

Splunk4Admins

User Management



Forward-looking statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as “expects,” “anticipates,” “targets,” “goals,” “projects,” “intends,” “plans,” “believes,” “momentum,” “seeks,” “estimates,” “continues,” “endeavors,” “strives,” “may,” variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the “Risk Factors” section of Splunk’s most recent report on Form 10-Q filed with the SEC on November 28, 2023. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by Cisco or Splunk, on Cisco or Splunk’s website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment or be relied upon in making a purchasing decision. We undertake no commitment, promise or obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk LLC in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners.

© 2025 Splunk LLC. All rights reserved.



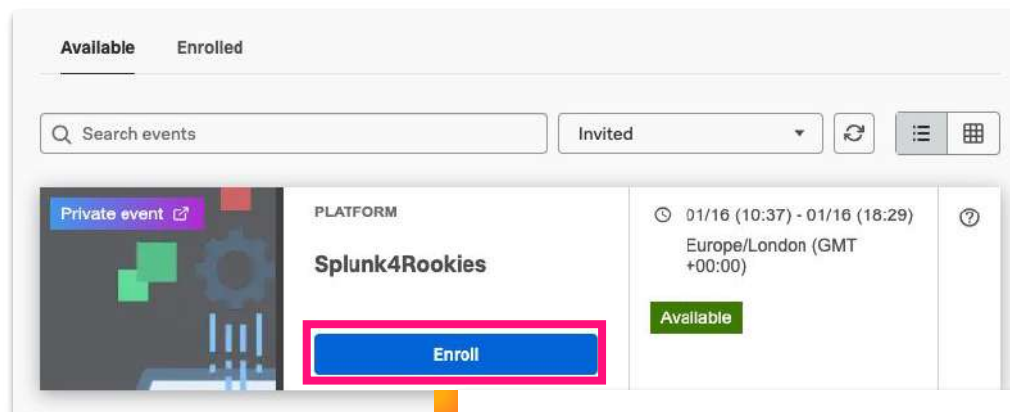
Enroll in Today's Workshop

Tasks

1. Get a splunk.com account if you don't have one yet:
<https://splk.it/SignUp>
2. Enroll in the Splunk Show workshop event:
<https://show.splunk.com/event/<eventID>>
3. Download the hands-on lab guide:
<https://splk.it/S4A-UM-Lab-Guide>

Contains step-by-step instructions for all of today's exercises!
4. Download a copy of today's slide deck:
<https://splk.it/S4A-UM-Attendee>

Goal



Enroll in today's event

Workshop Agenda

- Discuss Who?|What?|Why?
- Expectations
- User vs. Role
- How to Create a Role (and test with a local user) - Lab¹
- How to integrate Splunk with Active Directory - Lab²
- Map Splunk Roles to Active Directory Groups - Lab³
- Login with different users/roles/groups - Lab⁴
- How to integrate Splunk with Single Sign-On
- Other options for Authentication
- Summary

Audience

Who is this Workshop for?

- Splunk Admins
- “Required”: Power User Certified
- “Preferred”: Splunk Admin enabled (at least started ...), Certified

Please introduce yourself!

- Name
- Company/organisation
- Role
- Are you currently using Splunk?
- What are you interested in using Splunk for?



Expectations for Workshop

- Last roughly 60-75 minutes
- Understand the differences between Users and Roles
- Understand the differences between local and non-local User (and Role) management
- Know the available SAML/AD integrations (or at least where to find them)
- Experience User and Role creation - Lab¹
- Understand what is inherent in a Role definition
- Experience integration between Splunk and Active Directory (Lab²) as external Authenticator
- Learn some best practices for Role and User Management
- Excludes Cluster User and Role Management

Why are there Users and Roles?

- Users and Roles provide access to a Splunk instance
 - Differentiating Users from Roles ensures better security and greater flexibility
- A user can exist without a role, but would be unable to login
- The difference between Authentication and Authorization
 - Authentication means proving that the user exists and has privilege on the system
 - Username
 - Password
 - Authorization means the privileges that an authenticated user has access to (capabilities, indexes, resources)

User vs. Role

What makes a User? vs. What makes a Role?

- **Users**

- **Have**

- **Authentication**

- Name
 - [Password]
 - Full Name
 - Time zone
 - Default App
 - Default app inherited from
 - Roles (can be multiple)

- **Don't have**

- **Authorization**

- Inheritance
 - Capabilities
 - Indexes
 - Restrictions
 - Resources

The 'Create User' form includes fields for Name, Full name (optional), Email address (optional), Set password (New password), and Confirm password (Confirm new password). It also has a 'Time zone' dropdown (set to 'Default System Timezone'), a 'Default app' dropdown (set to 'launcher (Home)'), and an 'Assign roles' section with a list of available roles (admin, can_delete, power, splunk-system-role, user) and a 'Selected item(s)' list (currently empty). At the bottom, there are checkboxes for 'Create a role for this user' (unchecked) and 'Require password change on first login' (checked).

- **Roles**

- **Have**

- **Authorization**

- Inheritance
 - Capabilities
 - Indexes
 - Restrictions
 - Resources

- **Don't have**

- **Authentication**

- Name
 - [Password]
 - Full Name
 - Time zone
 - Default App
 - Default app inherited from
 - Roles (can be multiple)

The 'New Role' form has a 'Name' field. Below it are tabs for '1. Inheritance', '2. Capabilities', '3. Indexes', '4. Restrictions', and '5. Resources'. The 'Inheritance' tab is active, showing a list of roles to inherit from: admin, can_delete, power, splunk-system-role, and user. A 'Role name' filter is also present.

Workshop Agenda

- Discuss Who?|What?|Why?
- Expectations
- User vs. Role
- How to Create a Role (and test with a local user) - Lab¹
- How to integrate Splunk with Active Directory - Lab²
- Map Splunk Roles to Active Directory Groups - Lab³
- Login with different users/roles/groups - Lab⁴
- How to integrate Splunk with Single Sign-On
- Other options for Authentication
- Summary

User and Role Management

Various options ...

Known SSO/MFA providers:

Cisco Secure Access by Duo
Okta Adaptive MFA
Microsoft Entra ID/AD/AD FS
Ping Identity MFA
RSA SecurID
OneLogin
Optimal IdM
CA Siteminder
Many more capable

Local Users and Roles

- + Managed via direct access
- No independent MFA
- Difficult to manage at scale

AD/LDAP

- + Managed via access to the LDAP or AD server
- + Correct team managing
- + Widely used
- + Provides fine grain control over memberships
- No independent MFA

Obvious security issues for use with Splunk Cloud ...

SAML Single Sign-On

- + Can be managed directly or via LDAP/AD integration
- + Widely used
- + Provides same control as LDAP/AD
- + Can be integrated to existing Single Sign-On (SSO)
- + Directory admins are managing the Users and the Groups, rather than Splunk Admins
- + Fully integrated into Splunk, can even use OTP, Yubikey, biometrics
- + Provide MFA services

Scripted Access

- PAM, RADIUS, or other user account systems ...
- + Additional flexibility
 - + Effectively unlimited integration
 - Need to have appropriate skill sets to design, build, and manage

Roles, Roles, Roles ...

- Five (six in Splunk Cloud) built-in roles
- admin, (sc_admin), power, and user
 - Available to users as-built out of the box
 - Good examples to clone
 - Obviously, this means no users are ever assigned to “user” or “power user” directly, always to locally modified, custom roles
- **can_delete**
 - Special role that should only be assigned temporarily (**Best Practice**)
 - Presents certain regulatory hurdles
 - Separate monitoring to capture execution and context
- splunk-system-role
 - No defined user context

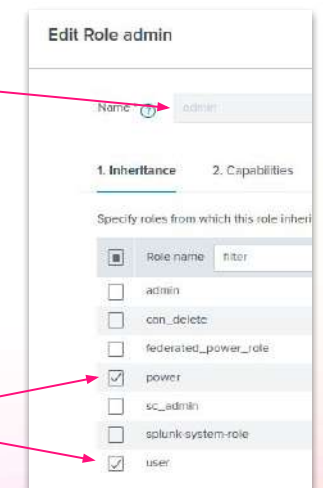
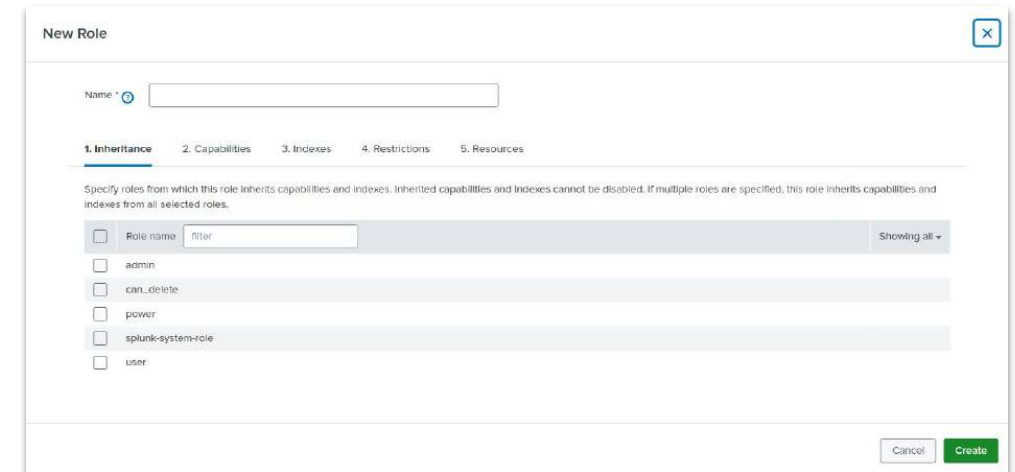


Custom Roles

- Business-specific role definition
- Permits customization to fit exactly what the business requires
- Uses capabilities to provide exactly the privileges necessary for the role
- Provide access to indexes
- Allow Splunk Administrators to restrict searches
- Provide resource availability, including using a search filter executed on every search issued by users that are members of the role
- And inheritance ...

And what, you ask, is inheritance...

- Inheritance is the passing of a role's configuration to another role
 - Very similar to other Authentication systems
- Implications
 - Any new role has all of the **configuration and settings** of the upstream role
 - Any new role has **access to all of the indexes** granted to the upstream role
 - Any new role has all of the **resource settings and configurations** of the upstream role
 - None of the configuration and settings can be **REMOVED** from an upstream role
 - Configurations and settings can **ONLY BE ADDED**
 - Spend time on building an effective inheritance strategy
 - Do avoid mistakes, use small number of capabilities, add as needed



Naming Conventions

- Be generous in your naming convention, but keep it simple and well defined
 - Make names as long as necessary to be readable but descriptive
 - Usernames will be governed by and from LDAP/AD/SSO system
 - Group names will exist (mapped from MFA/AD/SAML/SSO provider)
 - Assigning roles → Group names implies a solid mapping. In fact, if they are identical, it becomes significantly easier, permitting ...
 - Automated mapping works with SAML providers, but not LDAP
 - Be sure the names are clear as to the expected settings, but these need to be set at AD/LDAP/SSO

General Splunk Naming Conventions	https://lantern.splunk.com/Splunk_Success_Framework/Data_Management/Naming_conventions
Knowledge Object Naming Conventions	https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Developnamingconventionsforknowledgeobjecttitles
Thoughts on Naming Conventions in Splunk	https://community.splunk.com/t5/Splunk-SOAR-f-k-a-Phantom/Recommendations-for-naming-conventions-and-organization-of-m-p/501574

Emergency Users

- Always have at least **two** admin-capable users local to the system (whether Splunk Cloud or Enterprise)
 - “Break glass”-type event (External authentication provider is down and there is a security event occurring)
 - Never used other than in emergent situations and re-passworded after each use
 - Any attempted login by one of the “break glass” users should be logged and triggered
 - Username and password should be stored separately from other standard Authentication credentials.
 - Access will be via: https://<your_searchhead>/en-US/account/login?loginType=Splunk
 - Adding “/en-US/account/login?loginType=Splunk” to the end of the URL (after the trailing slash of the DNS name) bypasses the configured AD/SSO configuration, even in Splunk Cloud

How To Build a Custom Role

Strategize ...

- Understand requirements
 - What is the end goal of the role's purpose?
 - What are the minimum settings required to achieve that goal?
 - Are there any other teams within the organization that have similar responsibilities where an existing Splunk role could be reused?
 - Is role layering using inheritance or duplicating the role entirely the correct path?
- Buildout of Role
 - **Inheritance** - Are any configurations derived from another role?
 - **Capabilities** - What specific abilities are required within the role?
 - **Indexes** - What data needs to be available to search?
 - **Restrictions** - Should there be search or resource restrictions for the role?
 - **Resources** - What compute resources should be available to the role?

Workshop Agenda

- Discuss Who?|What?|Why?
- Expectations
- User vs. Role
- How to Create a Role (and test with a local user) - Lab¹
- How to integrate Splunk with Active Directory - Lab²
- Map Splunk Roles to Active Directory Groups - Lab³
- Login with different users/roles/groups - Lab⁴
- How to integrate Splunk with Single Sign-On
- Other options for Authentication
- Summary

Explore Splunk roles

Goal



- Generate a user capable of executing the use case goals
- When complete:
 - A role created with the requirements met
 - A user connected to the role
 - A test of the requirements by logging in as the user and attempting to use resources assigned

Let's Build a Custom Role

Use Case



- Use case: Create a dashboard developer role for the Finance organization, this role will build dashboards for Finance to better understand operations in the Finance Department
 - First, understand the requirements for the Use Case
 - Needs to be able to
 - Build dashboards
 - Run searches (including metrics)
 - Schedule searches
 - Install and edit apps
 - Access specific indexes
 - Limit the number of searches that can be executed concurrently to 6

Group Name for Role



- Work with your User management group (AD/LDAP/SSO admins) to get the name approved through governance ... this has long-term implications, so consider your requirements carefully, you will reuse the decision
- Ensure the name on the Splunk system (whether Cloud or Enterprise) match the imported group from AD/SAML
- Frequently: <biz_org>_<employeeType>_<roleName> works

General Splunk Naming Conventions	https://lantern.splunk.com/Splunk_Success_Framework/Data_Management/Naming_conventions
Knowledge Object Naming Conventions	https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Developnamingconventionsforknowledgeobjecttitles
Thoughts on Naming Conventions in Splunk	https://community.splunk.com/t5/Splunk-SOAR-f-k-a-Phantom/Recommendations-for-naming-conventions-and-organization-of/m-p/501574

Create the Role

Inheritance



- Create the Role with an appropriate name
- Define the role from which to inherit the base settings (here **buttercup_base_power**)

New Role

Name buttercup_finance_dev_reports

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.

	Role name	filter	Showing all ▼
<input type="checkbox"/>	admin		
<input checked="" type="checkbox"/>	buttercup_base_power		
<input type="checkbox"/>	buttercup_base_user		
<input type="checkbox"/>	can_delete		
<input type="checkbox"/>	power		
<input type="checkbox"/>	splunk-system-role		
<input type="checkbox"/>	user		

Cancel Create

Create the Role

Capabilities



- Define the capabilities to be added

- run_msearch
- schedule_search
- install_apps
- edit_local_apps

New Role

Name *

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

Select specific capabilities for this role.

Capability Name
<input checked="" type="checkbox"/> run_msearch

New Role

Name *

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

Select specific capabilities for this role.

Capability Name
<input checked="" type="checkbox"/> install_apps

New Role

Name *

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

Select specific capabilities for this role.

Capability Name
<input checked="" type="checkbox"/> install_apps

New Role

Name *

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

Select specific capabilities for this role.

Capability Name
<input checked="" type="checkbox"/> edit_local_apps

Create the Role

Indexes



- Define the indexes the role should have access to
 - finance_monitor
 - finance_security
 - finance_web-purchases

The screenshot shows the 'New Role' configuration page in Splunk. The 'Name' field is set to 'buttercup_finance_dev_reports_power'. The 'Indexes' tab is selected, showing a table of indexes. The 'Included' column has checkboxes for each index, and the 'Default' column has checkboxes. The 'Showing all' dropdown is set to 'all'. A pink arrow points from the 'finance_web-purchases' item in the list to the 'Included' checkbox, which is checked.

Index Name	Included	Default
._internal	<input type="checkbox"/>	<input type="checkbox"/>
._internalbucket	<input type="checkbox"/>	<input type="checkbox"/>
finance_monitor	<input checked="" type="checkbox"/>	<input type="checkbox"/>
finance_security	<input checked="" type="checkbox"/>	<input type="checkbox"/>
finance_web-purchases	<input checked="" type="checkbox"/>	<input type="checkbox"/>
history	<input type="checkbox"/>	<input type="checkbox"/>
main	<input type="checkbox"/>	<input type="checkbox"/>
summary	<input type="checkbox"/>	<input type="checkbox"/>

Create the Role

Restrictions



- No restrictions on this page for this role ...

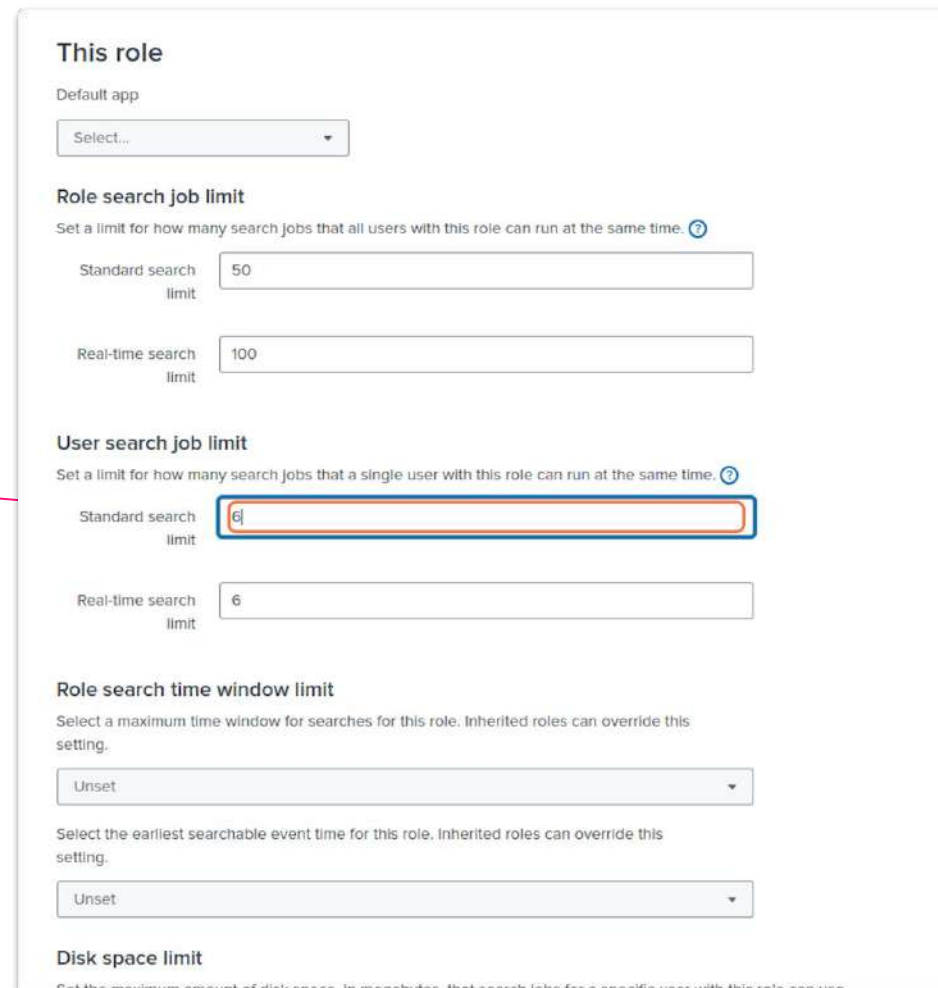
The screenshot shows the 'New Role' dialog box with the 'Restrictions' tab selected. The 'Name' field contains 'buttercup_finance_clay_reports_power'. The 'Restrict searches' section has a 'Search filter generator' on the left and a 'Search filter' text area on the right. The 'Search filter generator' includes a 'Indexed field and values time range' dropdown set to '60 seconds', an 'Indexed fields' dropdown, a 'Values' dropdown, and a 'Concatenation option' dropdown set to 'OR'. A 'Generated search filter' text area is at the bottom of the generator. The 'Search filter' text area is empty. A note on the right states: 'Note: the search filter can only include: source type, source, host, index, event type, search fields, the operators: "*", "OR", "AND", "NOT"'. At the bottom right are 'Cancel' and 'Create' buttons.

Create the Role

Resources

- Resource restrictions
 - Six searches permitted concurrently (to avoid runaways)
- Hit the **Create** button

```
[splunk@ip-172-31-42-94 local]$ pwd
/opt/splunk/etc/system/local
[splunk@ip-172-31-42-94 local]$ grep -E -A10 finance_dev_reports authorize.conf
[role_buttercup_finance_dev_reports]
edit_local_apps = enabled
importRoles = buttercup_base_power
install_apps = enabled
rtSrchJobsQuota = 0
srchIndexesAllowed = finance_monitor;finance_security;finance_web-purchases
srchJobsQuota = 6
srchMaxTime = 8640000
srchTimeEarliest = -1
srchTimeWin = -1
```



This role

Default app
Select...

Role search job limit
Set a limit for how many search jobs that all users with this role can run at the same time. ?

Standard search limit: 50

Real-time search limit: 100

User search job limit
Set a limit for how many search jobs that a single user with this role can run at the same time. ?

Standard search limit: 6

Real-time search limit: 6

Role search time window limit
Select a maximum time window for searches for this role. Inherited roles can override this setting.
Unset

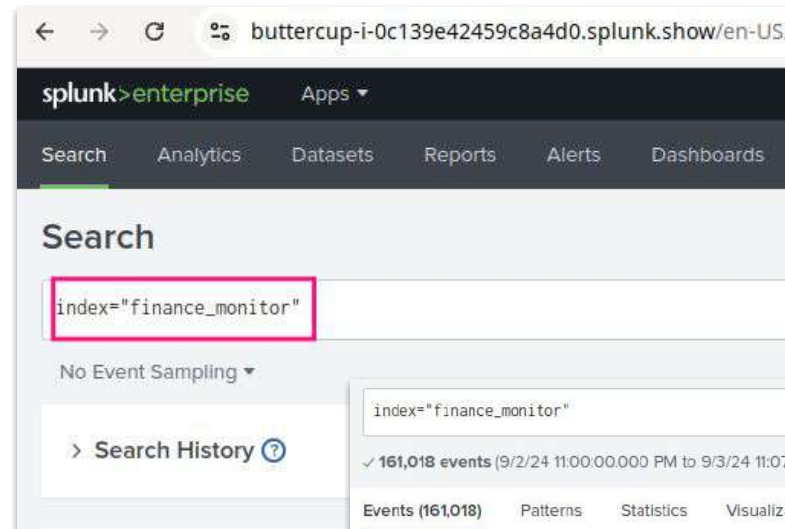
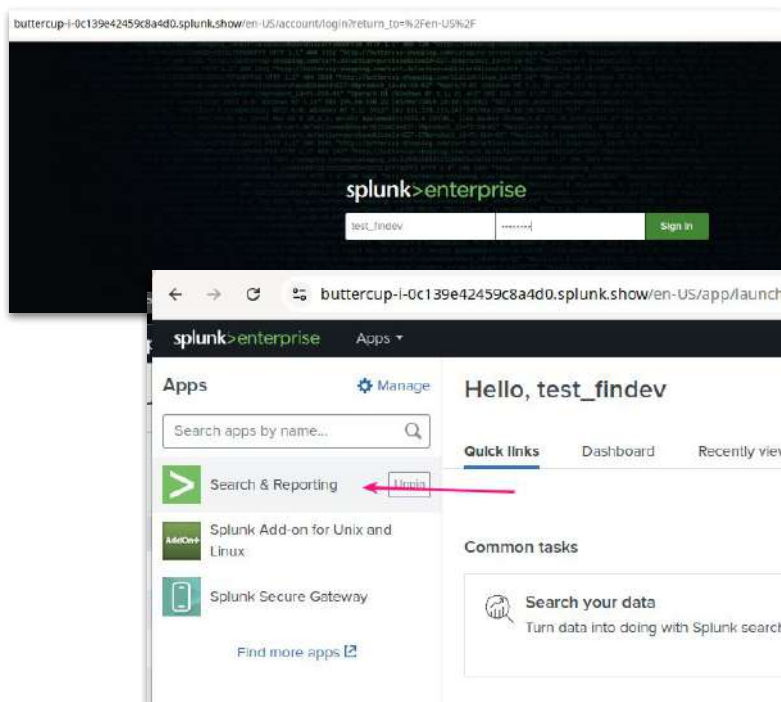
Select the earliest searchable event time for this role. Inherited roles can override this setting.
Unset

Disk space limit
Set the maximum amount of disk space, in megabytes, that search jobs for a specific user with this role can use.

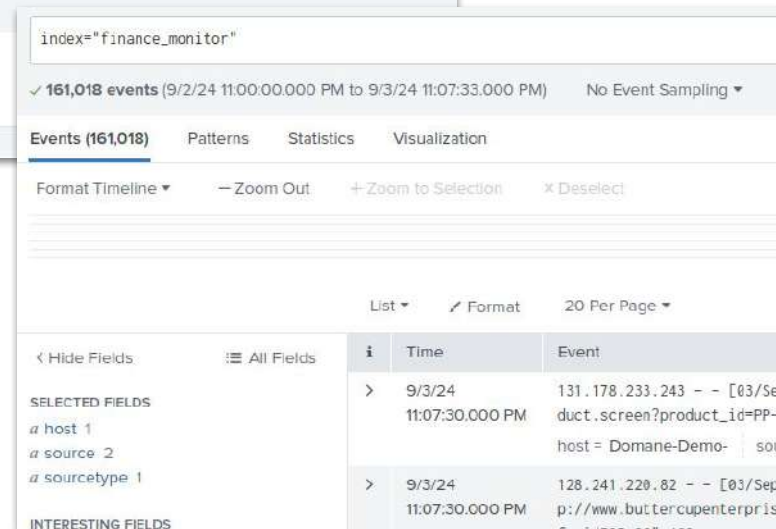


Ready-to-use Custom Role

Test - Test - Test



- Skip “take the tour?” twice ...



Ready-to-use Custom Role

Test - Test - Test



- Test locally

- Add a local user with an obvious to-be-removed name (test_findev) to validate the role behaves as expected
 - Create and edit local apps, schedule searches, and execute metrics searches
 - Access the finance_monitor, finance_security, and finance_web-purchases indexes
 - Attempt to execute more than six searches (see the seventh fail)
 - Remove temporary user ... don't forget this!

Workshop Agenda

- Discuss Who?|What?|Why?
- Expectations
- User vs. Role
- How to Create a Role (and test with a local user) - Lab¹
- How to integrate Splunk with Active Directory - Lab²
- Map Splunk Roles to Active Directory Groups - Lab³
- Login with different users/roles/groups - Lab⁴
- How to integrate Splunk with Single Sign-On
- Other options for Authentication
- Summary

Explore external auth in Splunk



Goal

- Generate a user capable of executing the use case goals, via an externally provided authentication process
- When complete:
 - Splunk instance connected to and using authentication and group membership from an Active Directory (AD) instance
 - A role connected to the group
 - A test of the requirements by logging in as an AD user and attempting to use resources assigned

Connect Splunk -> external Auth

AD/LDAP



- Friendly AD/LDAP administrator a **requirement**
 - Send them to the link (in references as well)
- One time configuration
- Ensure the splunk groups are nested under a separate leaf
- Build the authentication connection on a single machine, pull
\$SPLUNK_HOME/etc/system/local/authentication.conf and replicate via app
- Shared_secret permits not having plain-text passwords
- Requirements
 - LDAP strategy name
 - Host
 - User base DN
 - User name attribute
 - Real name attribute
 - Group base DN
 - Group name attribute
 - Static member attribute

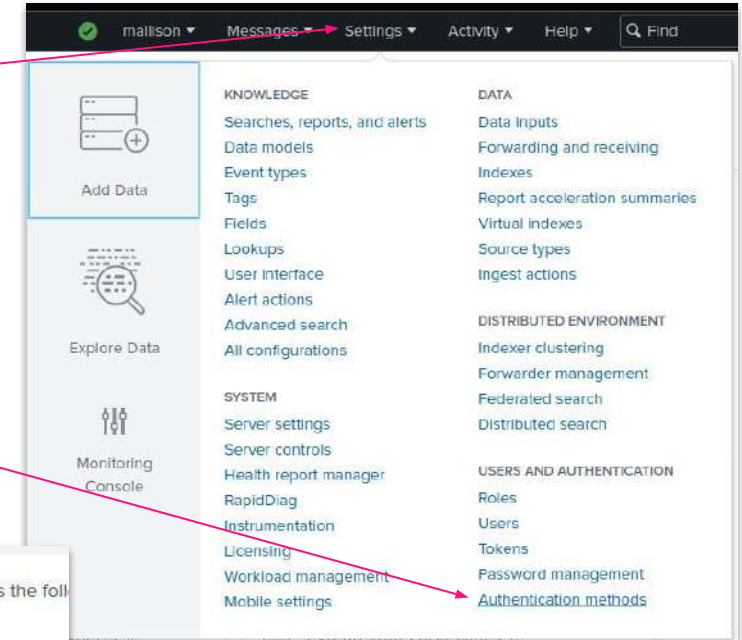
Setup authentication with LDAP	https://docs.splunk.com/Documentation/Splunk/latest/Security/SetupuserauthenticationwithLDAP
Configure MS AD FSfor use with Splunk	https://www.splunk.com/en_us/blog/tips-and-tricks/configuring-microsofts-adfs-splunk-cloud.html
LDAP auth configuration tips	https://www.splunk.com/en_us/blog/tips-and-tricks/ldap-auth-configuration-tips.html

Connect Splunk -> external Auth

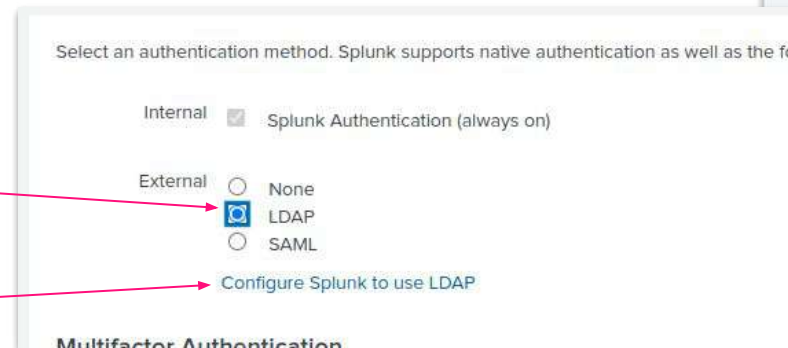
AD/LDAP



- Settings
- Authentication methods



- LDAP
- Configure Splunk to use LDAP



Setup authentication with LDAP	https://docs.splunk.com/Documentation/Splunk/latest/Security/SetupuserauthenticationwithLDAP
LDAP auth configuration tips	https://www.splunk.com/en_us/blog/tips-and-tricks/ldap-auth-configuration-tips.html

Connect Splunk -> external Auth

AD/LDAP



*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 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.

Bind DN Password
Enter the password for your Bind DN user.

Confirm password

User settings

* User base DN
The location of your LDAP users, specified by the DN of your user subtree. If necessary, you can specify several DNs separated by semicolons.

User base filter
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)'

* User name attribute
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'.

* Real name attribute
The user attribute that contains a human readable name. This is typically 'cn' (common name) or 'displayName'.

Windows Active Directory Running

rdp://34.219.127.39 [🔗](#)

Instance ID	Termination Date	User ID
665a359458b10bf59c416205	1 hour 36 minutes left	-

Connection Information

Username	Administrator 🔗
Admin Password 🔗
Remote Desktop	rdp://34.219.127.39 🔗
Admin Username	admin 🔗

Setup authentication with LDAP	https://docs.splunk.com/Documentation/Splunk/latest/Security/SetupuserauthenticationwithLDAP
LDAP auth configuration tips	https://www.splunk.com/en_us/blog/tips-and-tricks/ldap-auth-configuration-tips.html

Connect Splunk -> external Auth

AD/LDAP



The screenshot shows the 'LDAP configuration' interface in Splunk. Red arrows point to the following fields:

- Group base DN***: Set to 'CN=Users,DC=buttercup,DC=local'. Description: 'The location of your LDAP groups, specified by the DN of your group subtree. If necessary, you can specify several DNs separated by semicolons.'
- Group name attribute***: Set to 'cn'. Description: 'The group attribute that contains the group name. A typical value for this is 'cn'.'
- Static member attribute***: Set to 'member'. Description: '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.'
- Save button**: A green button at the bottom right.

Other visible fields include:

- Email attribute**: Empty. Description: 'The user attribute that contains the user's email address. This is typically 'mail'.'
- Group mapping attribute**: Empty. Description: '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.'
- Static group search filter**: Empty. Description: '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)'.'
- Dynamic group settings**: Includes 'Dynamic member attribute' and 'Dynamic group search filter', both empty.
- Advanced settings**: A checkbox that is currently unchecked.

Setup authentication with LDAP	https://docs.splunk.com/Documentation/Splunk/latest/Security/SetupuserauthenticationwithLDAP
LDAP auth configuration tips	https://www.splunk.com/en_us/blog/tips-and-tricks/ldap-auth-configuration-tips.html

Connect Splunk -> external Auth

AD/LDAP



filter				25 per page	
LDAP strategy name	Host	Port	Connection order	Status	Actions
buttercup_base		389	1	Enabled Disable	Map groups Clone Delete

- Successful connection to the AD server listed under “Host”
- Name, as defined, “buttercup_base”

Workshop Agenda

- Discuss Who?|What?|Why?
- Expectations
- User vs. Role
- How to Create a Role (and test with a local user) - Lab¹
- How to integrate Splunk with Active Directory - Lab²
- Map Splunk Roles to Active Directory Groups - Lab³
- Login with different users/roles/groups - Lab⁴
- How to integrate Splunk with Single Sign-On
- Other options for Authentication
- Summary

Map Splunk Roles -> AD Groups

AD/LDAP



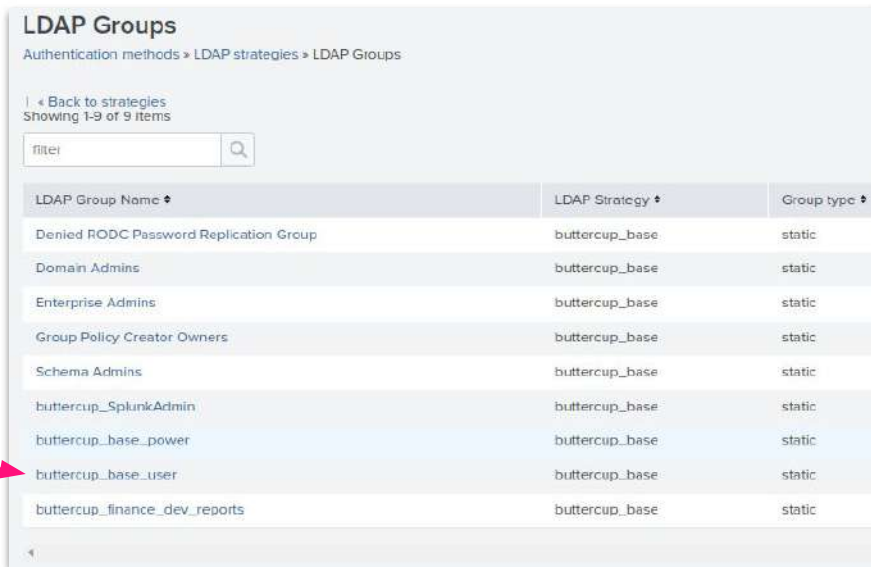
A screenshot of the Splunk AD/LDAP configuration interface. At the top, there is a search bar labeled "filter" and a magnifying glass icon. To the right, it says "25 per page". Below this is a table with the following columns: "LDAP strategy name", "Host", "Port", "Connection order", "Status", and "Actions". The first row of the table has the following values: "buttercup_base", a redacted host name, "389", "1", "Enabled | Disable", and "Map groups | Clone | Delete". A red arrow points from the top right towards the "Map groups" link in the "Actions" column.

LDAP strategy name	Host	Port	Connection order	Status	Actions
buttercup_base	[REDACTED]	389	1	Enabled Disable	Map groups Clone Delete

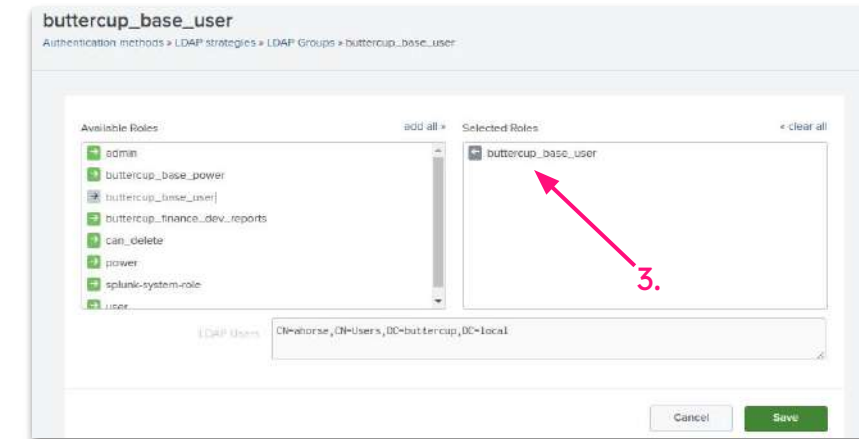
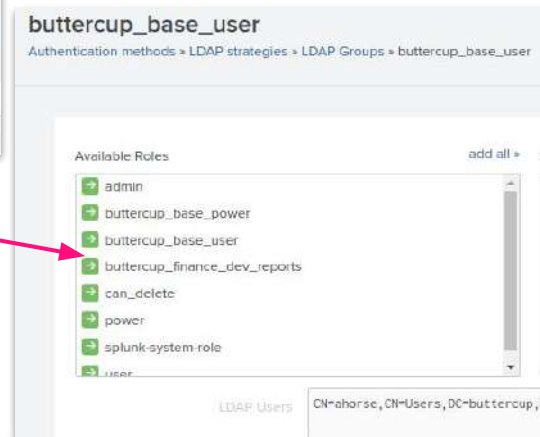
- From the previously successful lab ...

Map Splunk Roles -> AD Groups

AD/LDAP



1. Select "buttercup_base_user"
2. On the next screen, click on the Role "buttercup_base_user" to associate the group to the role
3. See the role associated to the group
4. Click "Save"



Map Splunk Roles -> AD Groups

AD/LDAP



- Continue with the same process to associate the AD groups with the 'samename' Splunk role:
 - "buttercup_base_power"
 - "buttercup_finance_dev_reports"
- ... except for "buttercup_SplunkAdmin"
 - Associate that with "admin"

Workshop Agenda

- Discuss Who?|What?|Why?
- Expectations
- User vs. Role
- How to Create a Role (and test with a local user) - Lab¹
- How to integrate Splunk with Active Directory - Lab²
- Map Splunk Roles to Active Directory Groups - Lab³
- Login with different users/roles/groups - Lab⁴
- How to integrate Splunk with Single Sign-On
- Other options for Authentication
- Summary

Login with different users/roles/groups



- Select known user from AD group/Splunk Role

- “ahorse” = “buttercup_user_base”
- “bhorse” = “buttercup_power_base”
- “chorse” = “buttercup_finance_dev_reports”
- “dhorse” = “buttercup_SplunkAdmins”
- “d_admin01” = “Domain Admins”
- “d_splk01” = “Domain Admins”
- Paragon of security, all passwords = “SplunkRocks!”



- Login as each of the “horses” and attempt to read the index “finance_monitor”

- Some user’s searches work, and some don’t, why?



Test the AD connection



- Select known user from AD group
- Have user login and attempt to read the index “finance_monitor”
- Diagnose
- Troubleshoot
- Resolve ...

Workshop Agenda

- Discuss Who?|What?|Why?
- Expectations
- User vs. Role
- How to Create a Role (and test with a local user) - Lab¹
- How to integrate Splunk with Active Directory - Lab²
- Map Splunk Roles to Active Directory Groups - Lab³
- Login with different users/roles/groups - Lab⁴
- **How to integrate Splunk with Single Sign-On**
- Other options for Authentication
- Summary

Connect Splunk -> External Auth

SAML SSO



- Splunk Authentication Management

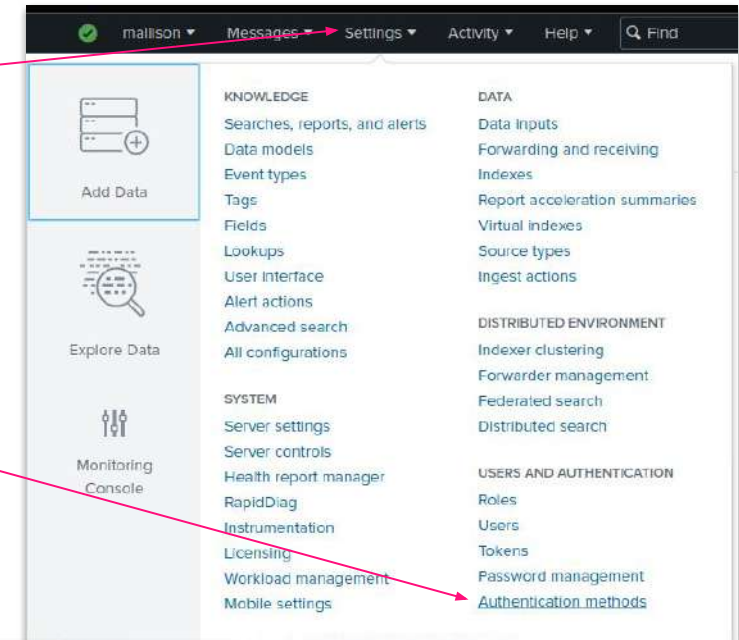
- Best Practice: Always integrate with a Directory Server ...
 - External SSO should be fed by locally controlled/managed AD
- Users exist only in groups, and the groups are ingested (via integration) from AD/SSO
- Secondary leaf contains all Splunk Groups/Users
- Awareness of limitations regarding SSO is essential. Splunk only supports a single SSO integration, meaning that if more than one SSO provider is required, there will be challenges.

Connect Splunk -> external Auth

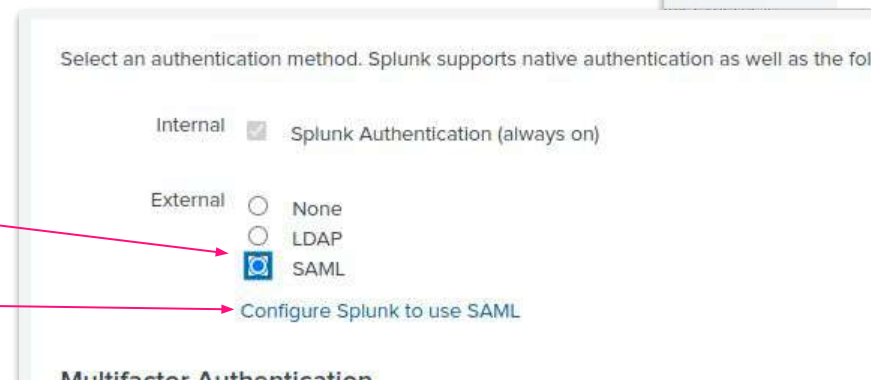
SAML SSO



- Settings
- Authentication methods



- SAML
- Configure Splunk to use SAML



Connect Splunk -> external Auth

SAML SSO



- Cloud or Enterprise SAML SSO provider
 - Something of a black box from Splunk's perspective
 - A service that Splunk uses (and monitors)
 - Should be secure
 - Optimal, fed from AD -> external Auth
- Friendly SSO administrator a **requirement**
 - Send them to the link (in references as well)
- Try very hard to get the XML file
- Otherwise ... Create SAML strategy by hand
- If there is a requirement for MFA, third-party solutions (Okta, Ping, etc.) work extremely well, and, in Splunk Cloud, are effectively required

<https://docs.splunk.com/Documentation/Splunk/latest/Security/HowSAMLSSOworks>

Connect Splunk -> external Auth

SAML SSO



- Click on SP Metadata File, send to SSO admin
 - Friendly SSO administrator a **requirement**
 - Send them to the link (in references as well)
- Click on Metadata XML File
- Select file from storage
- See settings auto-populate
- Click on **Save**

Configure single sign-on with SAML	https://docs.splunk.com/Documentation/Splunk/latest/Security/HowSAMLSSOWorks
Connecting Splunk to Okta	https://lantern.splunk.com/Data_Descriptors/Okta/Enabling_Okta_single_sign-on_in_the_Splunk_platform

SAML Configuration

Configure SAML for Splunk. [Learn More](#)

Download the SP Metadata from Splunk and add it to your SAML environment to connect to Splunk.

SP Metadata File

Import Identity Provider (IdP) metadata by browsing to an XML file, or copy and paste the information into the Metadata Contents text box.

Metadata XML File

Metadata Contents

General Settings

Single Sign-On (SSO) URL

Single Log Out (SLO) URL

IdP certificate path

IdP certificate chains

Replicate Certificates ☒

Issuer ID

Entity ID

Sign AuthnRequest ☒

Attribute Query Requests

Authentication Extensions

Alias

Advanced Settings

Name ID Format

Fully qualified domain name or IP of the load balancer

Redirect port - load balancer port

Redirect to URL after logout

SAML Binding

SLO Binding

Connect Splunk -> external Auth

SAML SSO - Troubleshooting



- How to get to a local login when SAML is no longer functioning ...
 - The trailing URL will be “/en-US/account/login?loginType=splunk”
 - Hence -
 - https://<sh_instance>/en-US/account/login?loginType=splunk
 - Using the local logins generated at instance creation, login, diagnose the failure of SAML with Splunk, and then revert
 - Explore the errors and responses in ‘_internal’
- Information passed back from the SAML provider via headers
 - Chrome extension ‘SAML Panel’ [link](#)
 - Firefox extension ‘SAML Message Decoder’ [link](#)
 - Microsoft Edge Add-on (just for confusion ...) - ‘SAML, WS-Federation and OAuth 2.0 tracer’ [link](#)

Workshop Agenda

- Discuss Who?|What?|Why?
- Expectations
- User vs. Role
- How to Create a Role (and test with a local user) - Lab¹
- How to integrate Splunk with Active Directory - Lab²
- Map Splunk Roles to Active Directory Groups - Lab³
- Login with different users/roles/groups - Lab⁴
- How to integrate Splunk with Single Sign-On
- Other options for Authentication
- Summary

Reverse Proxy (SSO) is supported

- To configure, be sure to have the network admin available to ensure correct configuration
- Settings
 - Pay attention to the 'trustedIP' settings, two exist - server.conf and web.conf
 - Understand the remoteUser SAML attribute
 - Be aware of the configuration requirements for the potential root_endpoint modifications

Configure Splunk to use a Reverse Proxy	https://docs.splunk.com/Documentation/Splunk/latest/Security/ConfigureSplunkSSO
SSO using a reverse proxy	https://docs.splunk.com/Documentation/Splunk/latest/Security/HowSplunkSSOworks

External Auth

Scripted Authentication



- Other types of authentication are available
 - RADIUS
 - PAM
- Create a python script that sends the **userLogin**, **getUserInfo**, and **getUsers** authentication functions relevant to Splunk

External Auth

Direct MFA

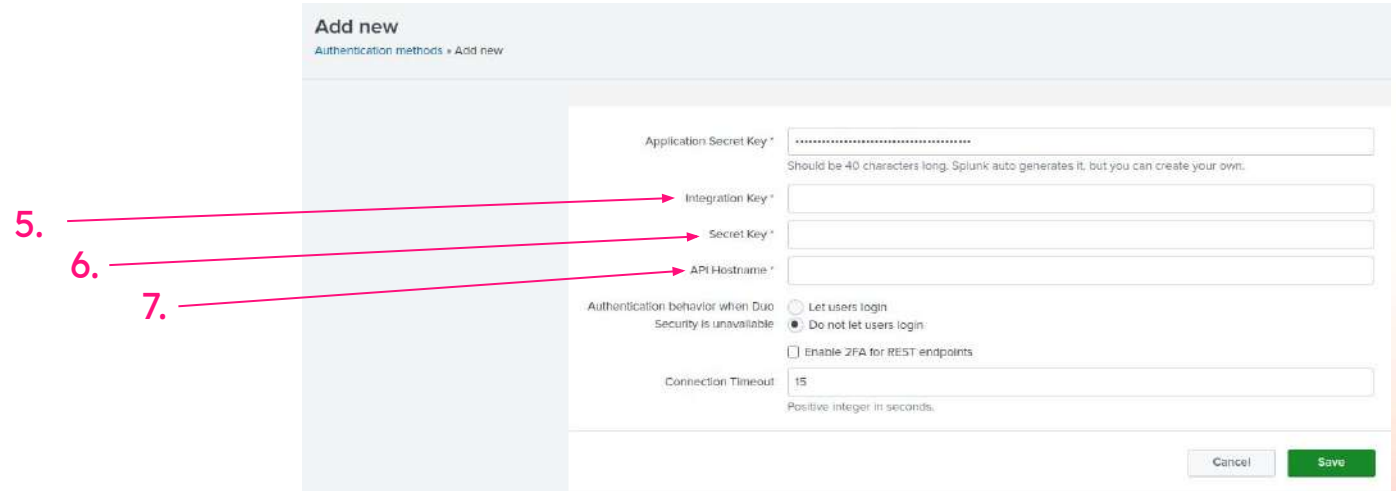
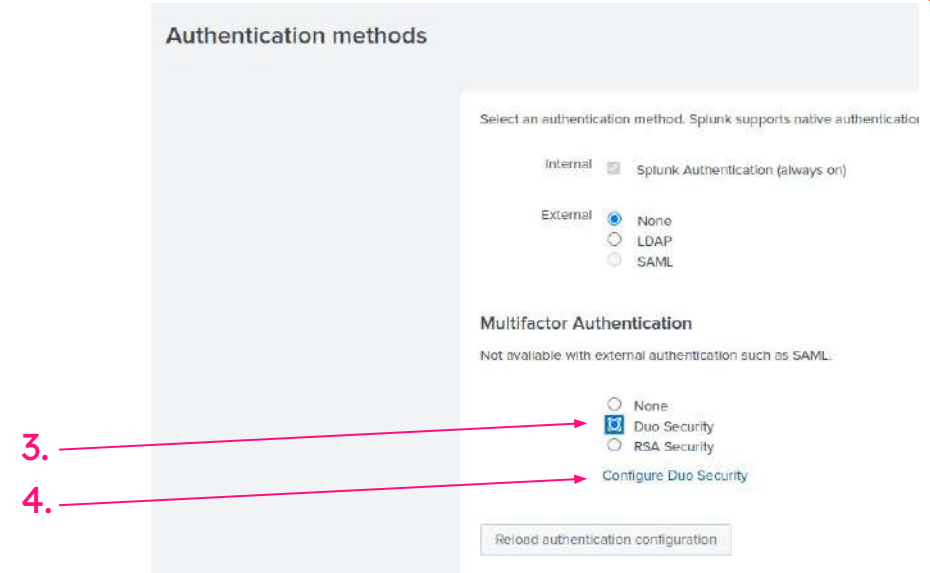
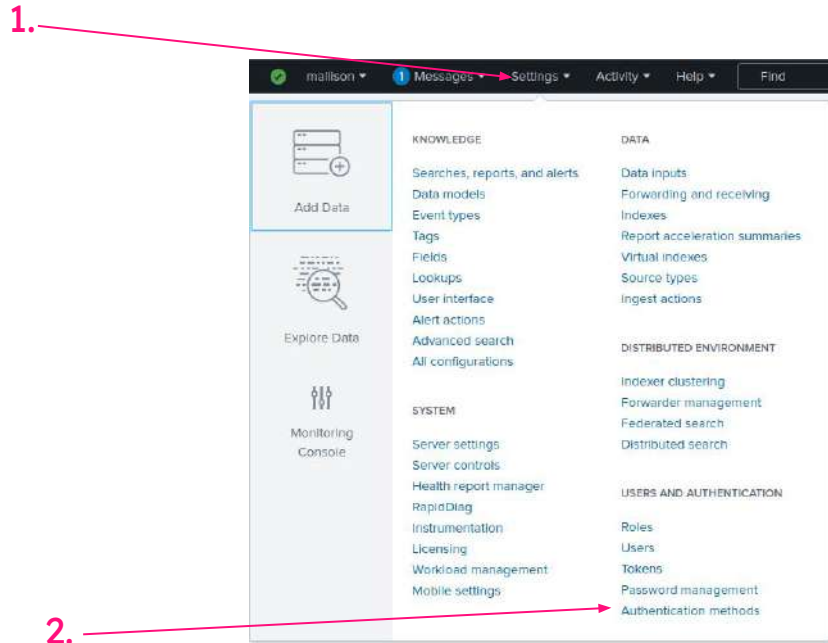


- Splunk supports the capability to interact directly with two MFA providers (Cisco Secure Access by Duo and RSA SecurID)
- Exclusive MFA - no additional external Auth [LDAP,SSO]

External Auth



Step sequence of how to get to the Duo configuration page.



SSO Monitoring



- Track access time (latency) and availability using synthetic monitoring
- Splunkbase Apps/TAs for SSO IdP providers
- SSO access becomes essential for the function of Splunk, and therefore affects the usability and value of Splunk
- Understanding the dependencies and track carefully
- Example : SOC integration
 - If SOC workers are unable to use Splunk, obviously, the security of the entire organization is compromised
- Ensure High Availability by design

SplunkBase (non-Splunk supported) - User Role Checker	https://splunkbase.splunk.com/app/4111
SplunkBase (non-Splunk supported) - Alert action for SAML user role map removal	https://splunkbase.splunk.com/app/5682

Workshop Agenda

- Discuss Who?|What?|Why?
- Expectations
- User vs. Role
- How to Create a Role (and test with a local user) - Lab¹
- How to integrate Splunk with Active Directory - Lab²
- Map Splunk Roles to Active Directory Groups - Lab³
- Login with different users/roles/groups - Lab⁴
- How to integrate Splunk with Single Sign-On
- Other options for Authentication
- Summary

User Management Summary

- Use local users sparingly, but ensure there are two available admins for “break glass” emergencies
- Track those users carefully, should not be used for anything other than emergency
- Off-host user management means that the Splunk Admins are NOT doing user management. This ensures better security and permits SSO/MFA more easily
- Ensure solid passwords using Splunk password control or the SSO/AD provider

Role Management Summary

- Roles are where the “good” stuff lives
 - Capabilities, access to indexes, search restrictions, resource restrictions, app context
 - Integration with off-host service providers ensures that the only aspect of administration that must be managed is the roles themselves, not necessarily membership by users in a role
 - Automatic role→group mapping provides lessening of administrative overhead, but can be done with manual mapping

SSO Management Summary

- Make friends with the AD/SSO administrator(s)
- Use AD/LDAP for Group/User memberships
 - Use a good naming convention for the groups
 - Sub-leaves to hold Splunk groups
- Feed AD/LDAP groups to SSO providers
- Use export for Metadata XML
- Use XML import for SSO definitions ... so much easier
- Ensure Role taxonomy matches Group taxonomy from SSO
- Track provider access and latency, slow SSO = slow Splunk

References

Create New Users	https://docs.splunk.com/Documentation/SplunkCloud/latest/Security/Addandeditusers
Create New Roles	https://docs.splunk.com/Documentation/Splunk/latest/Security/Rolesandcapabilities
Setup authentication with LDAP	https://docs.splunk.com/Documentation/Splunk/latest/Security/SetupuserauthenticationwithLDAP
Configure AD for use with Splunk	https://www.splunk.com/en_us/blog/tips-and-tricks/configuring-microsofts-adfs-splunk-cloud.html
LDAP auth configuration tips	https://www.splunk.com/en_us/blog/tips-and-tricks/ldap-auth-configuration-tips.html
Setup SAML SSO	https://docs.splunk.com/Documentation/Splunk/latest/Security/HowSAMLSSOworks
Troubleshooting SAML SSO	https://docs.splunk.com/Documentation/Splunk/latest/Security/TroubleshootSAMLSSO
Chrome extension : "SAML Chrome Panel"	https://chromewebstore.google.com/detail/saml-chrome-panel/paijfdbeenhembfhkhllainmocckace
Firefox extension : SAML Message Decoder	https://addons.mozilla.org/en-US/firefox/addon/saml-message-decoder-extension/
Edge Add-on : SAML, WS-Federation and OAuth 2.0 tracer	https://microsoftedge.microsoft.com/addons/detail/saml-wsfederation-and-o/boffpaecgbbopkboijhbmhecoefdehi
How-to with Shared Secrets	https://www.splunk.com/en_us/blog/tips-and-tricks/store-encrypted-secrets-in-a-splunk-app.html
Sync passwd file with splunk.secret	https://community.splunk.com/t5/Security/Synchronizing-the-passwd-file-between-Splunk-servers-with-a/m-p/234350
Splunk.secret information	https://community.splunk.com/t5/Knowledge-Management/What-is-the-splunk-secret-file-and-is-it-possible-to-change-it/m-p/331207
Distributed search KO/user replication	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/HowconfrepoworksinSHC
Securing the Splunk Cloud Platform (discussion about User and Role Management inherent)	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Administration/Securing_the_Splunk_Cloud_Platform
Connecting Splunk to Okta	https://lantern.splunk.com/Data_Descriptors/Okta/Enabling_Okta_single_sign-on_in_the_Splunk_platform
Configure Splunk to use a Reverse Proxy	https://docs.splunk.com/Documentation/Splunk/latest/Security/ConfigureSplunkSSO
SSO using a reverse proxy	https://docs.splunk.com/Documentation/Splunk/latest/Security/HowSplunkSSOworks
Splunk scripted authentication	https://docs.splunk.com/Documentation/Splunk/latest/Security/Createtheauthenticationscript
Splunk Direct Multi-Factor Authentication	https://docs.splunk.com/Documentation/Splunk/latest/Security/AboutMultiFactorAuth
General Splunk Naming Conventions	https://lantern.splunk.com/Splunk_Success_Framework/Data_Management/Naming_conventions
Knowledge Object Naming Conventions	https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Developnamingconventionsforknowledgeobjecttitles
Thoughts on Naming Conventions in Splunk	https://community.splunk.com/t5/Splunk-SOAR-f-k-a-Phantom/Recommendations-for-naming-conventions-and-organization-of/m-p/501574
SplunkBase (non-Splunk supported) - User Role Checker	https://splunkbase.splunk.com/app/4111
SplunkBase (non-Splunk supported) - Alert action for SAML user role map removal	https://splunkbase.splunk.com/app/5682

Thank you