Users, Roles, and Authentication >

Splunk Users

Settings > Access Controls

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

Users, Roles, and Authentication >

Splunk Roles

Settings > Access Controls

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

Users, Roles, and Authentication >

Custom Roles

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

Users, Roles, and Authentication >

Authentication Options

- Local
- LDAP
- SAML
- Scripted SSO

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

Users, Roles, and Authentication >

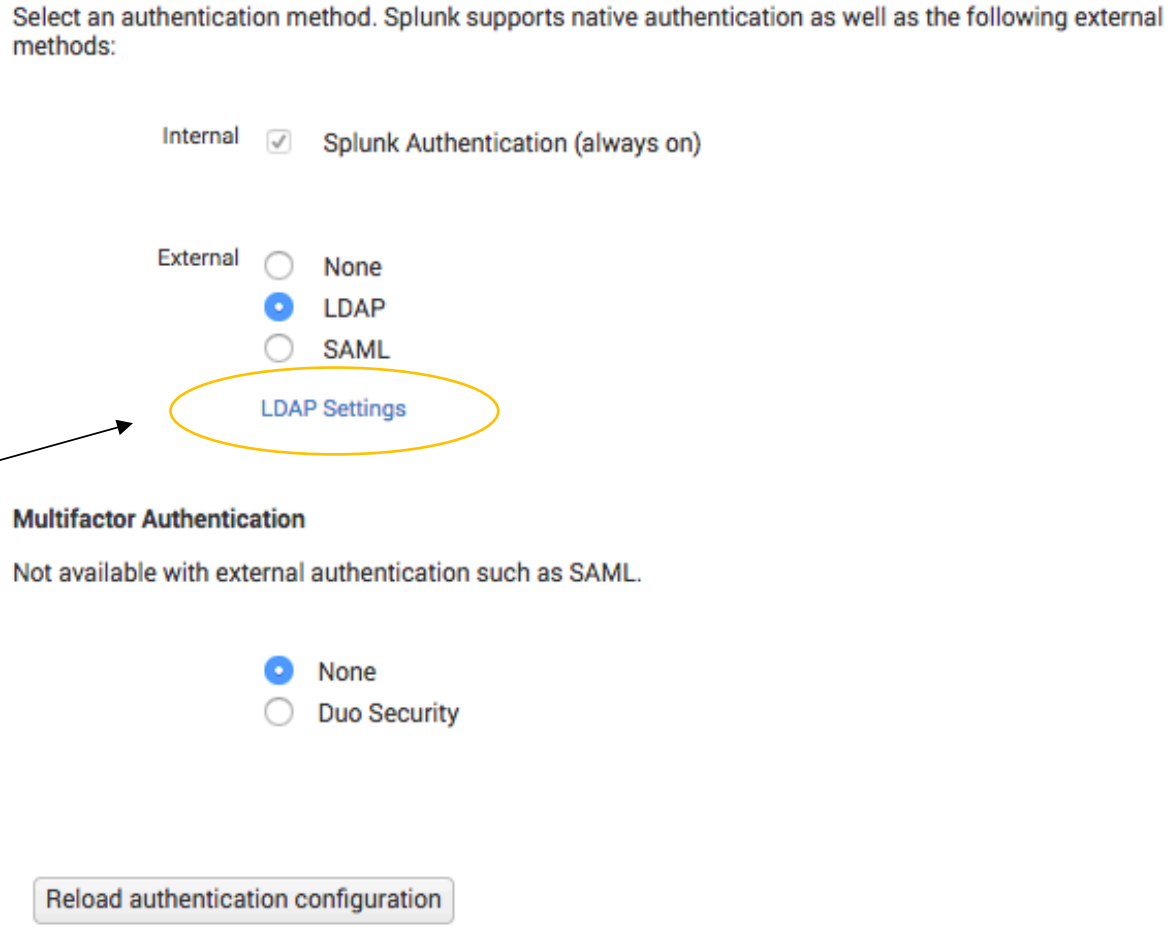
Creating an LDAP Strategy

Settings

> Access Controls

> > Authentication Method

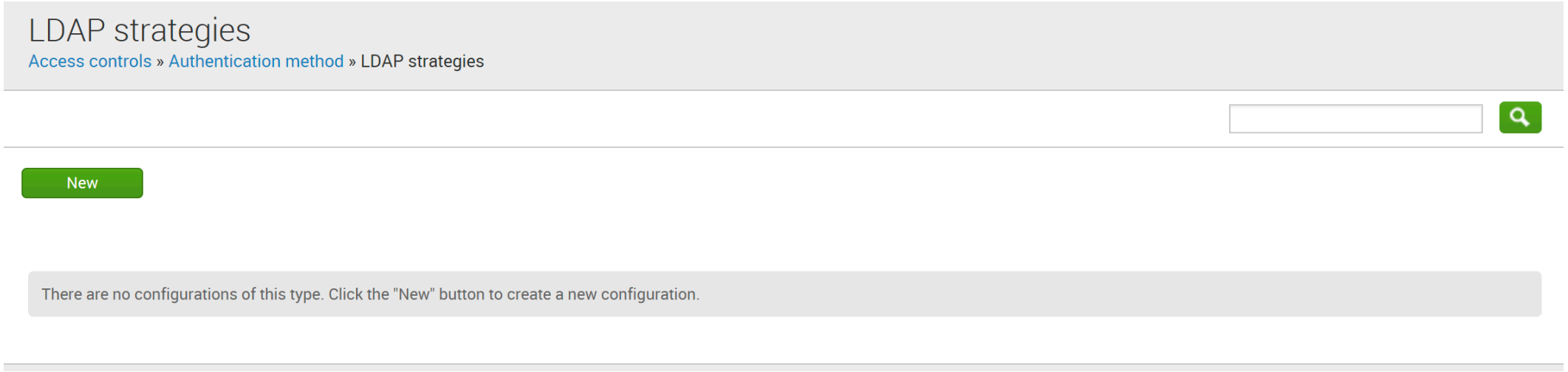
Choose LDAP, then LDAP settings



Users, Roles, and Authentication >

Creating an LDAP Strategy

Create a new LDAP strategy by clicking the New button



Users, Roles, and Authentication >

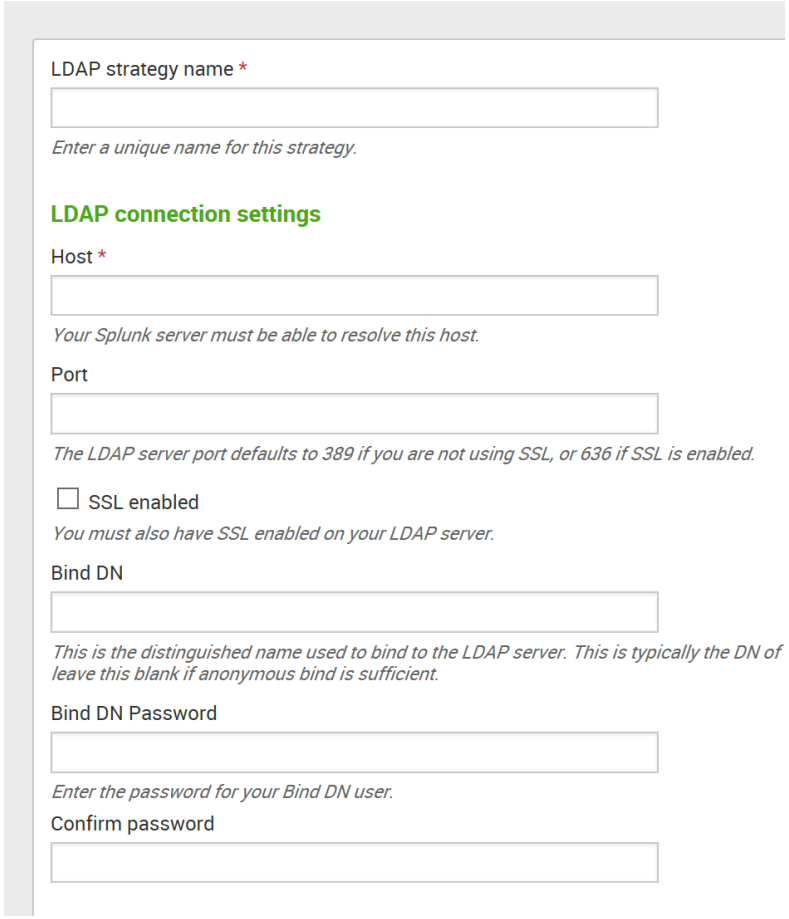
Name of your choosing

Your Domain Controller

Default ports 389 or 636

Check if SSL is enabled in your LDAP environment

An administrator or service account



Users, Roles, and Authentication >

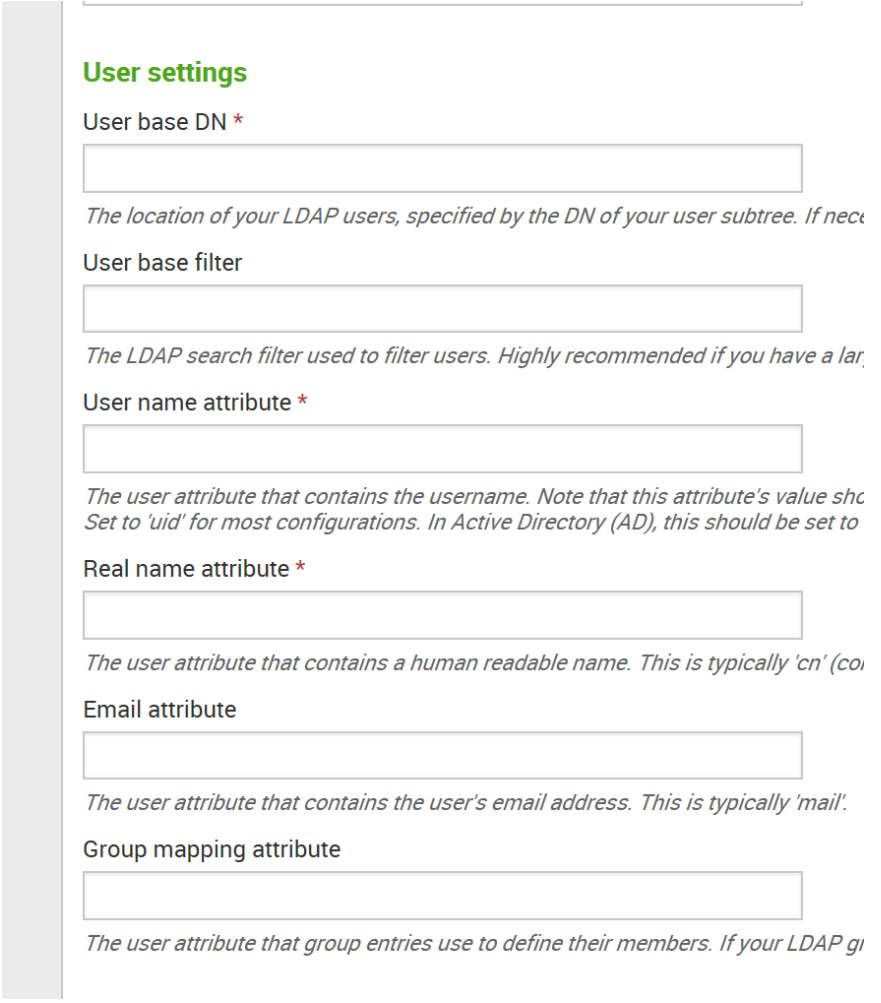
The location of your LDAP users, in “LDAP speak” (i.e. OU= OU= DC= DC=)

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

Set to cn

Set to mail

Set to dn

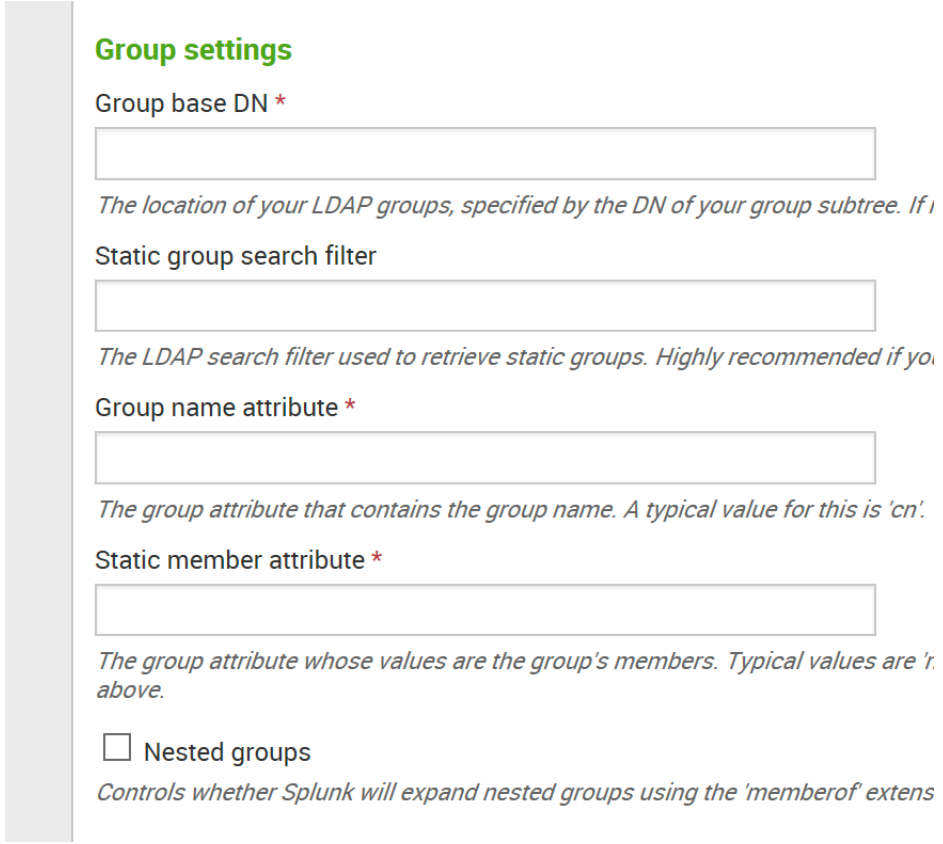


Users, Roles, and Authentication >

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

Set to cn

Set to member



Thanks, Splunkers!