Splunk Users

Settings > Access Controls



- Can be defined locally
- Can be defined in a directory like LDAP or AD

Splunk Roles

Settings > Access Controls

- Five built in roles
 - 1. admin
 - 2. power
 - 3. user
 - 4. can_delete
 - 5. splunk-system-role



Custom Roles

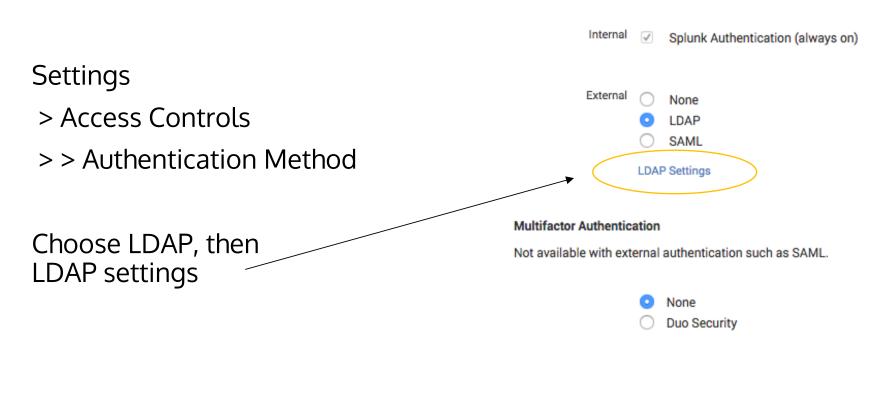
- Splunk Administrators can create custom roles
- Some apps come with custom roles
 - winfra-admin, vmware_admin, etc.

Authentication Options

- Local
- LDAP
- SAML
- Scripted SSO
- Splunk recommends using LDAP to manage user authentication.
- Splunk works with OpenLDAP and Active Directory

Creating an LDAP Strategy

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

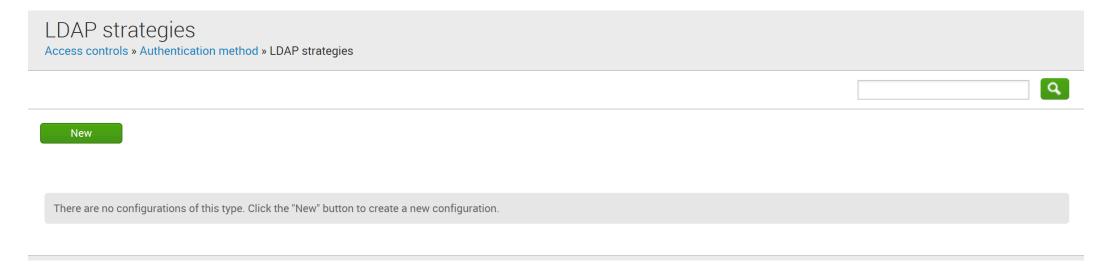


Reload authentication configuration

© Adam Frisbee, adamfrisbee.com

Creating an LDAP Strategy

Create a new LDAP strategy by clicking the New button



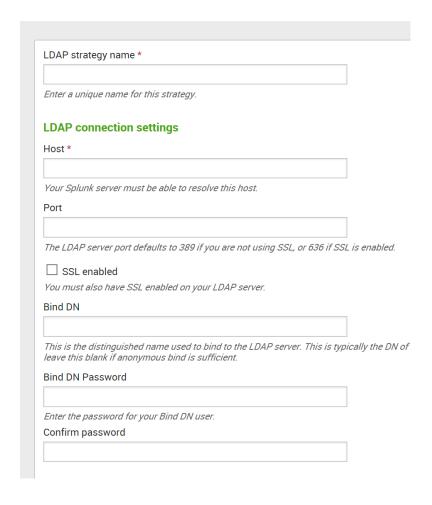
Name of your choosing

Your Domain Controller

Default ports 389 or 636

Check if SSL is enabled in your LDAP environment

An administrator or service account



The location of your LDAP users, in "LDAP speak" (i.e. OU= OU= DC= DC=)

For LDAP, set to uid, for AD set to sAMAccountname

Set to cn

Set to mail

Set to dn

User base DI	1 *
The location o	of your LDAP users, specified by the DN of your user subtree. If
oser base m	
The LDAP sea	rch filter used to filter users. Highly recommended if you have
User name a	ttribute *
	bute that contains the username. Note that this attribute's value most configurations. In Active Directory (AD), this should be se tribute *
Set to 'uid' for Real name at	most configurations. In Active Directory (AD), this should be se tribute *

The location of your LDAP groups, in "LDAP speak" (i.e. OU= OU= DC= DC=)

Set to cn

Set to member

Group ba	ase DN *
The locat	ion of your LDAP groups, specified by the DN of your group subtree.
Static gr	oup search filter
The LDAF	search filter used to retrieve static groups. Highly recommended if
Group na	ame attribute *
The group	p attribute that contains the group name. A typical value for this is 'cı
Static me	ember attribute *
The group above.	o attribute whose values are the group's members. Typical values are
☐ Nest	red groups
	whether Splunk will expand nested groups using the 'memberof' exte

Thanks, Splunkers!

