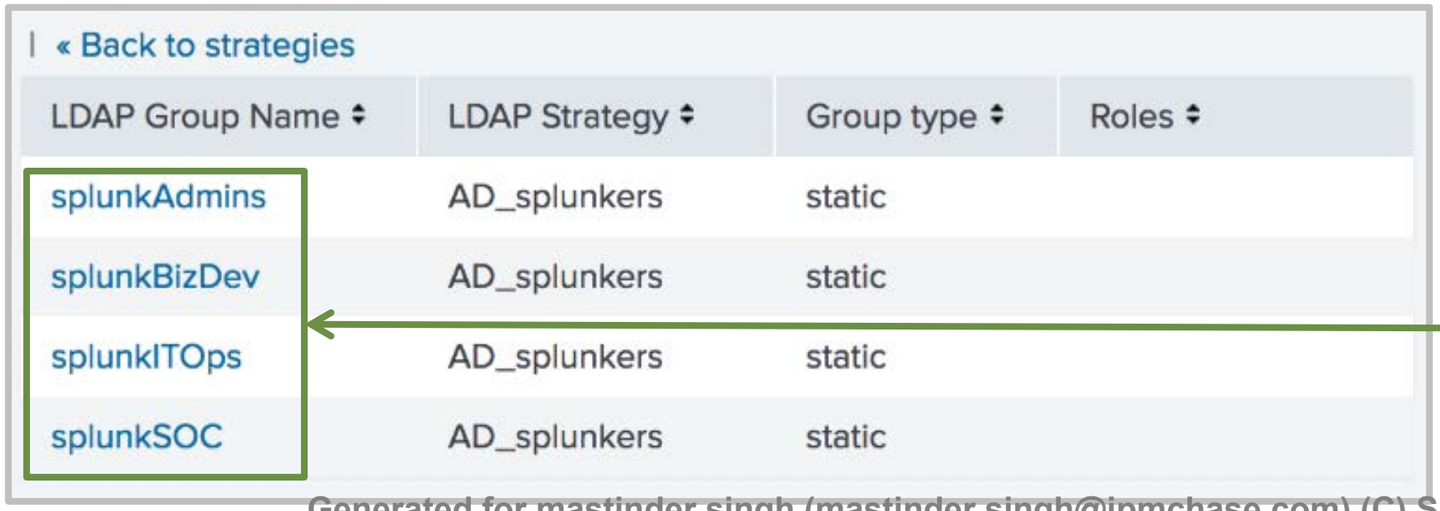
- Normally the configuration is based on the information given to you by the LDAP administrators
  - LDAP connection settings
  - User settings
    - Determine which part of the LDAP directory stores Splunk users
  - Group settings & Dynamic group settings
    - Determine which node in the directory contains your group definitions
  - Advanced settings

```
• host = 10.0.0.150
• port = 389
• SSLEnabled = 0
• bindDN = adsuser@buttercupgames.local
• bindDNpassword = <some_hashed_pw>

• userBaseDN =
  OU=splunk,DC=buttercupgames,DC=local
• userNameAttribute = samaccountname
• realNameAttribute = displayname

• groupBaseDN =
  OU=splunk,DC=buttercupgames,DC=local
• groupNameAttribute = cn
• groupMemberAttribute = member
• nestedGroups = 0
• groupMappingAttribute = dn

• network_timeout = 20
• sizelimit = 1000
• timelimit = 15
```

Mapping LDAP Groups to Roles

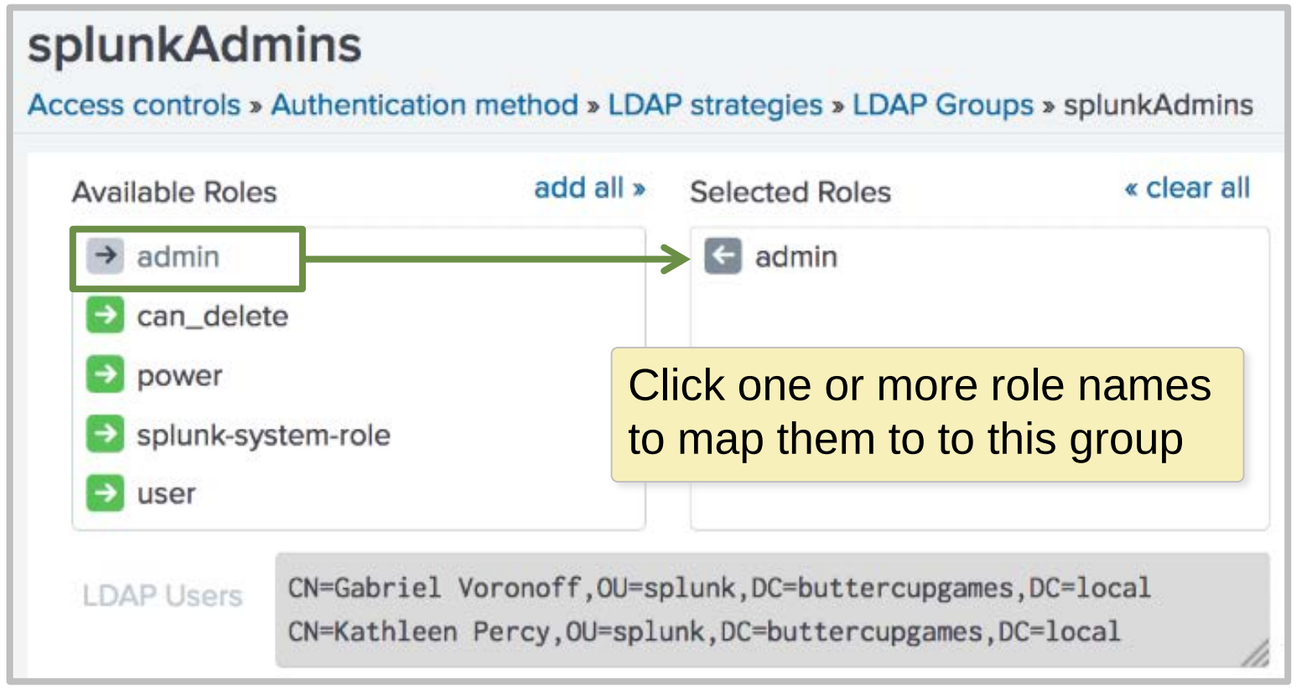


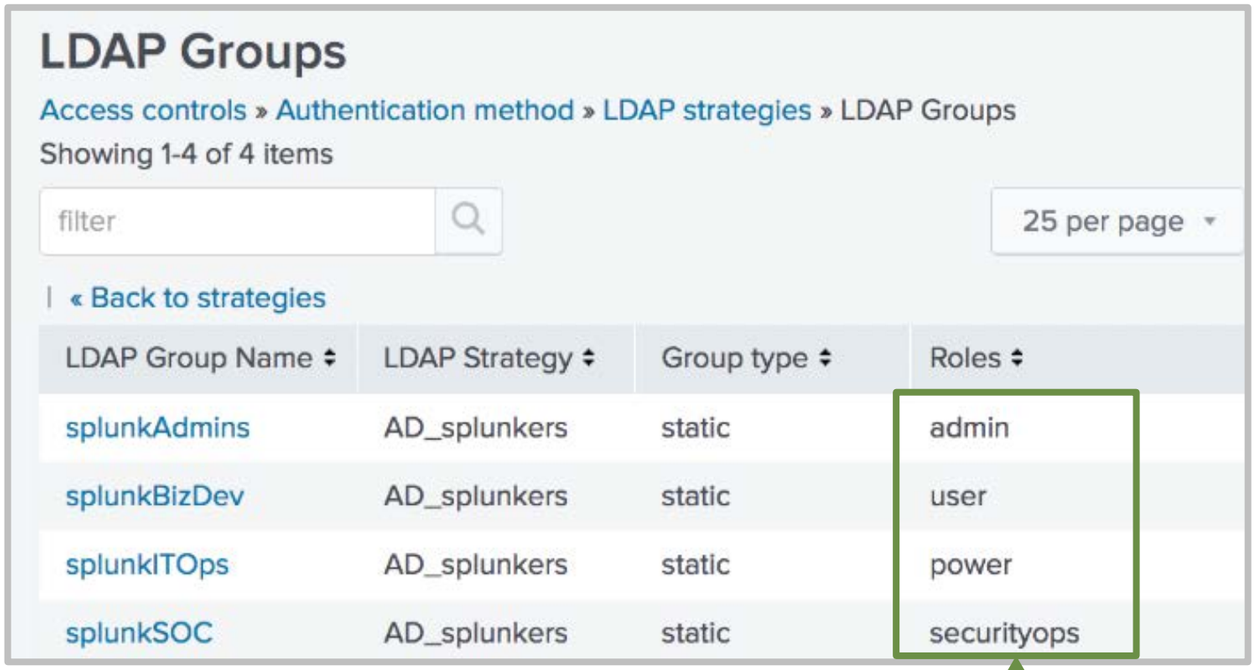
Select **Map groups** to define relationships between LDAP groups and Splunk roles



Click a LDAP group name to map it to one or more Splunk roles

Mapping LDAP Groups to Roles (cont.)

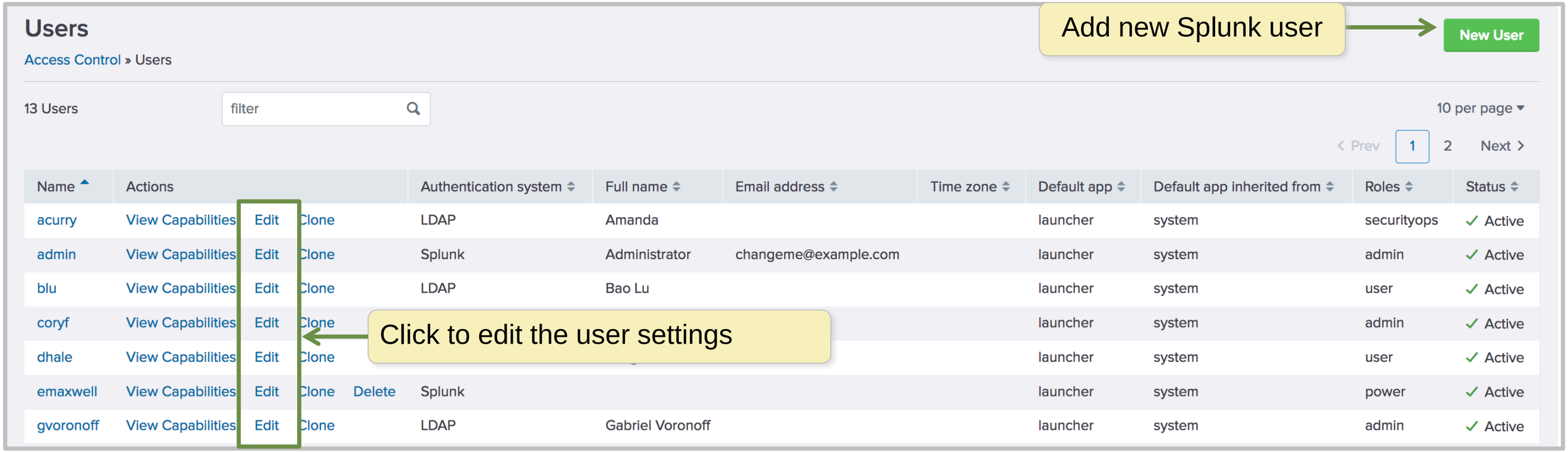




- Not all groups must be mapped
- Mappings can be changed at any time
  - The LDAP server is rechecked each time a user logs into Splunk
  - A user cannot log in unless they have a Splunk role

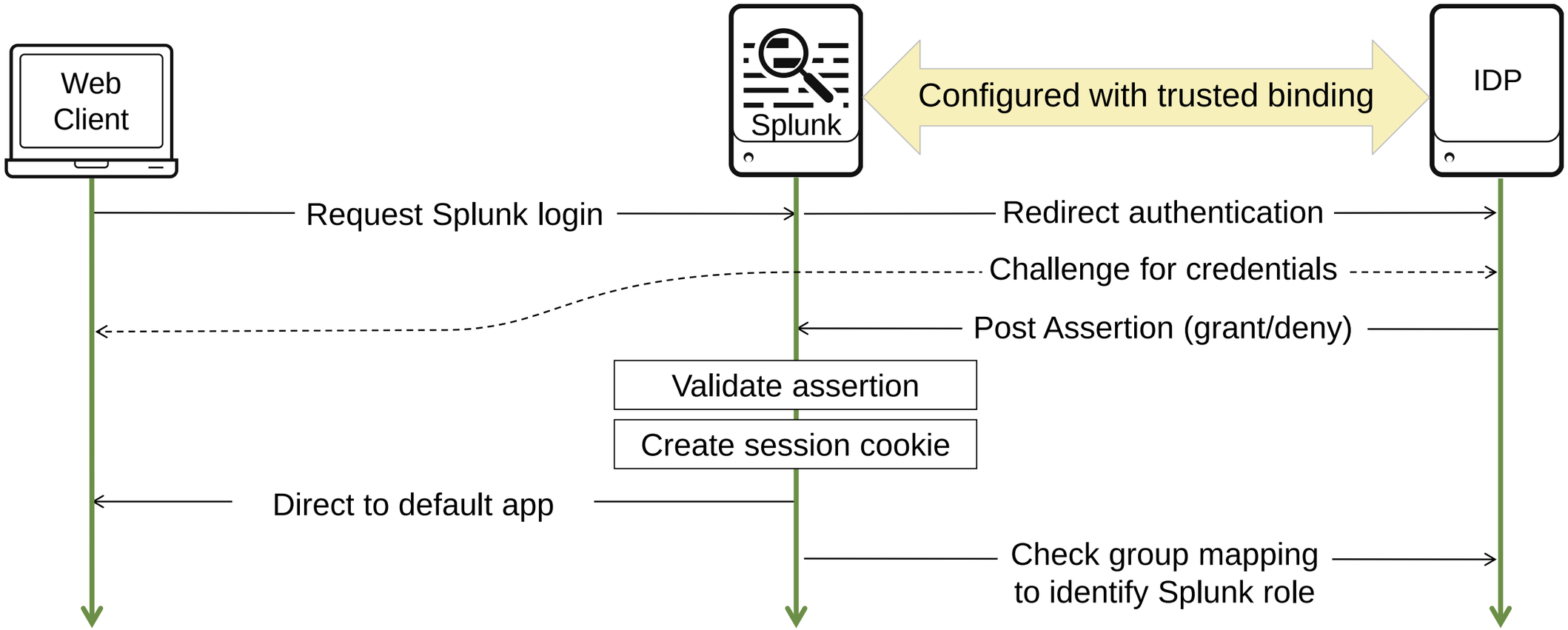
Managing Users in Splunk

- Splunk native users can be edited or deleted
- Only time zone and default app can be changed on LDAP or other users



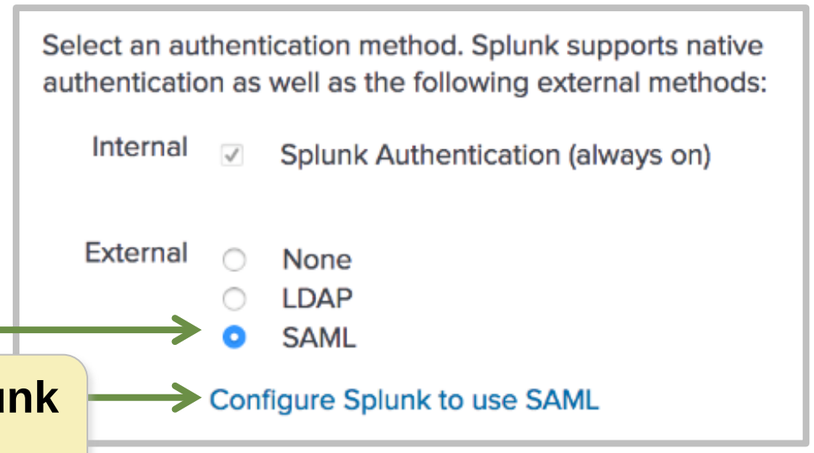
SAML 2.0 Single Sign On

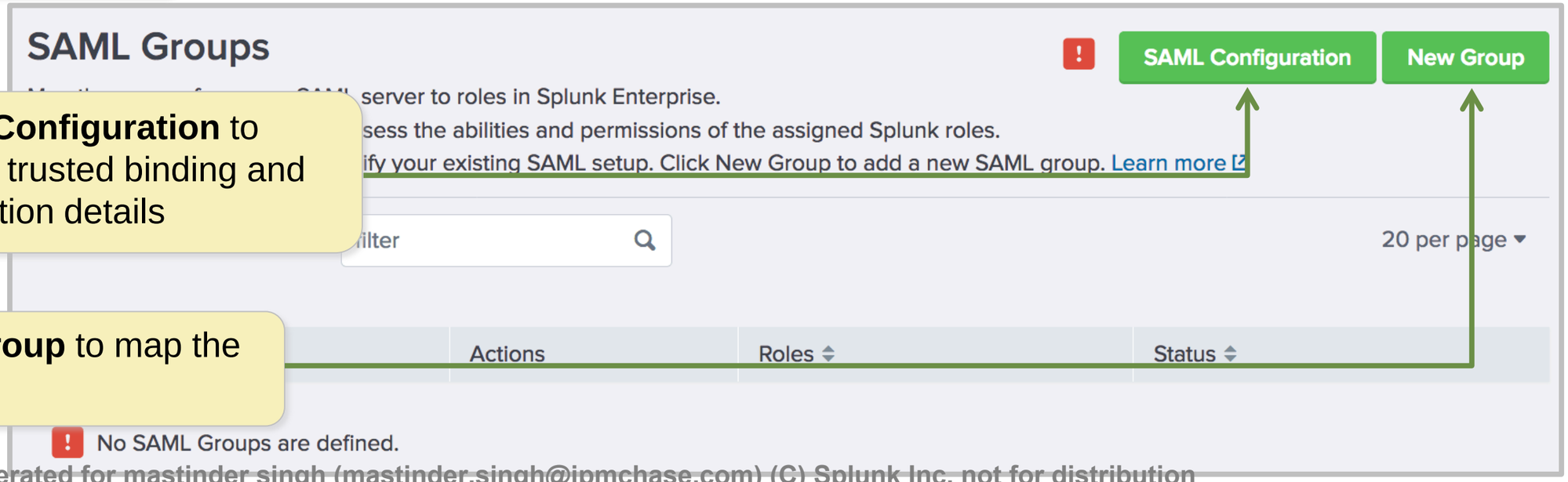
Identity provider (IDP) maintains the user credentials and handles authentication



Configuring SAML

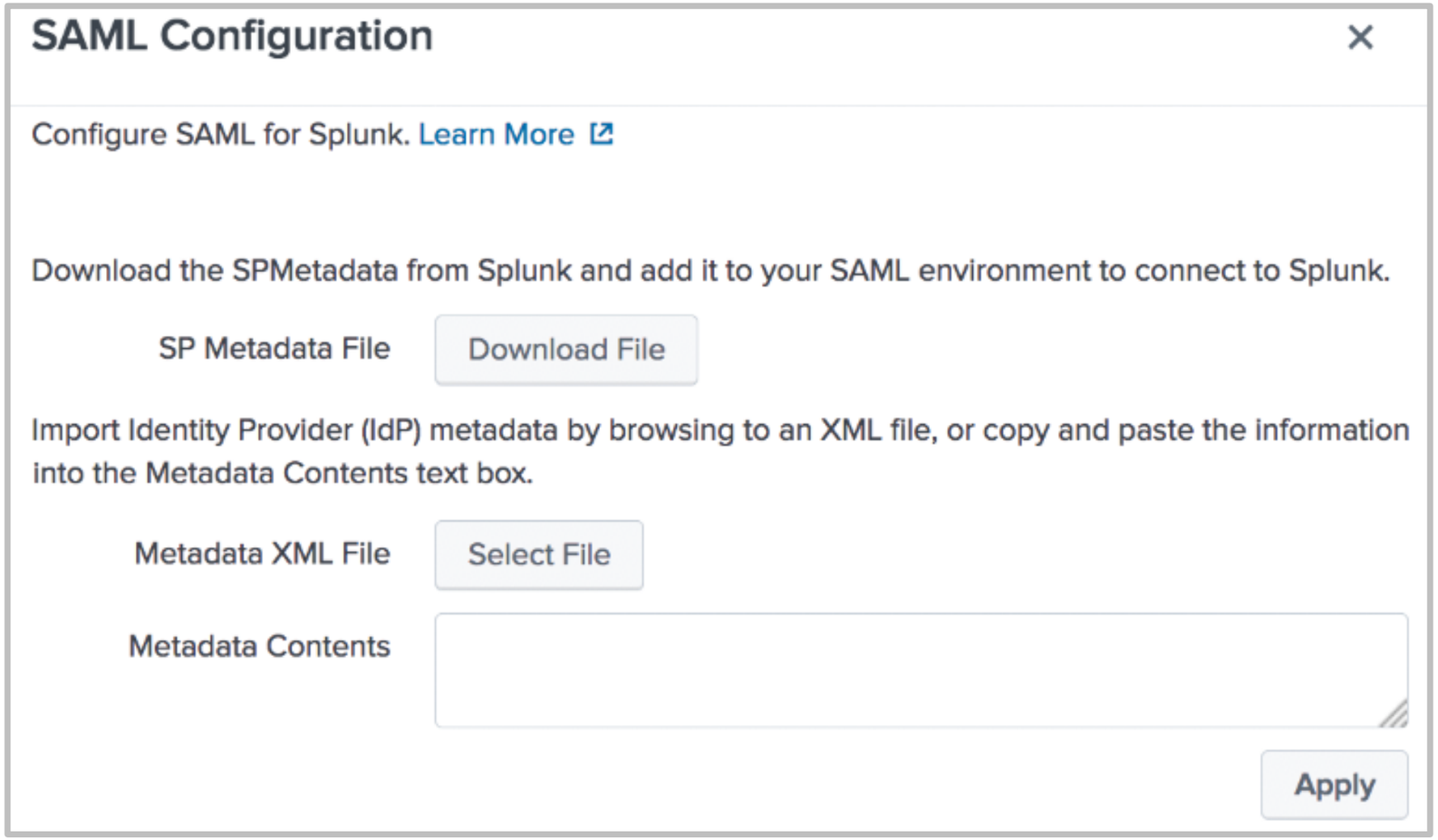
1. Click **SAML**
2. Click **Configure Splunk to use SAML**
3. Click **SAML Configuration** to configure the trusted binding and other connection details
4. Click **New Group** to map the new roles





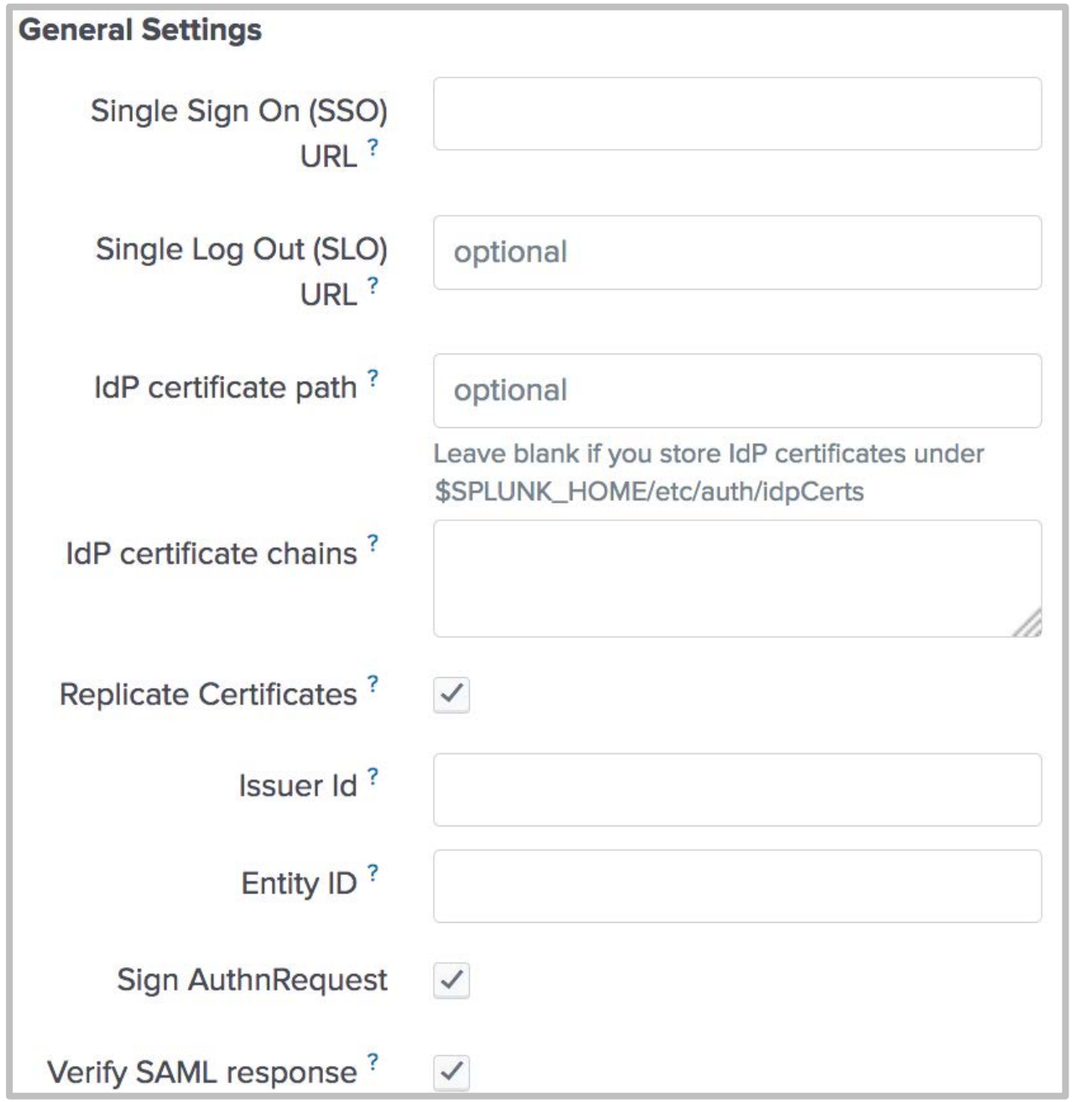
Configuring SAML – Splunk Settings

- Download the Splunk Service Provider Metadata file
- Import the IdP metadata into Splunk



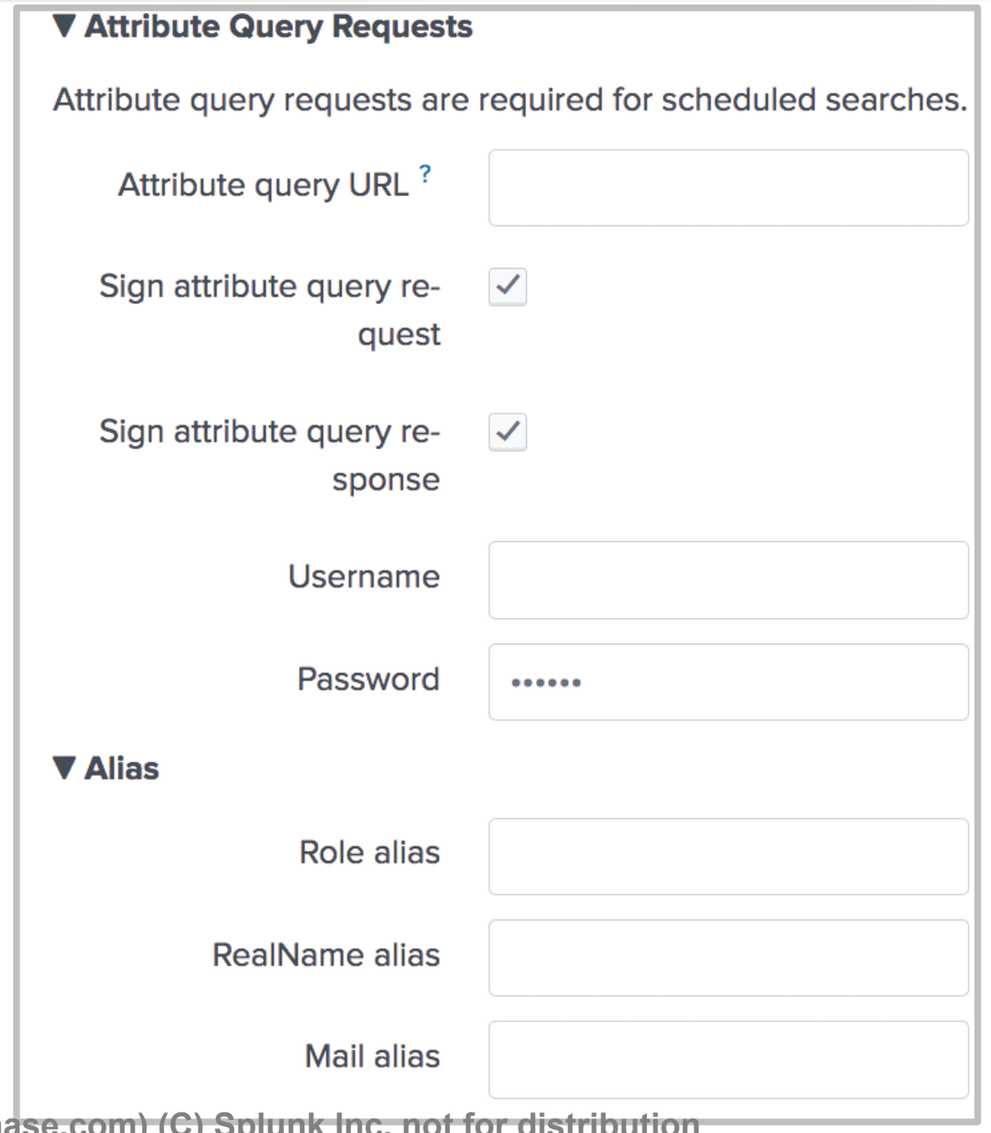
Configuring SAML – General Settings

- Contact your SAML administrator for the following configuration information:
  - Sign on/Log off URLs
    - These are the protected endpoints on the IdP which Splunk sends authentication requests
  - Certificate information



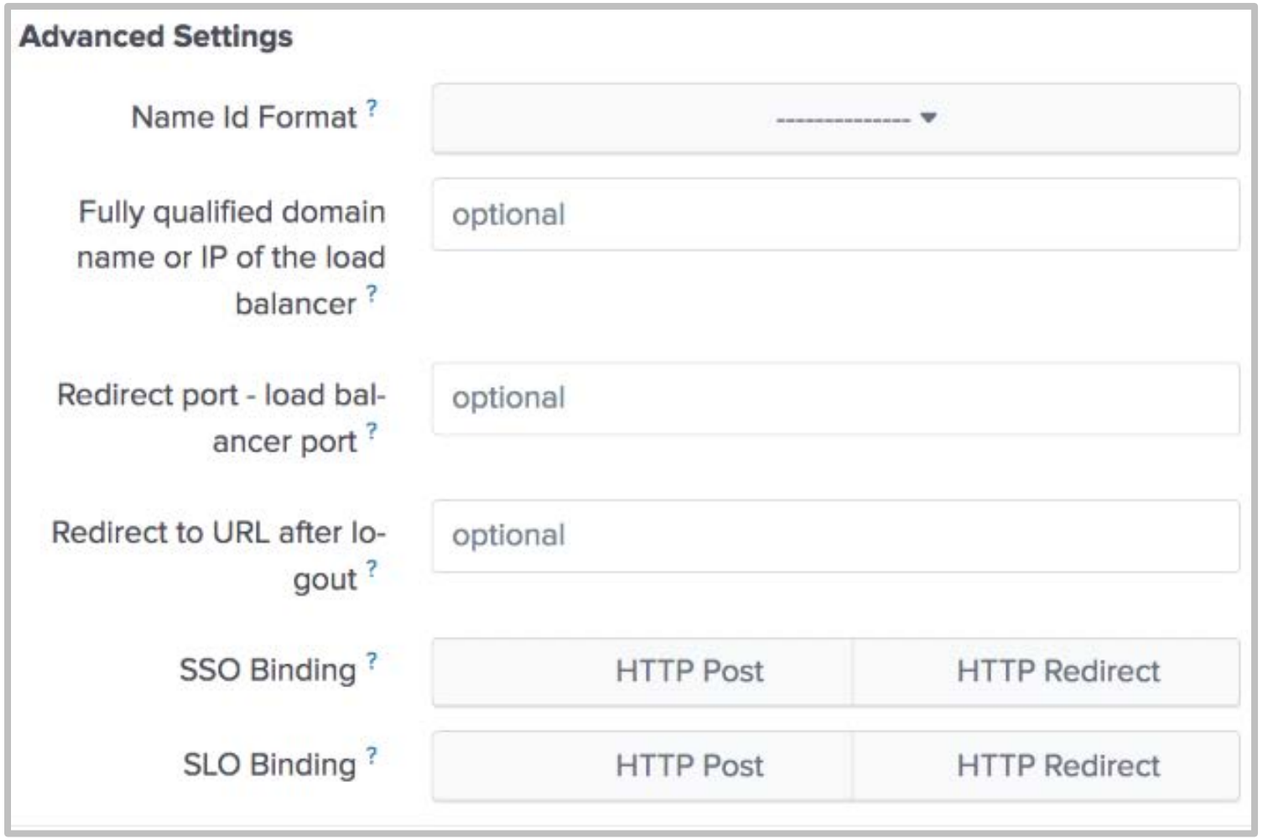
Configuring SAML – Query and Alias Settings

- Attribute Query Requests
  - Attribute query URL
    - Endpoint on the IdP to which queries over SOAP are sent
  - Sign attribute query request/response
    - Username/Password
- Aliases
  - Role
  - RealName
  - Mail



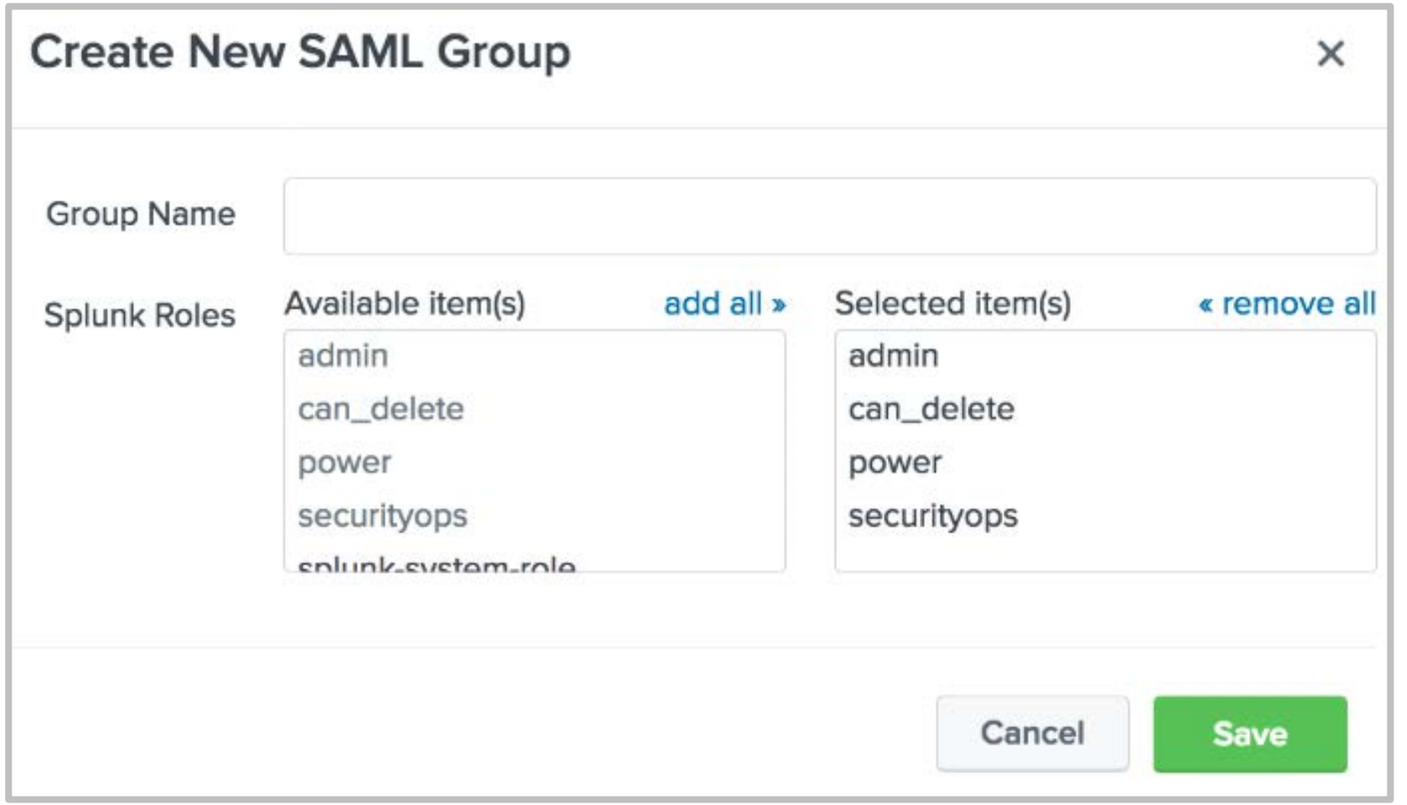
Configuring SAML – Advanced Settings

- Advanced Settings
  - Name Id Format
    - Leave this empty or pick the correct format configured on the IdP from the drop down list
  - Domain name/IP of load balancer
  - Redirect/load balancer port
  - Redirect URL after logout
  - SSO/SLO Binding
    - Protocol binding used for the SAML sign on/log off requests sent to the IdP



Creating SAML Groups

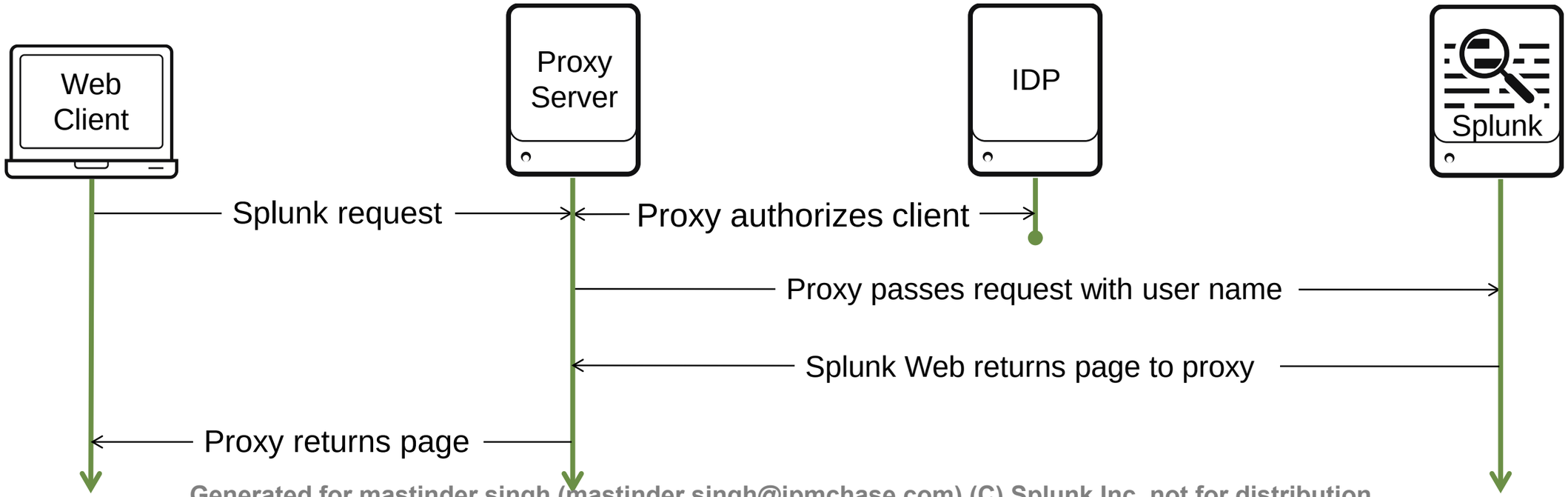
- Authorize groups on your SAML server to log into Splunk by mapping them to user roles
- Multiple groups can be mapped to a single user role
- A user must have a Splunk role in order to log in



Single Sign On with Reverse Proxy

- Splunk SSO allows you to use a web proxy to handle Splunk authentication
  - Authentication is moved to a web proxy, which passes along authentication to Splunk Web
  - Web proxy can use any method to authenticate (IDP in example)

docs.splunk.com/Documentation/Splunk/latest/Security/HowSplunkSSOworks



Scripted Authentication

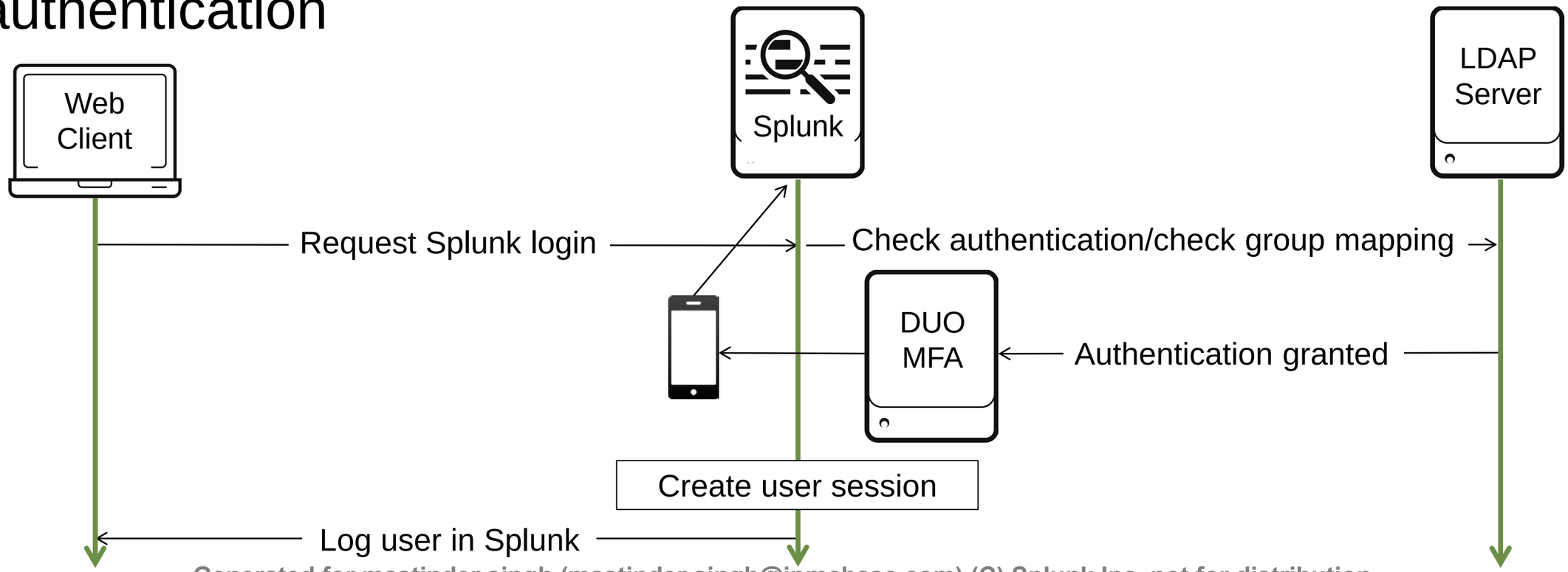
- There are other types of authentication systems that Splunk can integrate with using scripts
- For the most up-to-date information on scripted authentication, see the README file in:

  `SPLUNK_HOME/share/splunk/authScriptSamples/`

  - The directory includes sample authentication scripts

Duo Multi Factor Authentication

- Splunk supports Duo Security two-factor authentication logins
- LDAP maintains the user credentials including user ID and password, plus other information centrally and handles all authentication



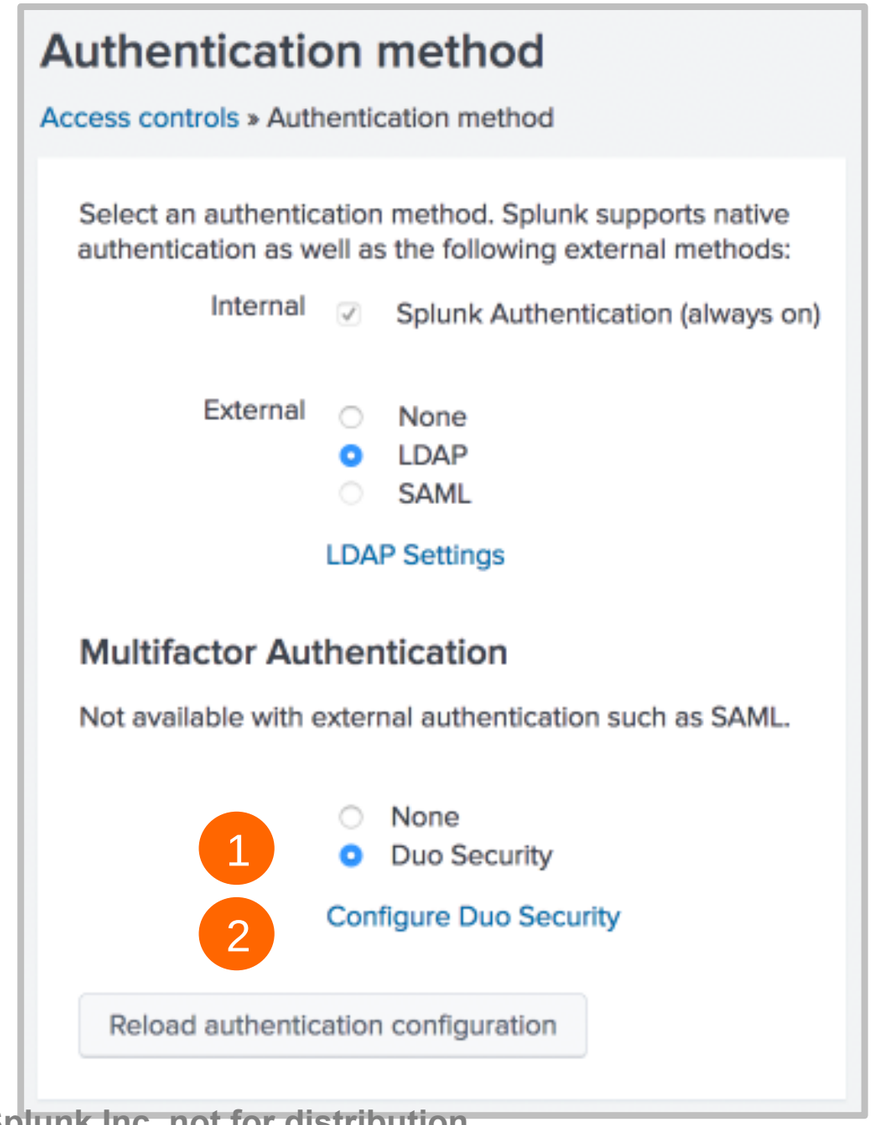
Configuring Duo MFA

Create an account for your Splunk configuration on the Duo website

Note: see https://duo.com

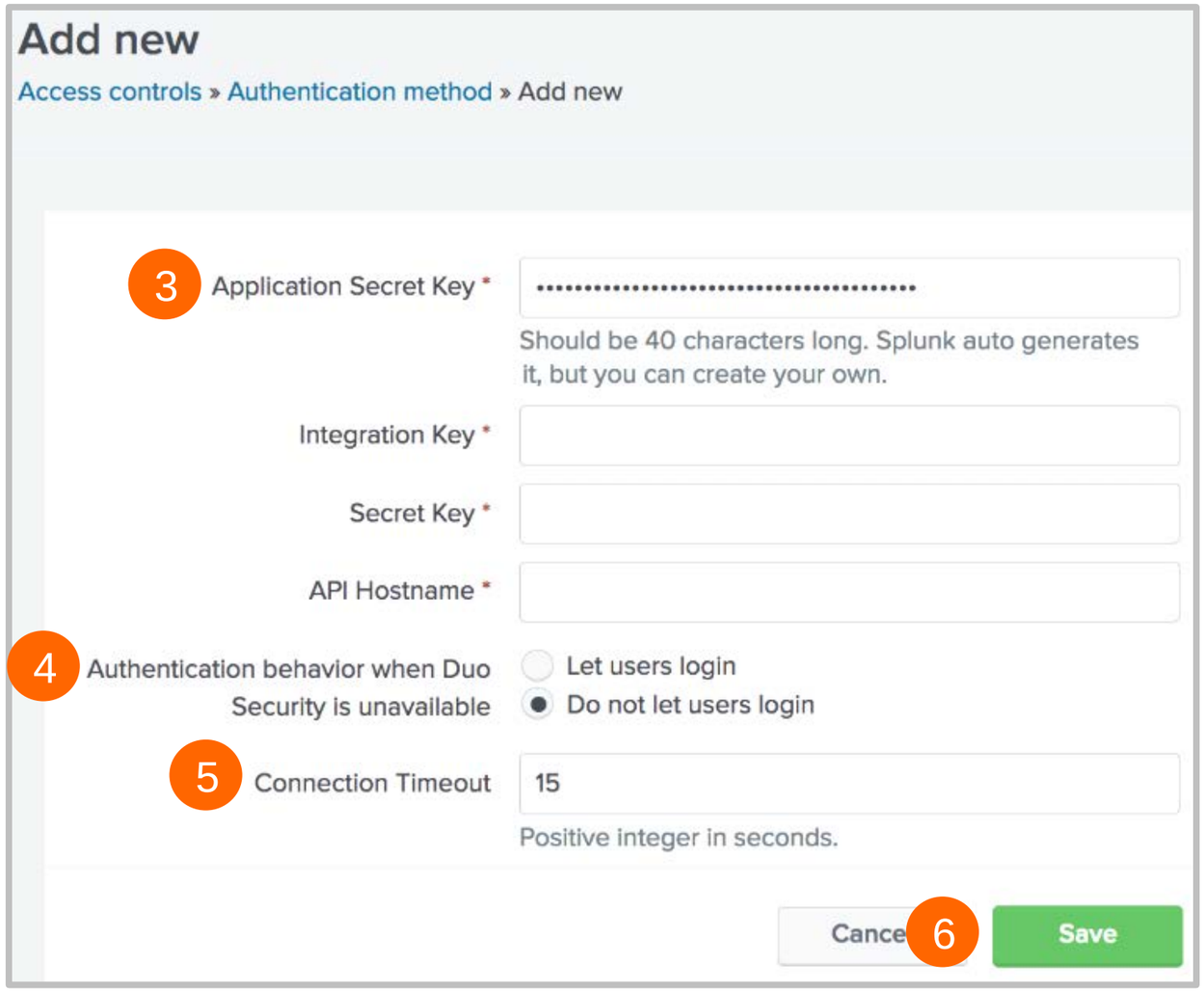
From your search head:

1. Select **Duo Security**
2. Click **Configure Duo Security**



Configuring Duo MFA (cont.)

3. Enter the following info (provided by the Duo administrator)
   - Application Secret Key
   - Integration Key
   - Secret Key
   - API Hostname
4. Authentication behavior if Duo is unavailable
5. Connection Timeout (in seconds)
6. Save



Lab Exercise 8 – Configure LDAP Authentication

- **Time**: 10 minutes
- **Tasks**:
- Configure Splunk to use LDAP authentication
- Map LDAP groups to Splunk roles
- Verify the configurations

- Lab notes:
  - **`open.sesam3`** is the password for all LDAP accounts

Module 9: Configuring Basic Forwarding

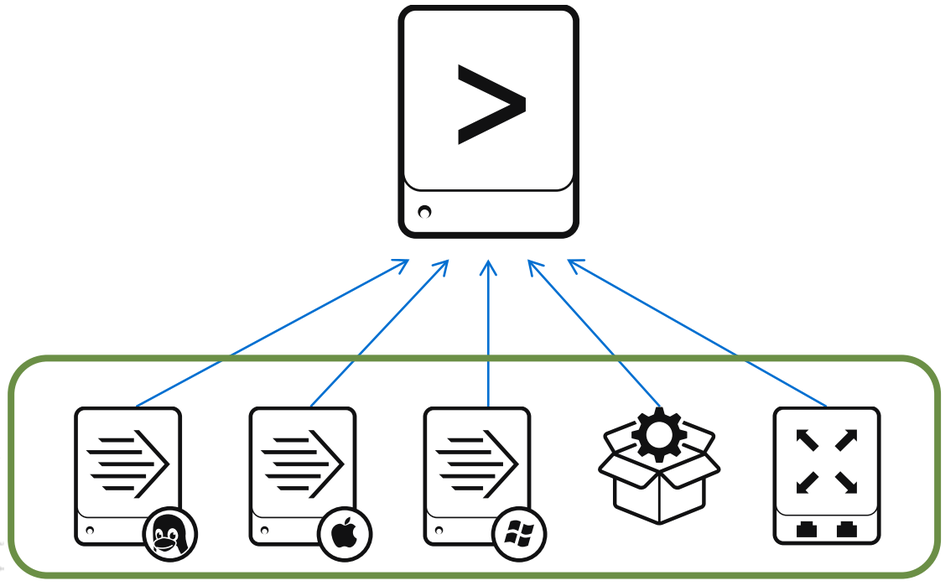
Module Objectives

- Identify forwarder configuration steps
- List Splunk forwarder types
- Configure the forwarder
- Identify forwarder configuration files

Got Data?

- Computers
- Network devices
- Virtual Machines
- Internet of Things (IoT)
- Communication devices
- Sensors
- Databases
- ***Any source***

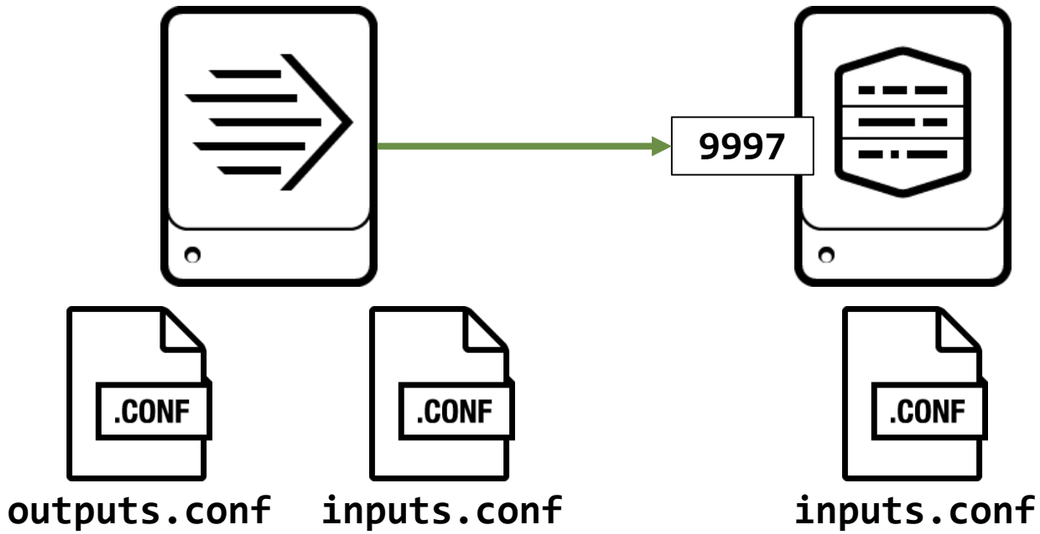
- Logs
- Configurations
- Messages
- Call Detail Records
- Clickstream
- Alerts
- Metrics
- Scripts
- Changes
- Tickets
- ***Any data***



Indexes any data from any source

Forwarders and Indexers

- In a production environment
  - Splunk indexers run on dedicated servers
  - The data you want is on remote machines
- Install Splunk **forwarders** on the remote machines to
  - Gather the data
  - Send it across the network to the Splunk indexer(s)
- Indexers listen on a **receiving port** for the forwarded data



Deployment Server/Forwarder Management

- In larger or production environments, forwarders can be managed remotely
- Splunk Deployment Server provides a Forwarder Management interface
  - A centralized configuration management tool to manage forwarder configuration
  - Allows forwarders to be managed in groups (server classes)
- In this class, we will set up a single forwarder manually, for testing
- Deployment server is discussed in detail in the Data Administration class

Forwarder Configuration Steps

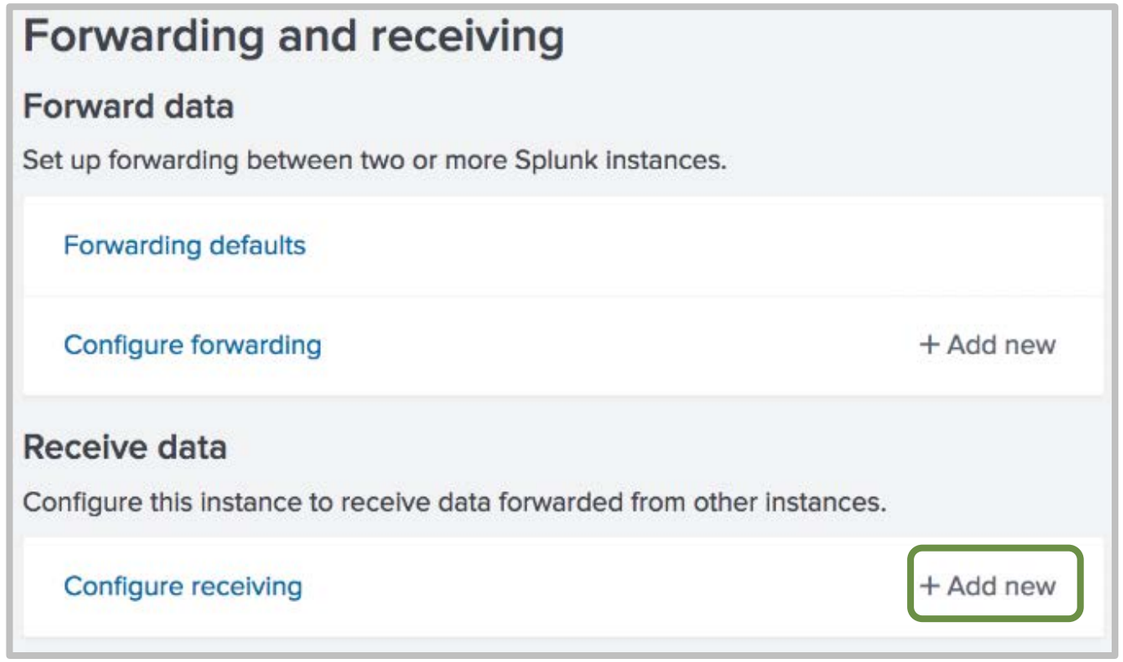
1. Set up a receiving port on each indexer
   - It is only necessary to do this once
2. Download and install Universal Forwarder
3. Set up forwarding on each forwarder
   - Either manually or using Deployment Server
4. Add inputs on forwarders, using one of the following:
   - Forwarder management
   - CLI
   - Edit `inputs.conf` manually

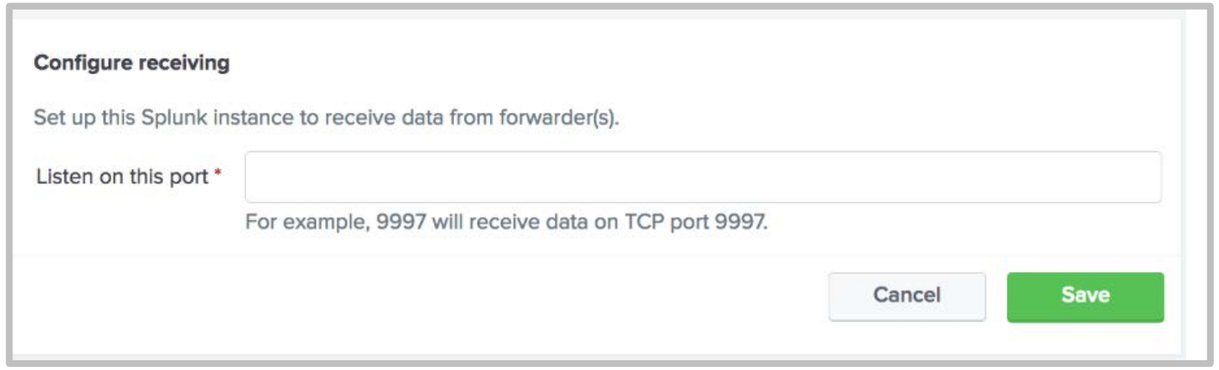
Configure the Receiving Port on Each Indexer

- Using Splunk Web:
  1. Select **Settings > Forwarding and receiving**
  2. Next to **Configure receiving**, select **Add new**
  3. Enter a port number and click **Save**
- Using CLI:

  `splunk enable listen <port>`
- The configuration is saved in **`inputs.conf`** as:

  `[splunktcp://portNumber]`



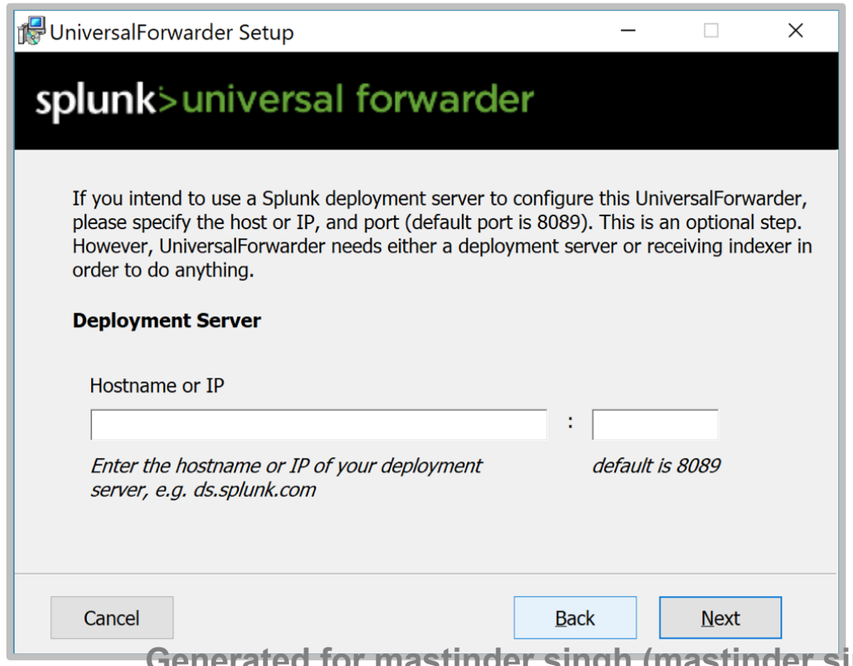


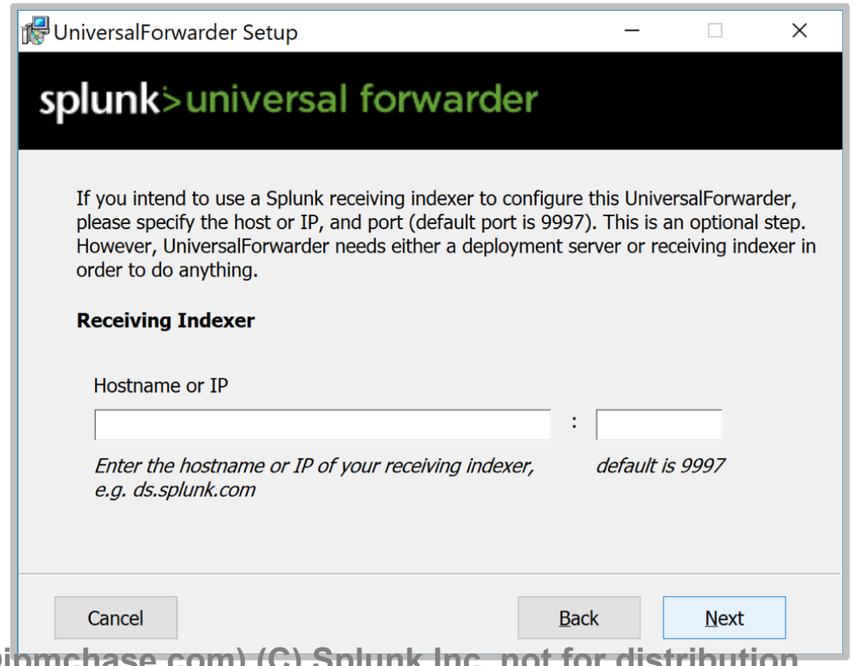
Installing Universal Forwarder

- *NIX: unpack the **`.tgz`** or **`.tgz.Z`** in the desired location
- Windows: execute the **`.msi`** or use the command line
  - Installed as a service
- **`SPLUNK_HOME`** is the installation directory, defaults to
  `/opt/splunkforwarder` or
  `c:\Program Files\SplunkUniversalForwarder`
- Same **`splunk`** command-line interface in **`SPLUNK_HOME/bin`**
  - Same commands for start/stop, restart, etc.
  - A password will have to be defined for the **admin** account
- When installing large numbers of forwarders, use an automated method

Using the Interactive Windows Installer

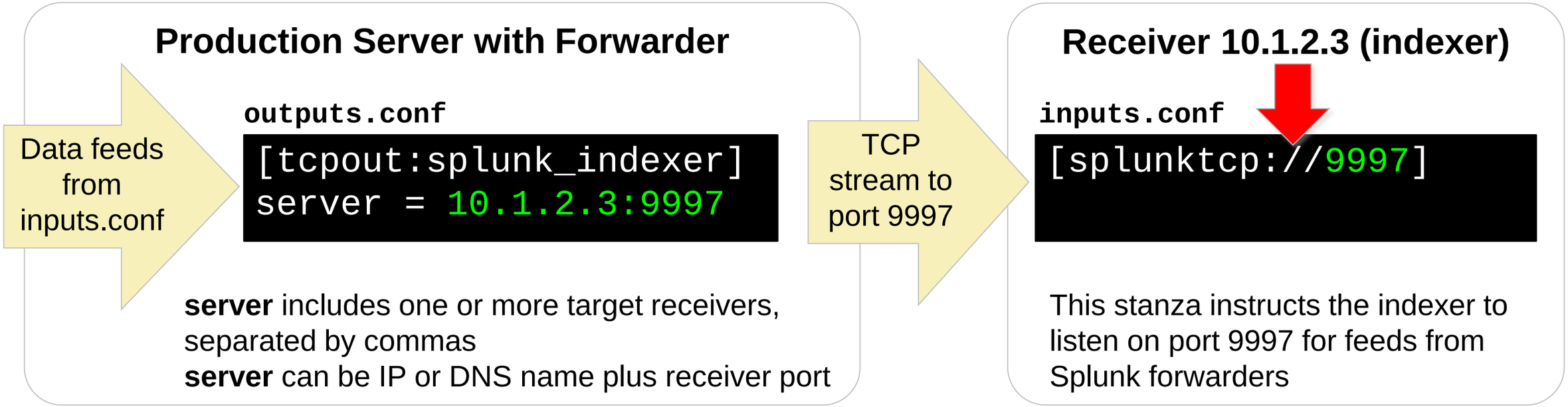
- Most forwarder settings can be configured using the installer wizard
  - Can run as a domain user without the domain user local administrator privileges
- CLI installation is available for scripted installations
  docs.splunk.com/Documentation/Forwarder/latest/Forwarder/InstallaWindowsuniversalforwarderfromthecommandline





Forwarder Configuration Files

- Forwarders require **`outputs.conf`**
  - **`outputs.conf`** points the forwarder to the receiver(s)
  - Can specify additional options for load balancing, SSL, compression, alternate indexers, and indexer acknowledgement



Defining Target Indexers on the Forwarder

- Execute on the forwarder:
  `splunk add forward-server indexer:receiving-port`
  - For example, **`splunk add forward-server 10.1.2.3:9997`** configures the **`outputs.conf`** as:

```
[tcpout]
defaultGroup = default-group

[tcpout:default-group]
server = 10.1.2.3:9997

[tcpout-server://10.1.2.3:9997]
```

http://docs.splunk.com/Documentation/Forwarder/latest/Forwarder/Configureforwardingwithoutputs.conf

Testing the Connection

- After running **`splunk add forward-server`**, the forwarder should be communicating with the indexer
  - Splunk forwarder logs are automatically sent to the indexer's **_internal** index
- To check for successful connection:
  - On the indexer, search **`index=_internal host=`***`forwarder_hostname`*
  - On the indexer, run **`splunk display listen`**
  - On the forwarder, run **`splunk list forward-server`**
- To remove the target indexer setting:
  - On the forwarder, run **`splunk remove forward-server`** *`indexer:port`*

Lab Exercise 9 – Basic Forwarder Configuration

- **Time**: 20 minutes
- **Tasks**:
- Set up your Splunk indexer as the receiver
- Use CLI to configure and prepare your forwarder to send event data to the receiver
- Confirm the forwarder connection with the MC
- View the contents of the **`outputs.conf`** file on the forwarder and the **`inputs.conf`** file on the indexer

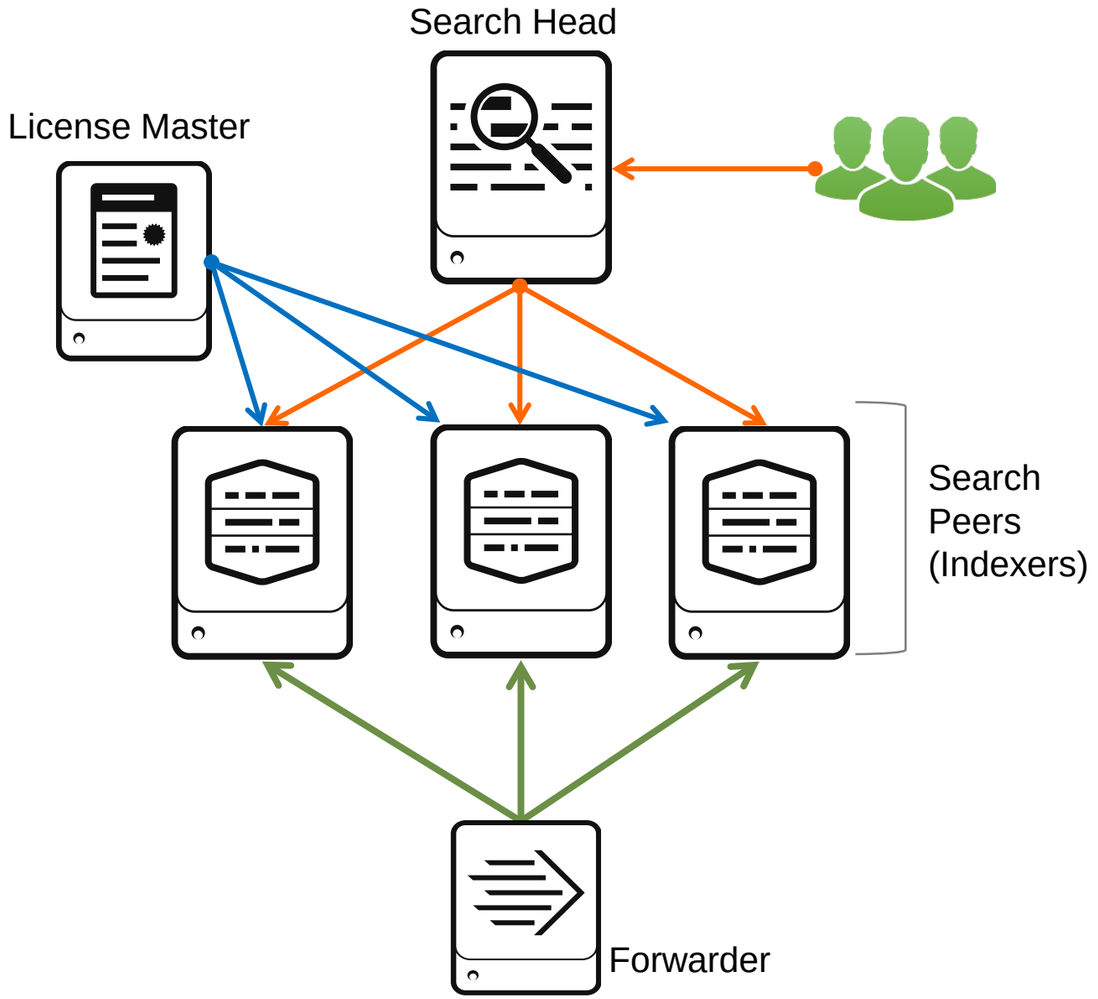
Module 10: Distributed Search

Module Objectives

- Describe how distributed search works
- Explain the roles of the search head and search peers
- Configure a distributed search group
- List search head scaling options

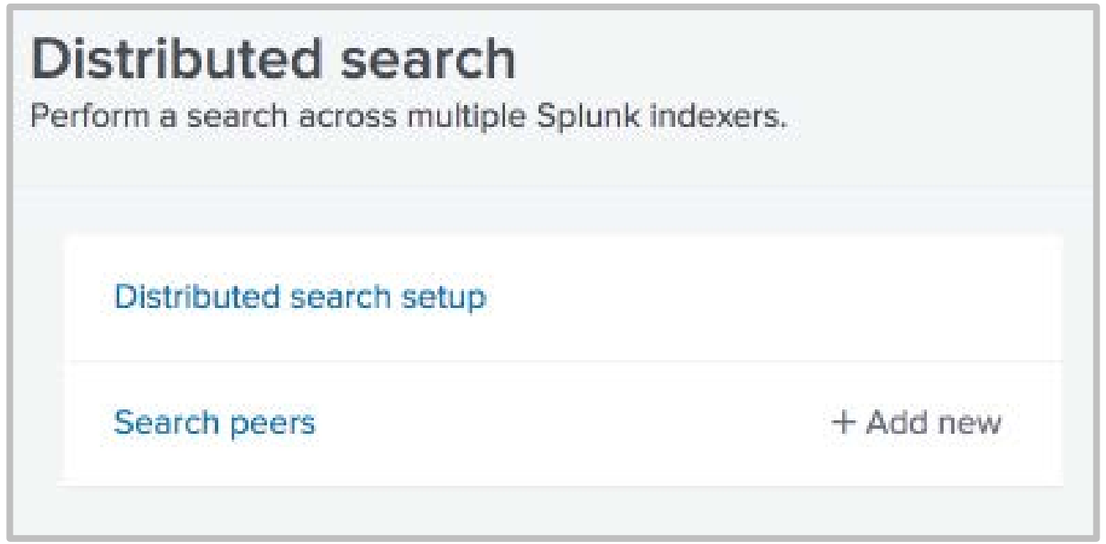
Distributed Search

- Production servers with universal forwarders send data to indexers
- Indexers (peers) store their portion of the data
- Users log on to the search head and run reports
  - The search head dispatches searches to the peers
  - Peers run searches in parallel and return their portion of results
  - The search head consolidates the individual results and prepares reports



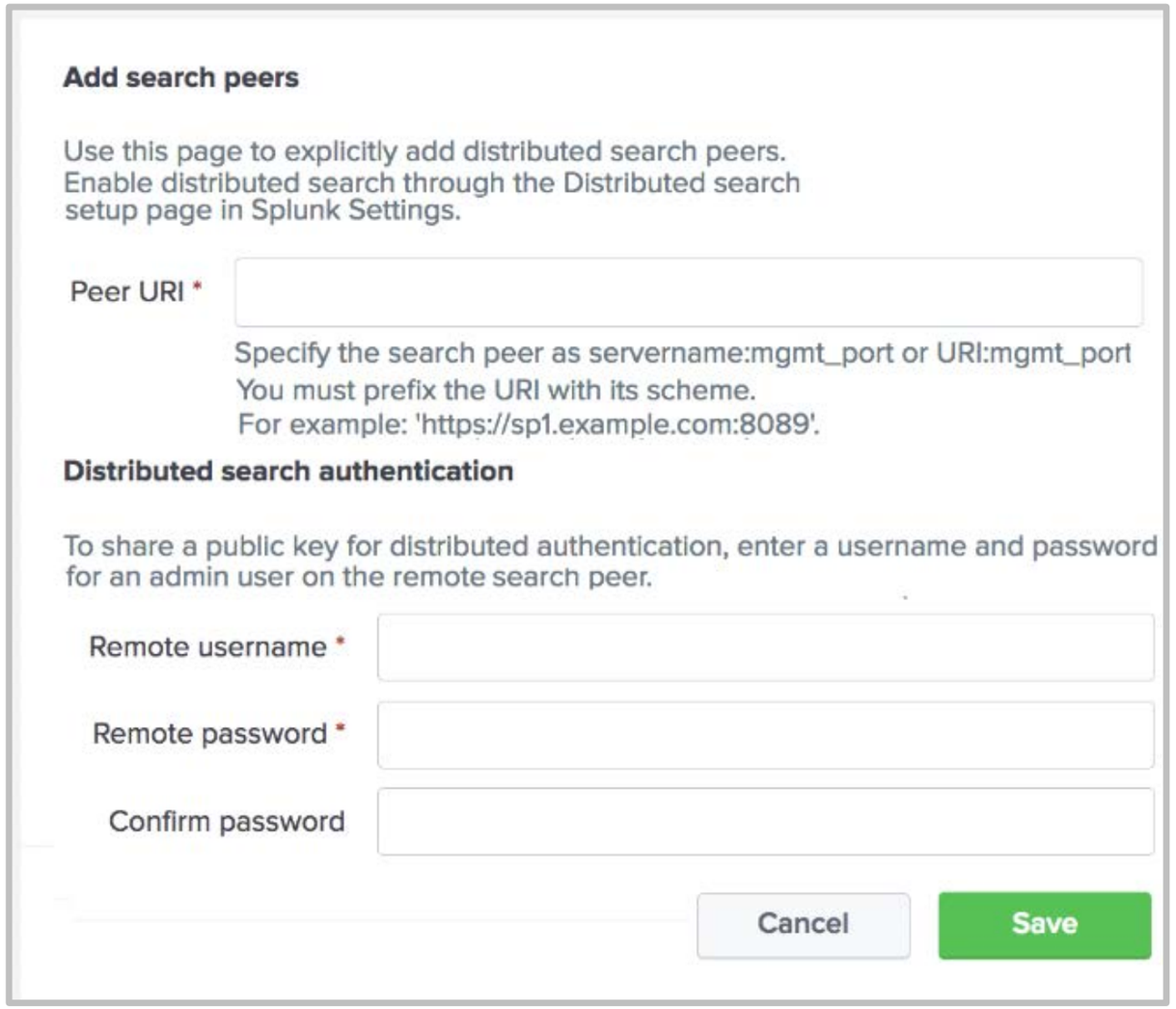
Setting Up Distributed Search

- Install Splunk on each search head and peers (indexers)
- Set up the same indexes on all peers
- All search heads and peers should use a license master
- Add a user to each peer with a role that has the **`edit_user`** capability
  - Used only for authenticating a search head to the peers
- On the search head, configure search peers by selecting:
  Settings > Distributed search
  - Distributed search is turned **on** by default, so just add search peers



Adding Search Peers

- Select **Settings > Distributed search > Search peers > Add new**
- Enter the **`servername:port`** for a search peer
- Enter a username and password of an account on the search peer
  - The account must have the **`edit_user`** capability
  - You should create an account on each peer for this purpose



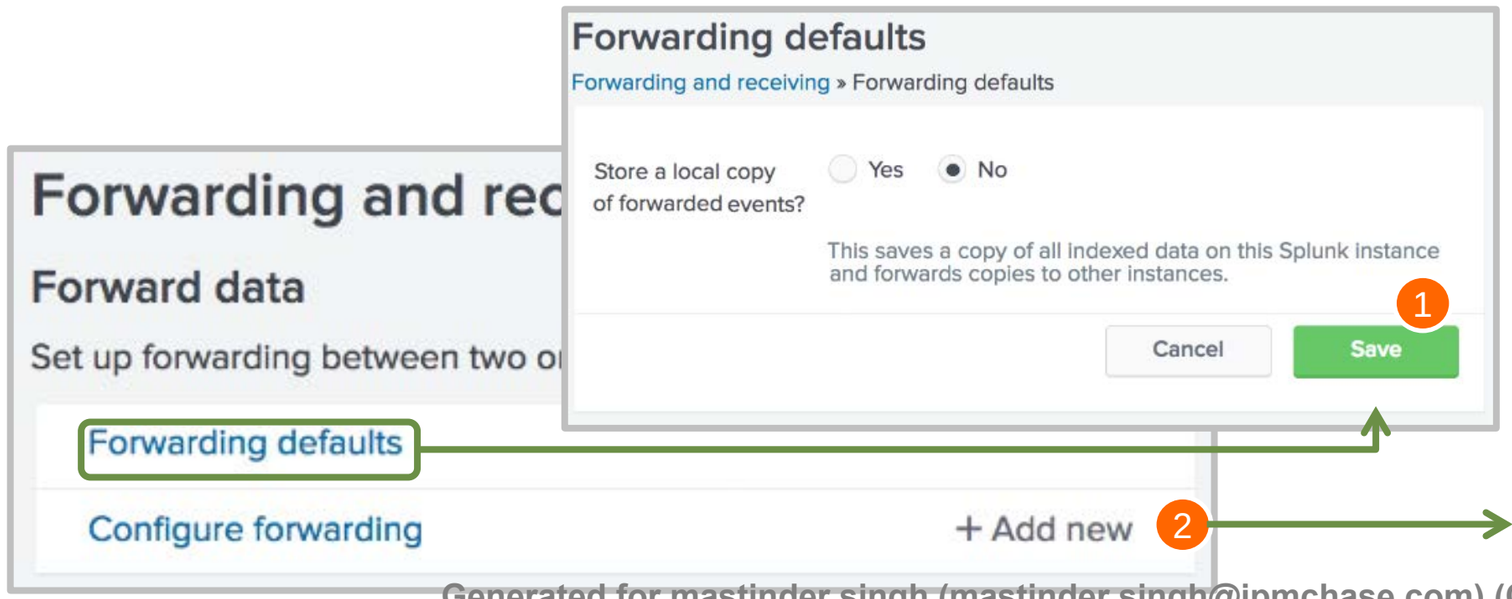
Knowledge Bundles and Replication

- Knowledge bundles are distributed to search peers by the search head when a distributed search is initiated
- They contain the knowledge objects required by the indexers for searching
- Knowledge bundles locations:

  `$SPLUNK_HOME/var/run` on the search head
  `$SPLUNK_HOME/var/run/searchpeers` on the search peer
- Replication status of knowledge bundles can be viewed from **Replication Status** column of the Splunk Web home page **Settings > Distributed search > Search peers**

Distributed Search Best Practice

- Forward all search head indexes to the search peer (indexer) layer
  - Simplifies the process of managing indexes
  - Can diagnose from other search heads if one goes down
  - Allows other search heads to access all summary indexes

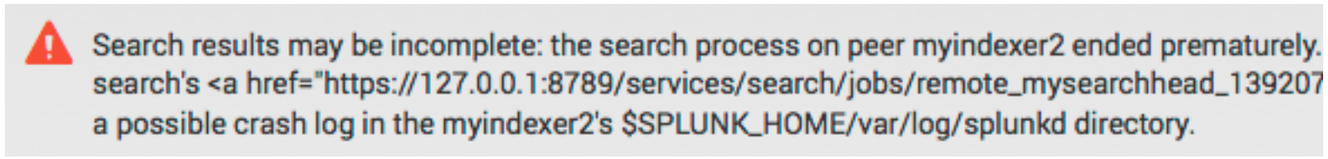


outputs.conf

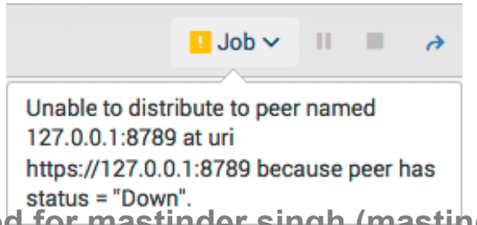
```
[indexAndForward]
index = false

[tcpout]
defaultGroup = default-autolb-group
forwardedindex.filter.disable = true
indexAndForward = false

[tcpout:default-autolb-group]
server=idx1:9997,idx2:9997
```

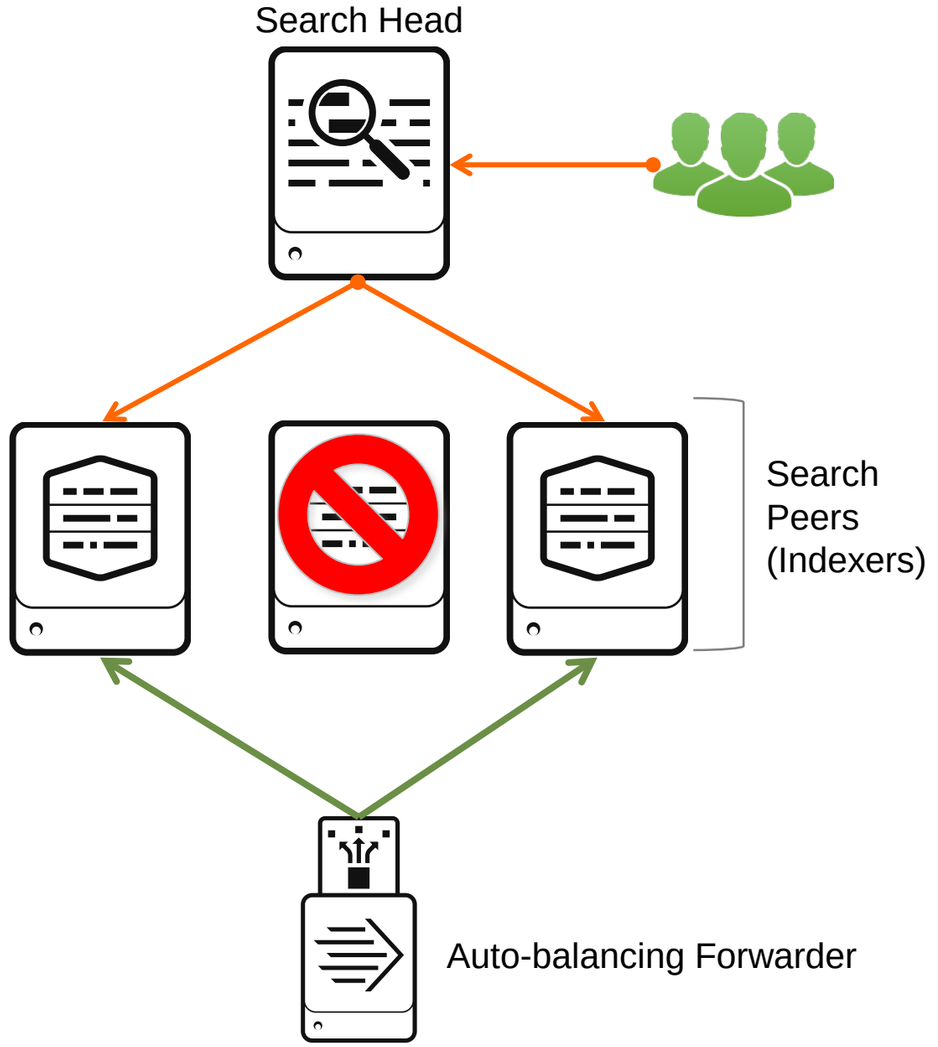
Peer Failure

- When an indexer goes down:
  - The forwarder automatically uses only the available indexers
  - The offline indexer does not participate in searches
  - The remaining indexers handle all indexing and searches
- If a peer goes down during a job, a notification is sent to the user that the job is potentially incomplete



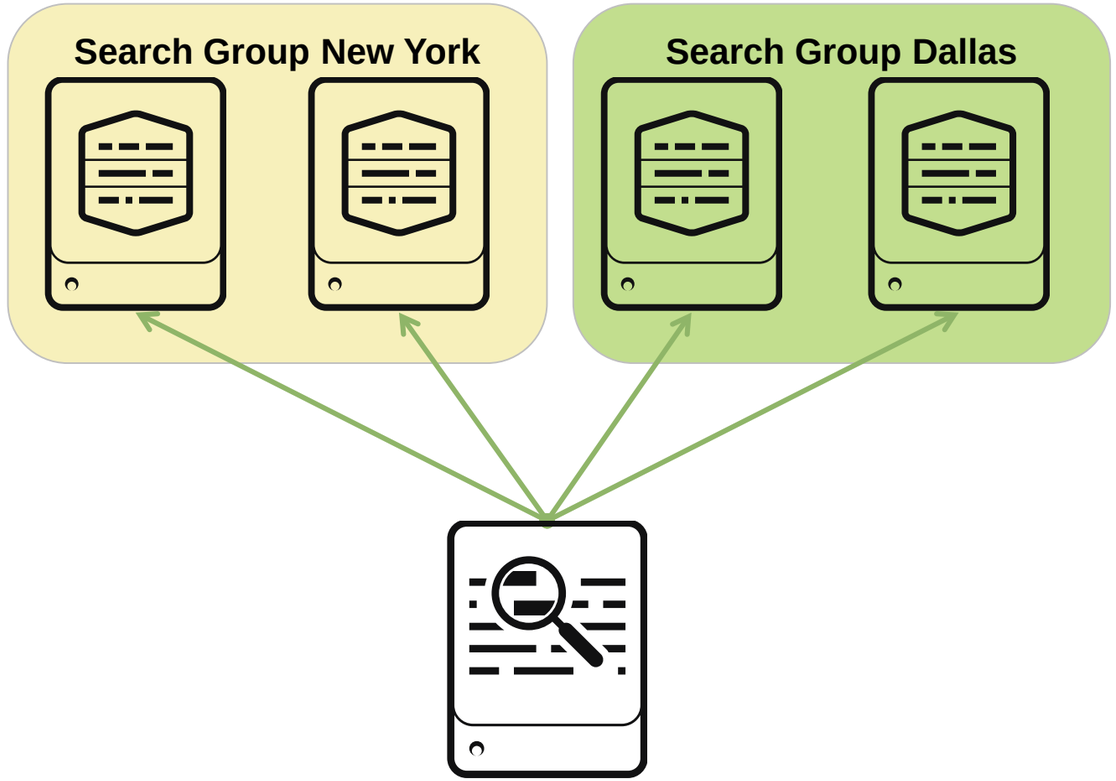
- If a peer is already down, a message indicates which peer is down

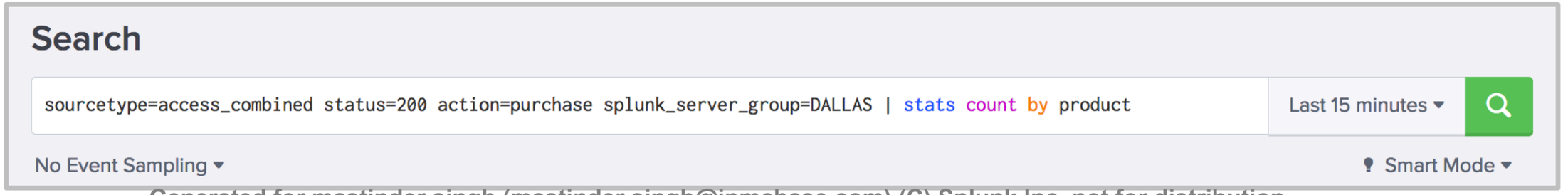




Distributed Search Groups

- Search peers can be grouped to facilitate searching on a subset of them
- Allows you to perform a search across peers that spans different locations from a single location





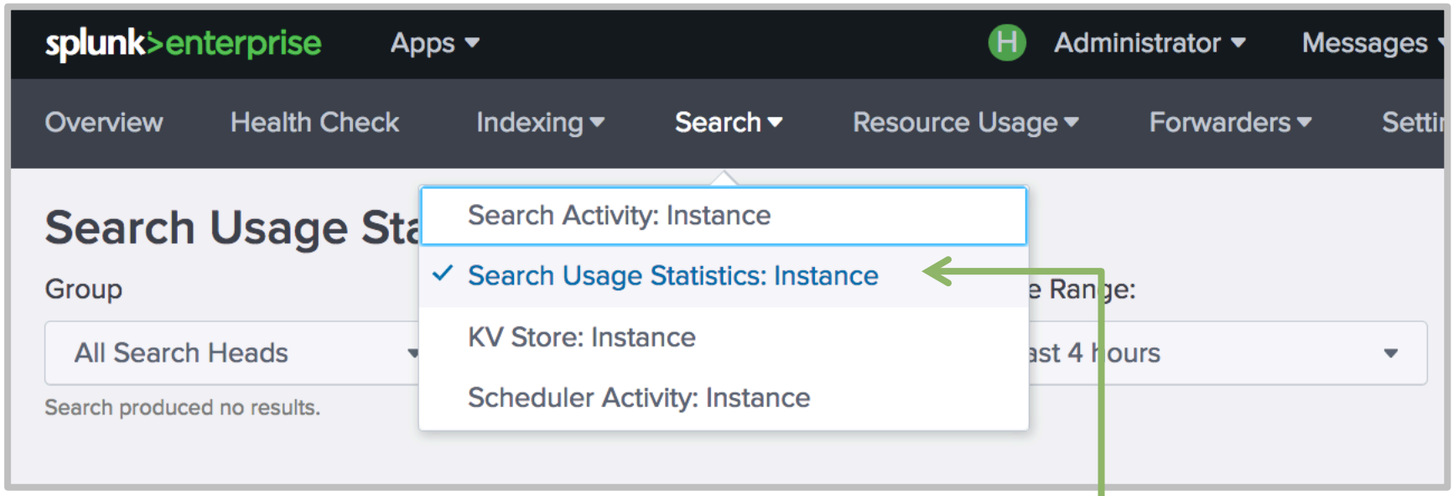
Distributed Search Groups (cont.)

Defined with the following stanzas in **`distsearch.conf`**

```
[distributedSearch]
servers = 192.168.1.1:8089, 192.168.1.2:8089, 175.143.1.1:8089, 172.

[distributedSearch:NYC]
default = false
servers = 192.168.1.1:8089, 192.168.1.2:8089

[distributedSearch:DALLAS]
default = false
servers = 175.143.1.1:8089, 175.143.1.2:8089, 175.143.1.3:8089
```


Viewing Search Peer Status with MC

- The **Search Activity: Instance** dashboard in the MC provides a graphical view of the status of your search peers
  - Median resource usage (Memory, CPU)
  - Top 10 Memory-Consuming Searches
  - Aggregate Search Runtime



Search Peer Quarantine

- If a search peer is experiencing performance issues, it can be quarantined from participating in future searches
  - Allows you to perform live troubleshooting by not stopping the search peer
  - It is prevented from performing new searches but continues to attempt to service any currently running searches
  - Only affects the relationship between search peer and search head
- From the search head, run the following CLI command:
  `splunk edit search-server –auth <user>:<password> <host:<port> -action quarantine`
- To use Splunk Web: **Settings > Distributed search > Search peers**

Use Cases for Multiple Search Heads

- Access control
  - Control who can access which indexes using what apps
  - Dedicate a search head for each functional area – IT Ops, Security, or BI
- Manage geo-dispersed data
  - Allow local offices to access their own data while maintaining centralized indexers
- Performance enhancement
  - Distribute indexing and search loads across multiple servers
    - Facilitates horizontal scaling

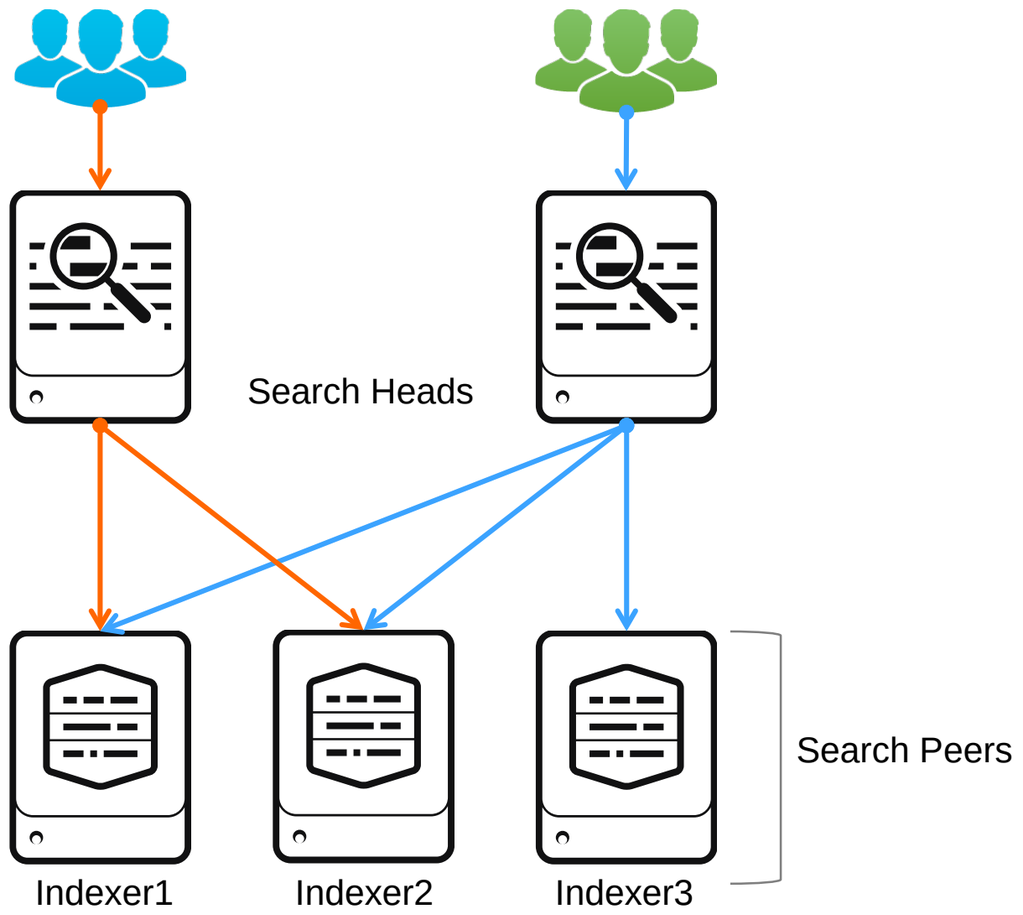
How Many Search Heads?

- One dedicated search head can handle around 8 to 12 simultaneous searches (ad hoc or scheduled)
  - Exact numbers depend on types of searches and the hardware of the search head; especially number of CPU cores
- Search heads can be added to the distributed group at any time
- Search heads can be **dedicated** or **clustered**
  - Dedicated search heads don't share knowledge objects (separate small teams)
  - Search head cluster shares a common set of knowledge objects (large teams)
    - Discussed in detail in **Splunk Cluster Administration** class

http://docs.splunk.com/Documentation/Splunk/latest/DistSearch/AboutSHC

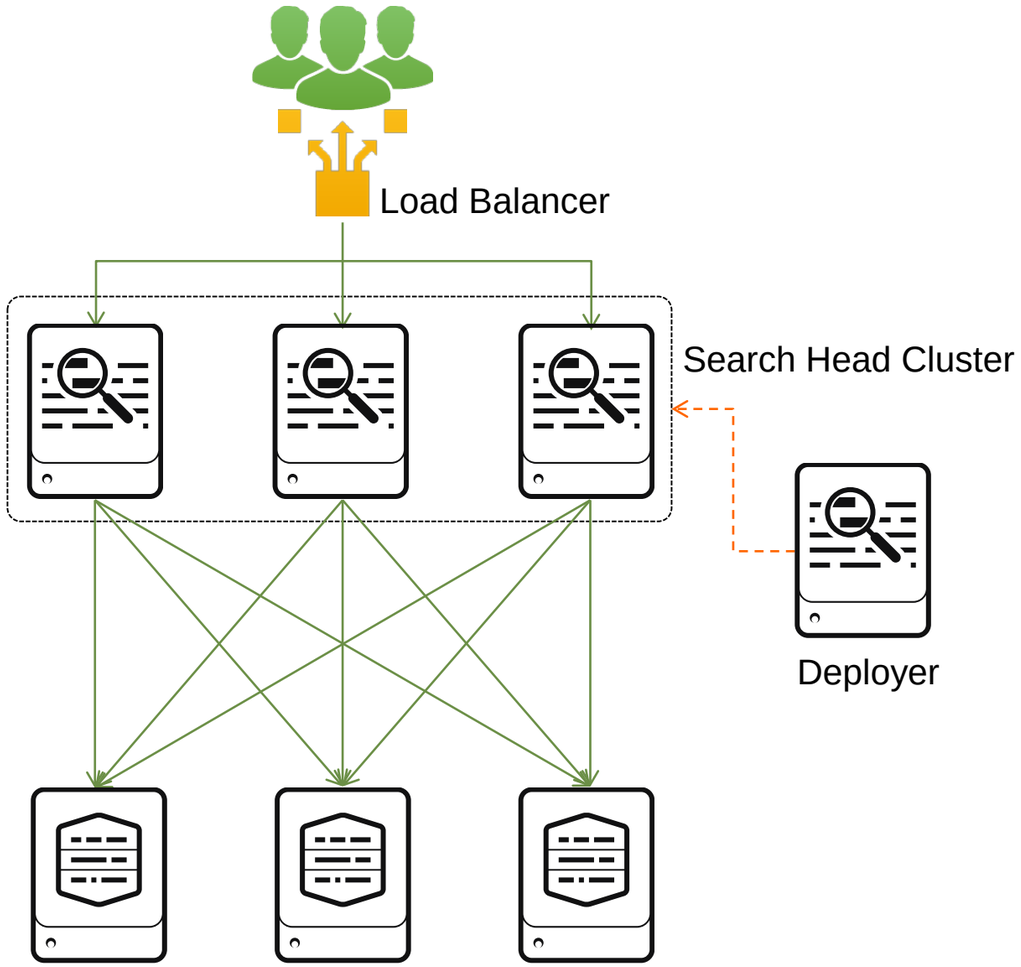
Dedicated Search Heads

- More than one search head can be configured for the same set of search peers
- Each search head
  - Contains its own unique set of reports, dashboards, etc.
  - Is dedicated to one team of users who want to have unique knowledge objects for their own use
- Good when you have teams of different people who don't share knowledge objects



Search Head Cluster

- Accommodates large enterprise use cases
  - Search head high-availability
  - Unified user experience across SHs
  - Search scaling foundation
    - Configuration sharing
    - Artifact replication
    - Job distribution
    - Alert management
    - Load balancing
- Can configure an external (non-Splunk) load balancer to provide transparent access to the cluster



Lab Exercise 10 – Distributed Search

- **Time**: 10 minutes
- **Tasks**:
- Add a search peer to your search head
- Search for indexes and source types on the search peer

Module 11: Introduction to Splunk Clusters

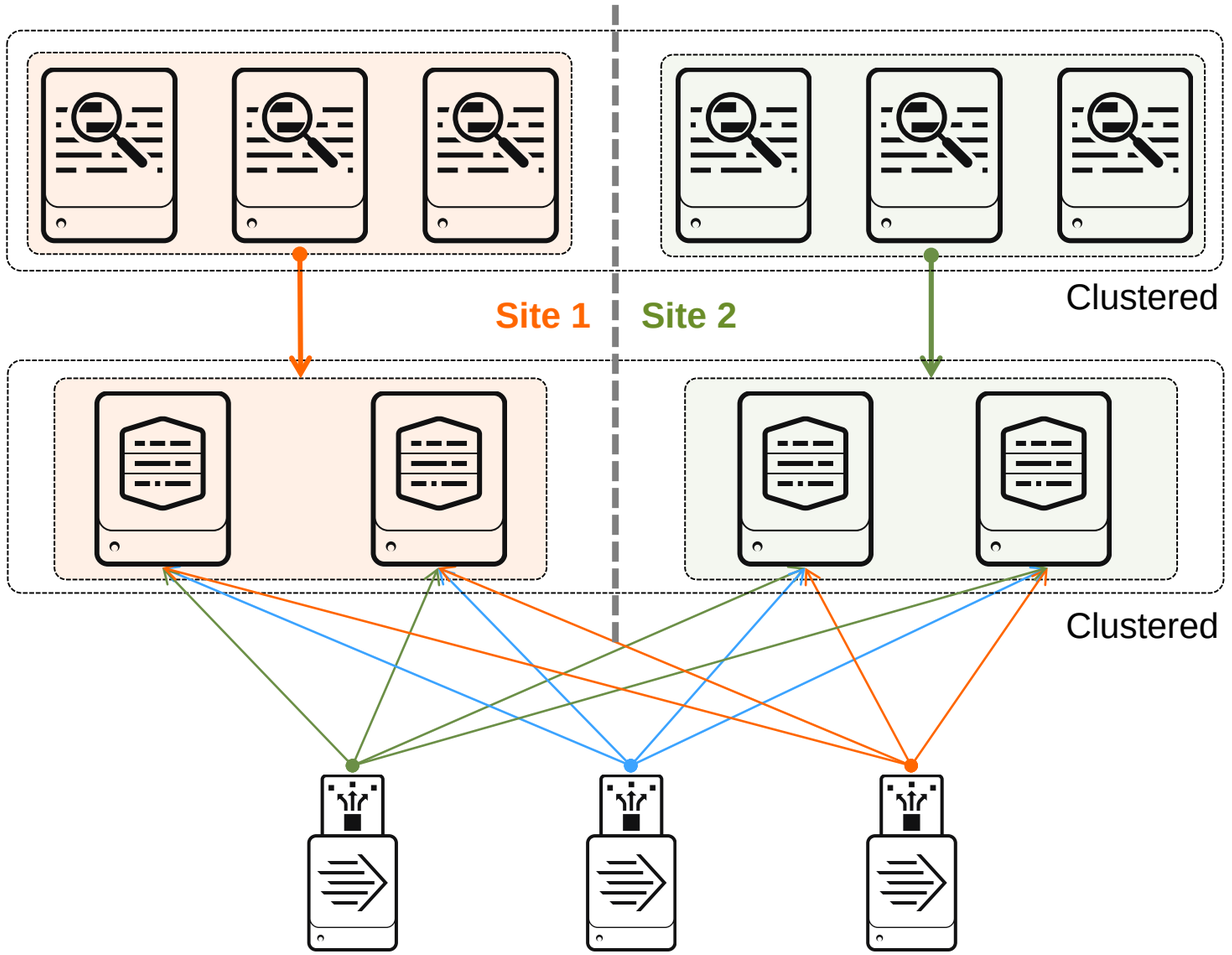
Module Objectives

Introduce Splunk clustering concepts

Splunk Clustering

- Splunk provides two types of clustering: search head clustering and indexer clustering
- Search head clustering
  - Replicates knowledge objects across search heads
  - Briefly described in module 10
- Indexer clustering
  - Replicates buckets (data) across indexers
  - Can be configured as single-site or multi-site
  - Allows you to balance growth, speed of recovery, and overall disk usage
- Requires only Splunk enterprise license
- Splunk Clustering is discussed in detail in **Splunk Cluster Administration** class

Splunk Cluster Overview



Search Heads

Indexers

Load-balanced Forwarders

Additional Components

- Cluster Node
- Monitoring Console
- Deployment Server
- Deployer
- License Master

Index Replication

- Allows for rapid failure recovery
- Requires additional disk space
  - Level of replication can be configured to manage space required
- Allows for Auto Indexer Discovery
  - Forwarders “discover” the available indexers instead of hard-coding outputs.conf
- Does not require or use additional license quota
- Basic indexer cluster concepts:

  http://docs.splunk.com/Documentation/Splunk/latest/Indexer/Basicconcepts

Further Reading: Clustering

- Basic clustering concepts for advanced users

  docs.splunk.com/Documentation/Splunk/latest/Indexer/Basicconcepts

- Configure the search head

  docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCconfigurationoverview

- Indexer discovery

  docs.splunk.com/Documentation/Splunk/latest/Indexer/indexerdiscovery

Course Wrap-up

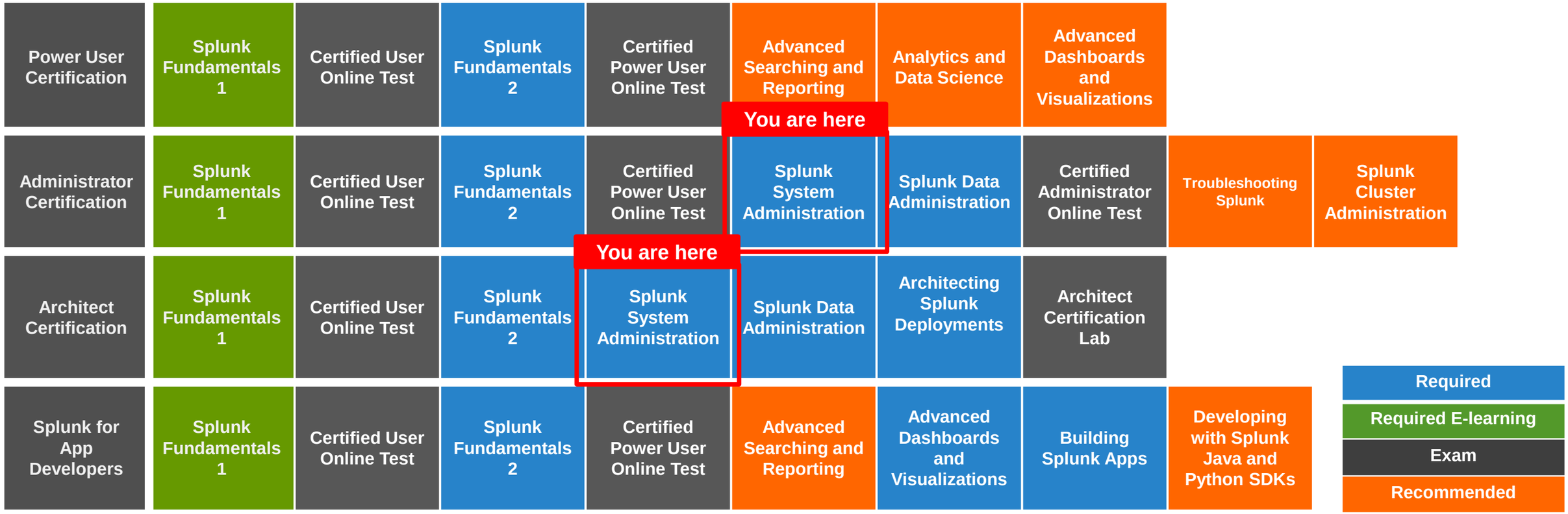
Support Programs

- **Community**
  - **Answers:** answers.splunk.com
    Post specific questions and get them answered by Splunk community experts.
  - **Splunk Docs:** docs.splunk.com
    These are constantly updated. Be sure to select the version of Splunk you are using.
  - **Wiki:** wiki.splunk.com
    A community space where you can share what you know with other Splunk users.
  - **IRC Channel:** #splunk on the EFNet IRC server Many well-informed Splunk users “hang out” here.
- **Global Support**

  Support for critical issues, a dedicated resource to manage your account – 24 x 7 x 365.
  - **Phone: (855) SPLUNK-S or (855) 775-8657**
  - **Web:** http://www.splunk.com/index.php/submit_issue
- **Enterprise Support**

  Access your customer support team by phone and manage your cases online 24 x 7 (depending on support contract).

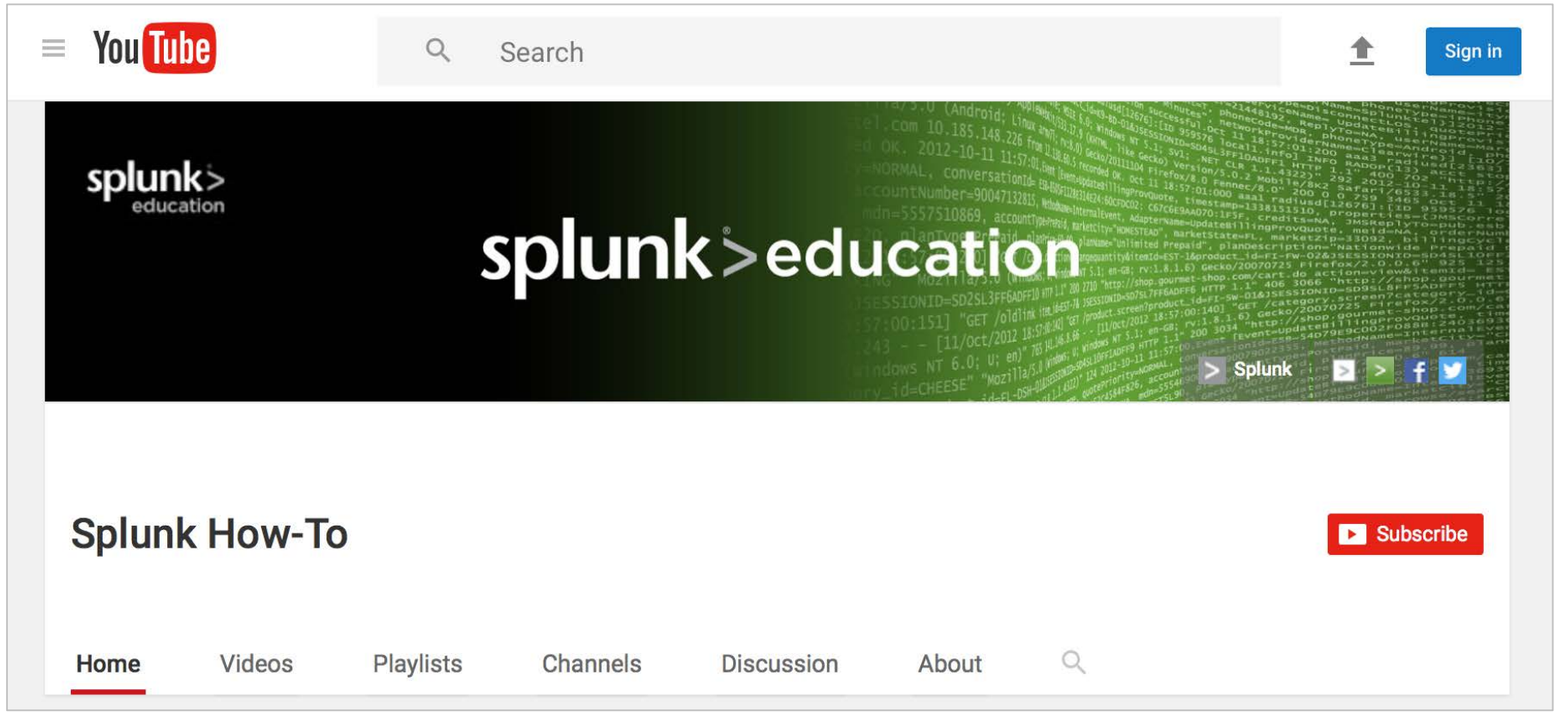
What's Next?



For detailed course and certification information go to: http://splk.it/g8q
If you have further questions, send an email to: certification@splunk.com

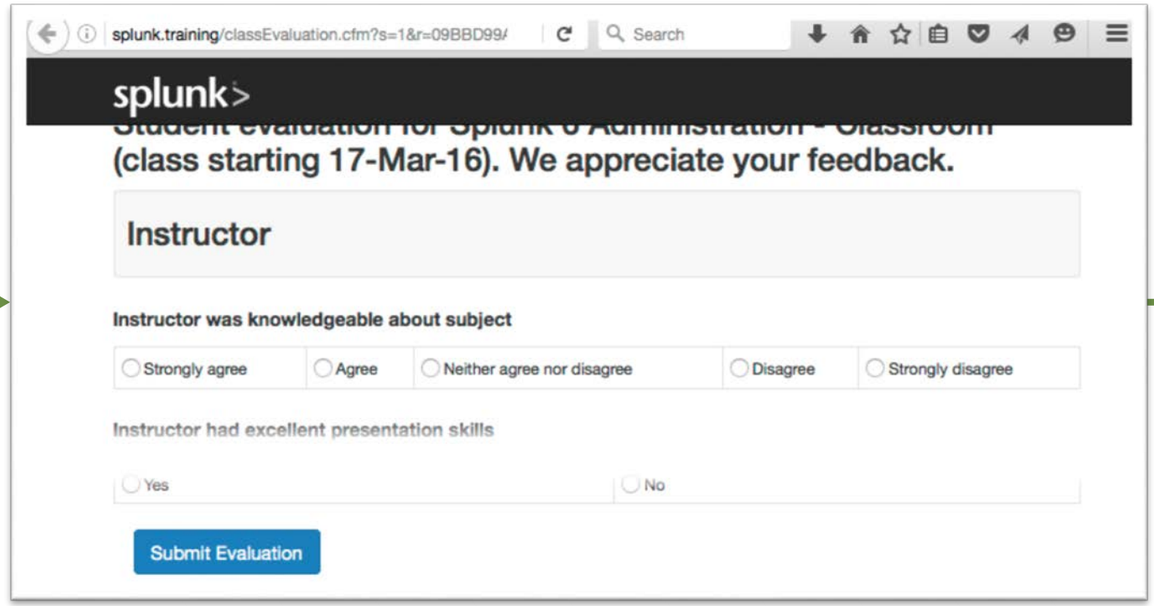
YouTube: The Splunk How-To Channel

- In addition to our roster of training courses, check out the Splunk Education How-To channel: http://www.youtube.com/c/SplunkHowTo
- This site provides useful, short videos on a variety of Splunk topics



Thank You

- Complete the Class Evaluation to be in this month's drawing for a $100 Splunk Store voucher
  1. Look for the invitation email, *What did you think of your Splunk Education class*, in your inbox
  2. Click the link or go to the specified URL in the email



Thank You