

Study Club for Splunk @ BSides22



Hands-on with AD & LDAP

We have a dedicated Study Club for Splunk Slack channel on splunk-usergroups. It is named study-club-for-splunk. The direct link is <https://bit.ly/study-club-slack>.

Step 1 - Request a personal lab

<https://bit.ly/bsides22-studyclub>

Enter a nickname and an email address and click the Request Lab Now button.




Request your Study Club for Splunk BSides22 Personal LAB

You will receive full instructions via email in 5-10 minutes from gas_admin@bitsioinc.com
Check your spam folder in case it lands there.


Nick Name (Required)

Do not use spaces or special characters

Email Address (Required)



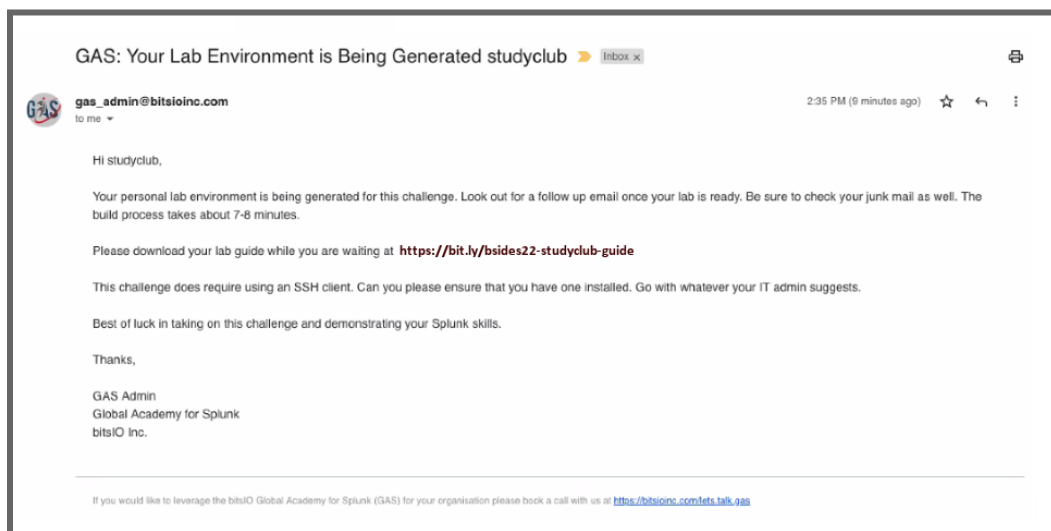
Many thanks to our friends at [bitsIO](#) for allowing free access to the Global Academy for Splunk (GAS)
Please note that all lab data is deleted automatically at the end of each lab session. Access logs are deleted every 30 days. We can delete all logs relating to any email immediately on request to gas_admin@bitsioinc.com



You will receive a request confirmation



You will receive an initial email notification within a minute or so.
Check your spam folder and allow emails from gas_admin@bitsioinc.com if needed



You will receive a further email with full lab instructions after approximately 7-8 minutes

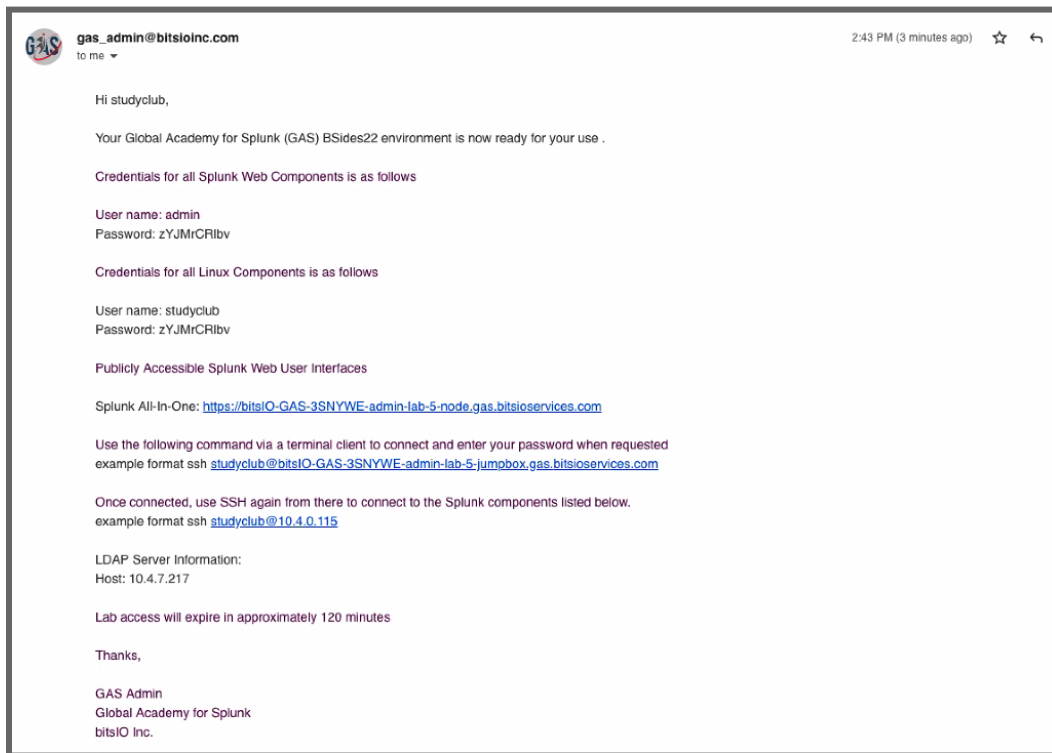


Figure 1 - Lab Environment

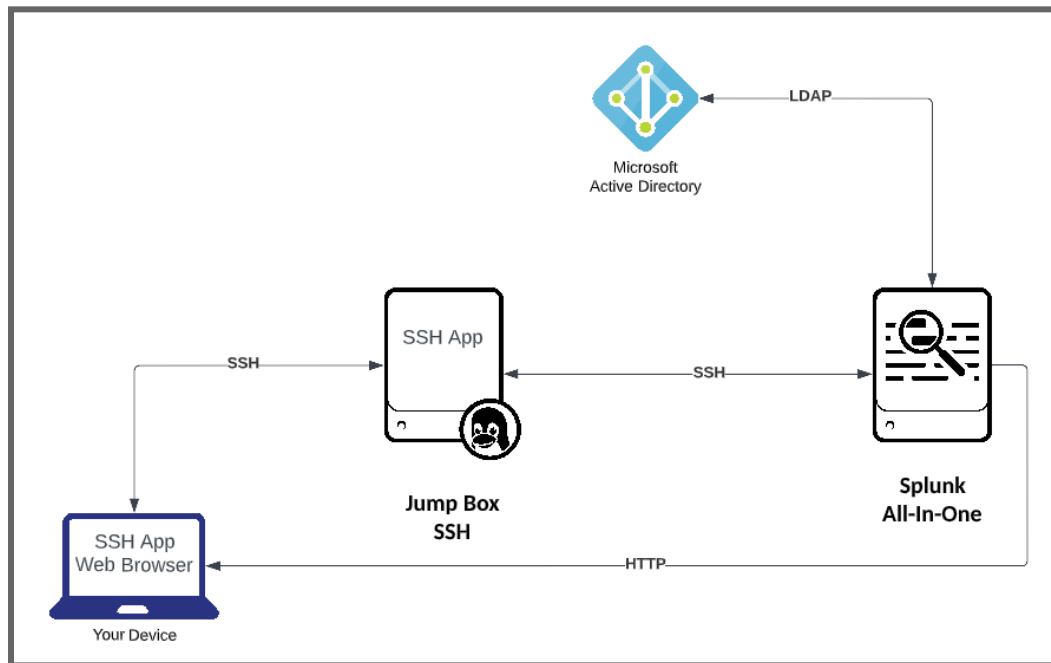
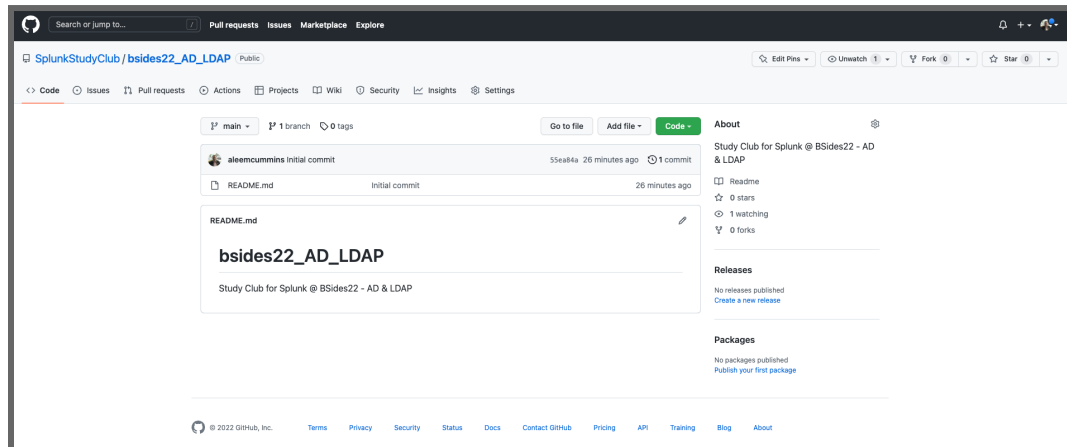


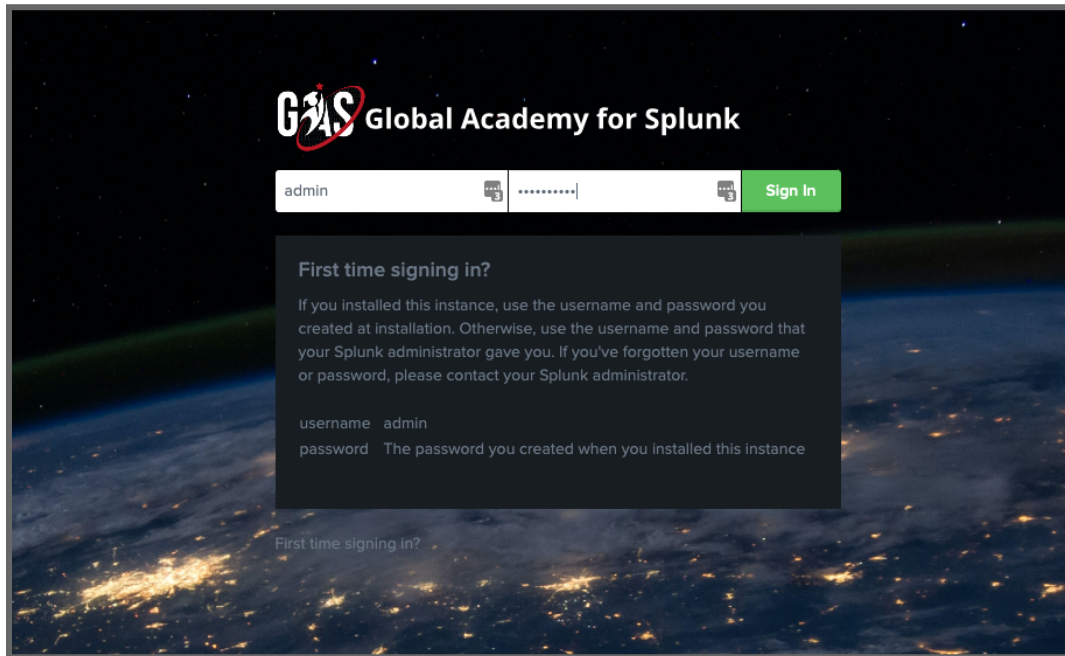
Figure 2 - GitHub Repository

Link is <https://bit.ly/bsides-studyclub-github>. Looks out for additional files and assets

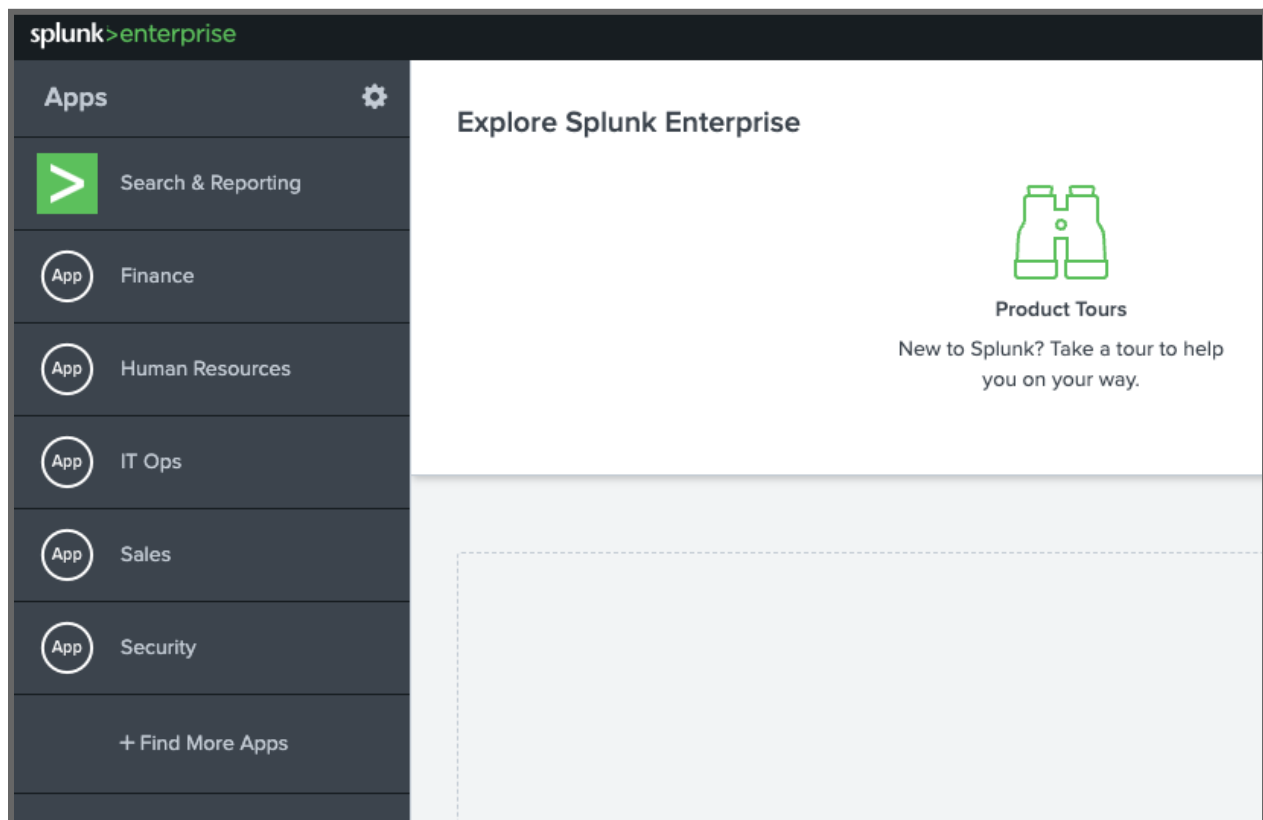


Step 2 - Login to Splunk

Use the credentials from the second email



Notice that there are five custom apps visible to you as the admin user

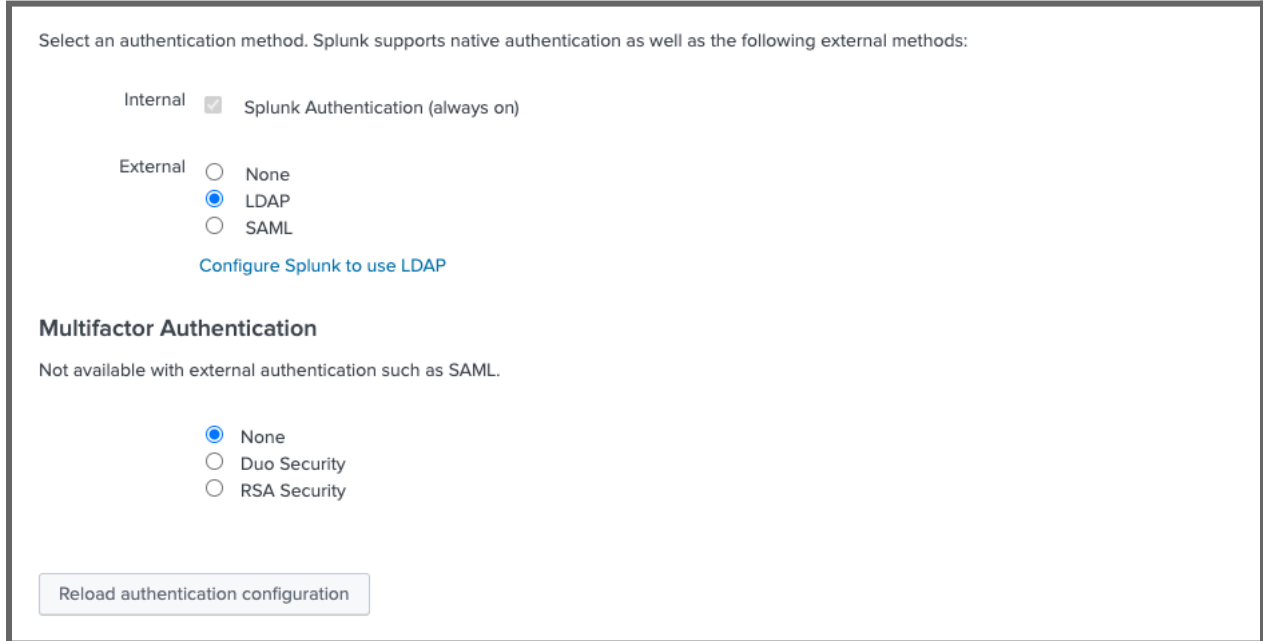


Step 3 - Configure LDAP

Excellent tutorial by SplunkTrust member Tom Kopchak over at Hurricane Labs

<https://hurricanelabs.com/splunk-tutorials/the-practical-users-guide-for-setting-up-ldap-in-splunk/>

Click **Settings** followed by **Authentication Methods**



Select an authentication method. Splunk supports native authentication as well as the following external methods:

Internal ☒ Splunk Authentication (always on)

External ☐ None
☒ LDAP
☐ SAML

[Configure Splunk to use LDAP](#)

Multifactor Authentication

Not available with external authentication such as SAML.

☒ None
☐ Duo Security
☐ RSA Security

[Reload authentication configuration](#)

Logan Carter and Dustin Church did a great user group session on SAML and LDAP with Okta
Check it out at <https://bit.ly/saml-ldap-okta>

Click **Configure Splunk to use LDAP**

Click **New LDAP** green button

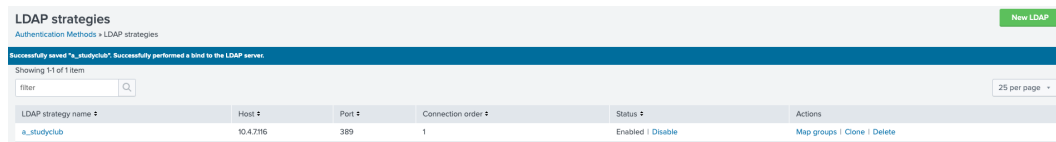
New LDAP

<p>LDAP strategy name * <input type="text"/></p> <p>Enter a unique name for this strategy.</p> <p>LDAP connection settings</p> <p>Host * <input type="text"/></p> <p>Your Splunk server must be able to resolve this host.</p> <p>Port <input type="text"/></p> <p>The LDAP server port defaults to 389 if you are not using SSL, or 636 if SSL is enabled.</p> <p><input type="checkbox"/> SSL enabled</p> <p>You must also have SSL enabled on your LDAP server.</p> <p>Bind DN <input type="text"/></p> <p>This is the distinguished name used to bind to the LDAP server. This is typically the DN of an administrator with access to all LDAP users you wish to add to Splunk. However, you can leave this blank if anonymous bind is sufficient.</p> <p>Bind DN Password <input type="password"/></p> <p>Enter the password for your Bind DN user.</p> <p>Confirm password <input type="password"/></p>	<p>a_studyclub</p> <p>10.4.7.116</p> <p>389</p> <p>CN=SplunkAdmin Student,CN=Managed Service Accounts,DC=bitsio,DC=local</p> <p>spladmin123!</p>
--	--

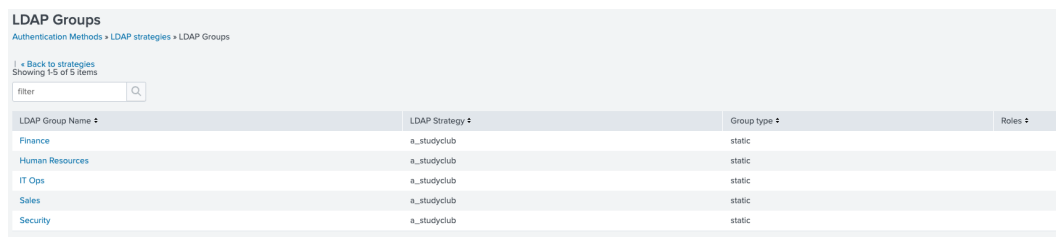
<p>User settings</p> <p>User base DN * <input type="text"/></p> <p>The location of your LDAP users, specified by the DN of your user subtree. If necessary, you can specify several DNs separated by semicolons.</p> <p>User base filter <input type="text"/></p> <p>The LDAP search filter used to filter users. Highly recommended if you have a large amount of user entries under your user base DN. For example, '(department=IT)'</p> <p>User name attribute * <input type="text"/></p> <p>The user attribute that contains the username. Note that this attribute's value should be case insensitive. Set to 'uid' for most configurations. In Active Directory (AD), this should be set to 'sAMAccountName'.</p> <p>Real name attribute * <input type="text"/></p> <p>The user attribute that contains a human readable name. This is typically 'cn' (common name) or 'displayName'.</p> <p>Email attribute <input type="text"/></p> <p>The user attribute that contains the user's email address. This is typically 'mail'.</p> <p>Group mapping attribute <input type="text"/></p> <p>The user attribute that group entries use to define their members. If your LDAP groups use distinguished names for membership you can leave this field blank.</p>	<p>CN=Users,DC=bitsio,DC=local</p> <p>samaccountname</p> <p>cn</p> <p>mail</p> <p>dn</p>
--	--

Group settings	
Group base DN *	<div><input type="text" value="OU=Splunk,DC=bitsio,DC=local"/></div> <p>The location of your LDAP groups, specified by the DN of your group subtree. If necessary, you can specify several DNs separated by semicolons.</p>
Static group search filter	<div><input type="text"/></div> <p>The LDAP search filter used to retrieve static groups. Highly recommended if you have a large amount of group entries under your group base DN. For example, '(department=IT)'</p>
Group name attribute *	<div><input type="text" value="cn"/></div> <p>The group attribute that contains the group name. A typical value for this is 'cn'.</p>
Static member attribute *	<div><input type="text" value="member"/></div> <p>The group attribute whose values are the group's members. Typical values are 'member' or 'memberUid'. Groups list user members with values of groupMappingAttribute, as specified above.</p>
<input type="checkbox"/> Nested groups Controls whether Splunk will expand nested groups using the 'memberof' extension. Only check this if you have nested groups and the 'memberof' extension on your LDAP server.	
Dynamic group settings	
Dynamic member attribute	<div><input type="text"/></div> <p>The dynamic group attribute that contains the LDAP URL used to find members. This setting is required to configure dynamic groups. A typical value is 'memberURL'.</p>
Dynamic group search filter	<div><input type="text"/></div> <p>The LDAP search filter used to retrieve dynamic groups (optional). For example, '(objectclass=groupOfURLs)'</p>
<input type="checkbox"/> Advanced settings	
<div><div>Cancel</div><div>Save</div></div>	

Click the green SAVE button



Step 4 - Map AD Groups to Splunk Roles



Click Finance



Click finance under Available Roles

Click green Save button

Repeat for **Security** and **Human Resources**

Notice that there are no existing Splunk roles for **IT Ops** and **Sales**
Add by clicking on **Settings** followed by **Roles**

Roles New Role

5 Roles filter

Name ▾	Actions	Native capabilities	Inherited capabilities	Default App ▾
admin	Edit ▾	96	32	
can_delete	Edit ▾	4	0	
power	Edit ▾	9	23	
splunk-system-role	Edit ▾	0	128	
user	Edit ▾	23	0	

Click the down arrow in the **Actions** column for **admin** role and select **Clone**

Roles

5 Roles filter

Name ▴	Actions
admin	Edit ▾
can_delete	
power	
splunk-system-role	
user	

Edit

View Capabilities

View Indexes

Clone

Add IT Ops as Name

Edit Role it ops

×

Name *

1. Inheritance 2. Capabilities 3. Indexes 4. Restrictions 5. Resources

Specify roles from which this role inherits capabilities and indexes. Inherited capabilities and indexes cannot be disabled. If multiple roles are specified, this role inherits capabilities and indexes from all selected roles.

<input type="checkbox"/>	Role name	filter	Showing all ▾
<input type="checkbox"/>	admin		
<input type="checkbox"/>	can_delete		
<input type="checkbox"/>	finance		
<input type="checkbox"/>	human resources		
<input type="checkbox"/>	it ops		
<input checked="" type="checkbox"/>	power		
<input type="checkbox"/>	sales		
<input type="checkbox"/>	security		
<input type="checkbox"/>	splunk-system-role		
<input checked="" type="checkbox"/>	user		

Cancel Save

Repeat to add **Sales** role

Now we need to Map AD Groups to these newly created Splunk Roles

Click **Settings** followed by **Authentication Methods**

Check the **LDAP** radio button followed by **LDAP Settings**

Click **Map groups** from the **Actions** column

LDAP Groups

Authentication Methods > LDAP strategies > LDAP Groups

1 < Back to strategies
Showing 1-5 of 5 items

filter

LDAP Group Name ▴	LDAP Strategy ▴	Group type ▴	Roles ▴
Finance	a_studyclub	static	finance
Human Resources	a_studyclub	static	human resources
IT Ops	a_studyclub	static	
Sales	a_studyclub	static	
Security	a_studyclub	static	security

Click **IT Ops** and repeat steps from earlier

Click **Sales** and repeat steps from earlier

All Splunk roles are now mapped to AD Groups

LDAP Group Name ▴	LDAP Strategy ▴	Group type ▴	Roles ▴
Finance	a_studyclub	static	finance
Human Resources	a_studyclub	static	human resources
IT Ops	a_studyclub	static	it ops
Sales	a_studyclub	static	sales
Security	a_studyclub	static	security

Step 4 - Configure App Permissions

Lock down permissions for finance app to finance role

Security role is also added as best practice

App permissions

Users with read access can only save objects for themselves, and require write access to be able to share objects with other users.

Roles	Read	Write
Everyone	<input type="checkbox"/>	<input type="checkbox"/>
admin	<input type="checkbox"/>	<input type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>
finance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
human resources	<input type="checkbox"/>	<input type="checkbox"/>
it ops	<input type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input type="checkbox"/>
sales	<input type="checkbox"/>	<input type="checkbox"/>
security	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
splunk-system-role	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>

Apply selected role permissions to:

[Learn more](#)

☒ This app only (Finance) ☐ All apps (system)

Cancel

Save

Repeat to

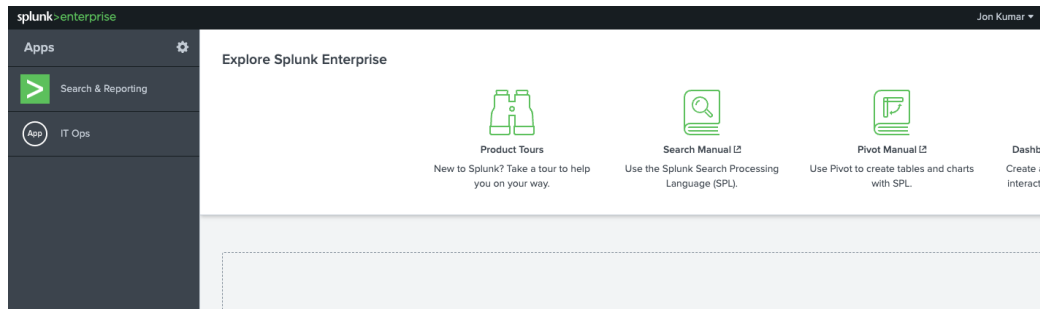
- Lock down permissions for IT Ops app to IT Ops role
- Lock down permissions for Sales app to Sales role
- Lock down permissions for Security app to Security role
- Lock down permissions for Human Resources app to Human Resources role

Step 5 - Test App Permissions

Test 1

Logout as **Admin** user

Login as IT Ops user **jon.kumar** with password **spljk123!**

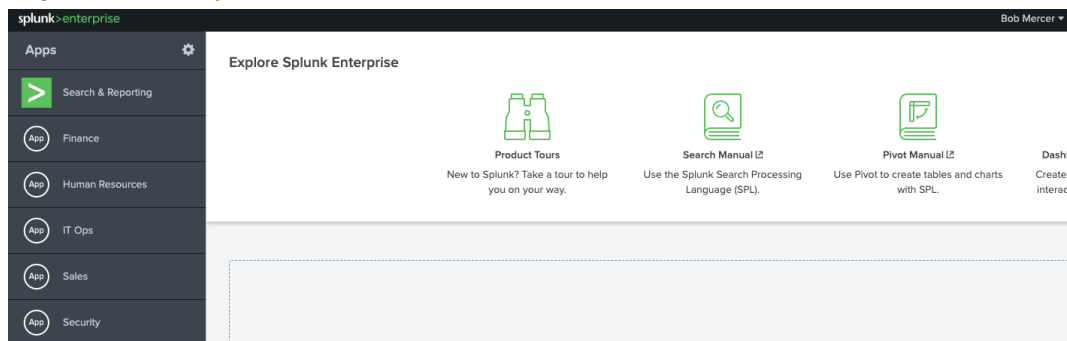


Jon from the IT Ops Splunk role mapped to the AD Group IT Ops can only see the IT Ops dashboard as anticipated.

Logout as **jon.kumar** user

Test 2

Login as Security user **bob.mercer** with password **splbm123!**



Bob from the Security Splunk role mapped to the AD Group Security can see the Security dashboard and also the dashboards from Sales, Human Resources, IT Ops and Finance as anticipated.

Logout as **bob.mercer** user

A complete list of AD Groups and Users can be seen in Appendix B

Feel free to play around with the app permissions on the UI or even in the CLI to aid your shared learning

Step 6 - Validate Configuration Files

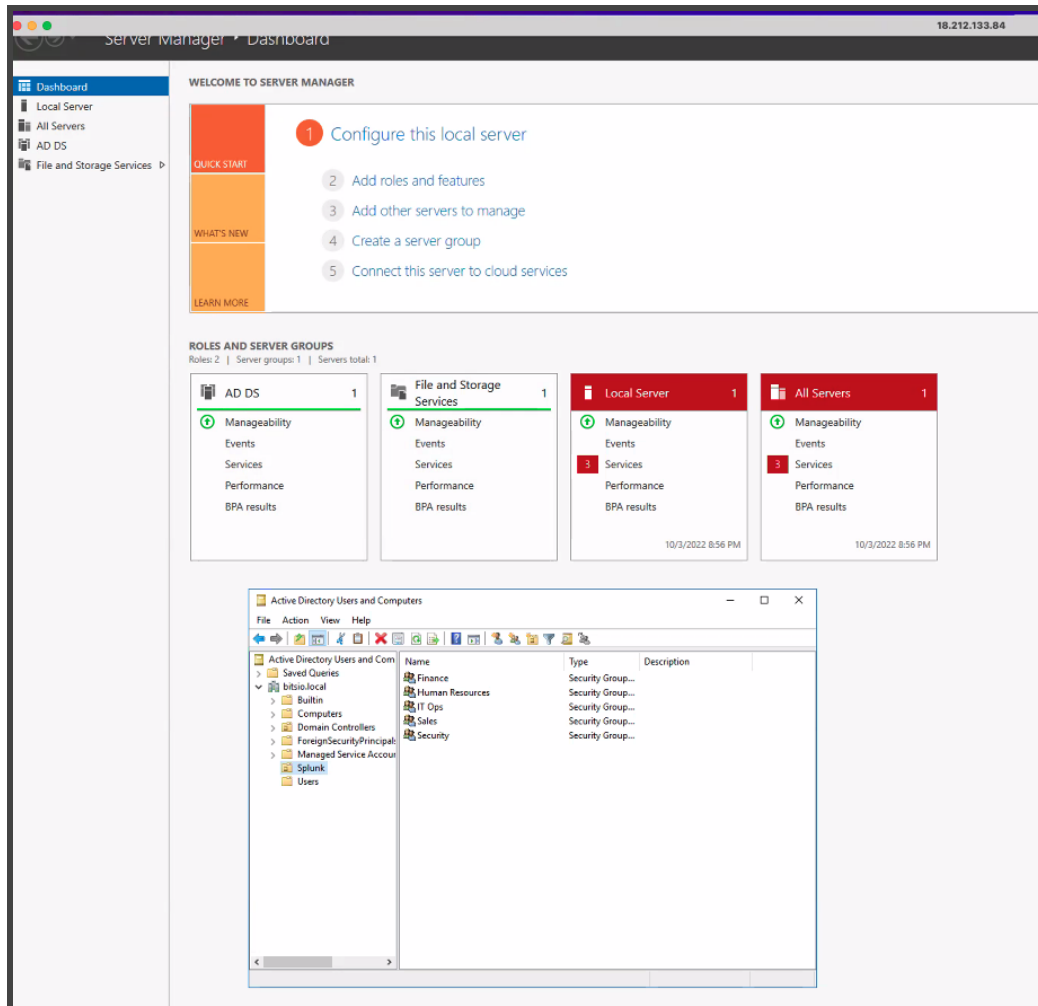
Is there a cool btool command to locate the files

```
/opt/splunk/bin/splunk cmd btool authorize list --debug | grep /local  
cat
```

```
/opt/splunk/bin/splunk cmd btool authentication list --debug | grep /local
```

Appendix A - Microsoft Active Directory (AD)

The study club lab includes a configured and active Microsoft AD. It is accessible via the Splunk LDAP configuration only. For reference, this is what the user interface looks like for the lab.



Appendix B - AD Groups and Users

AD Group	AD User	AD Username	AD User Password
IT Ops	Jon Kumar	jon.kumar	spljk123!
IT Ops	Laurel Carson	laurel.carson	spllc123!
IT Ops	Sally Pitts	sally.pitts	splsp123!
Security	Gita Singh	gita.singh	splgs123!
Security	Bob Mercer	bob.mercer	splbm123!
Security	Rita Murphy	rita.murphy	splrm123!
Finance	Heidi Wilder	heidi.wilder	splhw123!
Finance	Lacey Rosario	lacey.rosario	spllr123!
Finance	Rea Nelson	rea.nelson	splrn123!
Human Resources	Siena Salazar	siena.salazar	splss123!
Human Resources	Jude Fountain	jude.fountain	spljf123!
Human Resources	Otto Bull	otto.bull	splob123!
Sales	Tia Lister	tia.lister	spltl123!
Sales	Emma Kenny	emma.kenny	splek123!
Sales	Brent Ireland	brent.ireland	splbi123!