

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

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

Internal ☒ Splunk Authentication (always on)

External ☐ None
☒ LDAP
☐ SAML

[LDAP Settings](#)

Multifactor Authentication

Not available with external authentication such as SAML.

☒ None
☐ Duo Security

[Reload authentication configuration](#)

Users, Roles, and Authentication >

Creating an LDAP Strategy

Create a new LDAP strategy by clicking the New button

LDAP strategies

[Access controls](#) » [Authentication method](#) » LDAP strategies



New

There are no configurations of this type. Click the "New" button to create a new configuration.

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

LDAP strategy name *

Enter a unique name for this strategy.

LDAP connection settings

Host *

Your Splunk server must be able to resolve this host.

Port

The LDAP server port defaults to 389 if you are not using SSL, or 636 if SSL is enabled.

☐ SSL enabled

You must also have SSL enabled on your LDAP server.

Bind DN

This is the distinguished name used to bind to the LDAP server. This is typically the DN of leave this blank if anonymous bind is sufficient.

Bind DN Password

Enter the password for your Bind DN user.

Confirm password

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

User settings

User base DN *

The location of your LDAP users, specified by the DN of your user subtree. If necessary, use the following format: ou=users,dc=example,dc=com

User base filter

The LDAP search filter used to filter users. Highly recommended if you have a large number of users.

User name attribute *

The user attribute that contains the username. Note that this attribute's value should be unique. Set to 'uid' for most configurations. In Active Directory (AD), this should be set to sAMAccountName.

Real name attribute *

The user attribute that contains a human readable name. This is typically 'cn' (common name) in AD.

Email attribute

The user attribute that contains the user's email address. This is typically 'mail'.

Group mapping attribute

The user attribute that group entries use to define their members. If your LDAP group entries use a specific attribute to define their members, set it here.

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

Group settings

Group base DN *

The location of your LDAP groups, specified by the DN of your group subtree. If you

Static group search filter

The LDAP search filter used to retrieve static groups. Highly recommended if you

Group name attribute *

The group attribute that contains the group name. A typical value for this is 'cn'.

Static member attribute *

The group attribute whose values are the group's members. Typical values are 'r' above.

☐ Nested groups

Controls whether Splunk will expand nested groups using the 'memberof' extens

Thanks, Splunkers!

