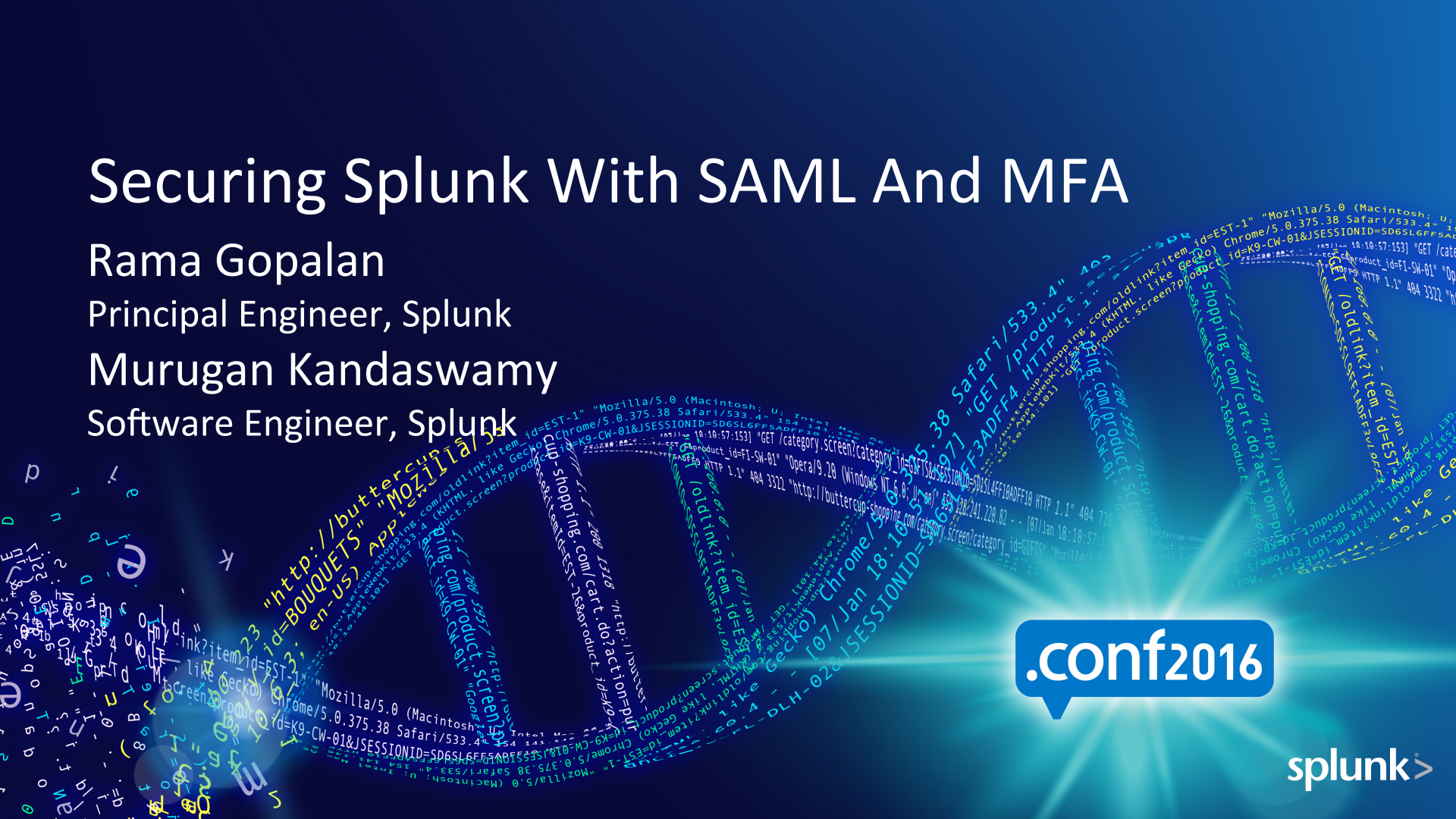
Securing Splunk With SAML And MFA

Rama Gopalan

Principal Engineer, Splunk

Murugan Kandaswamy

Software Engineer, Splunk



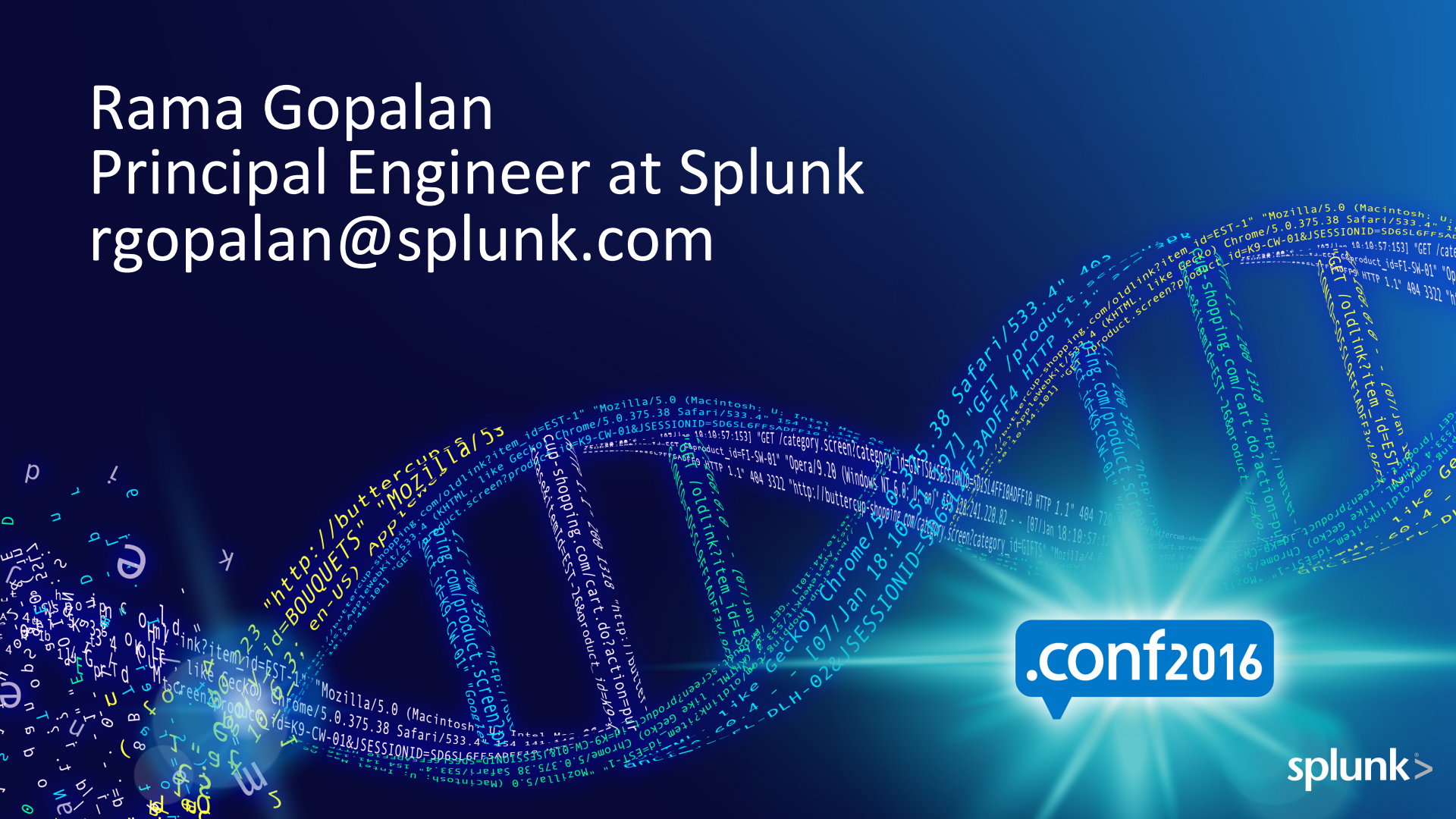
.conf2016

splunk>

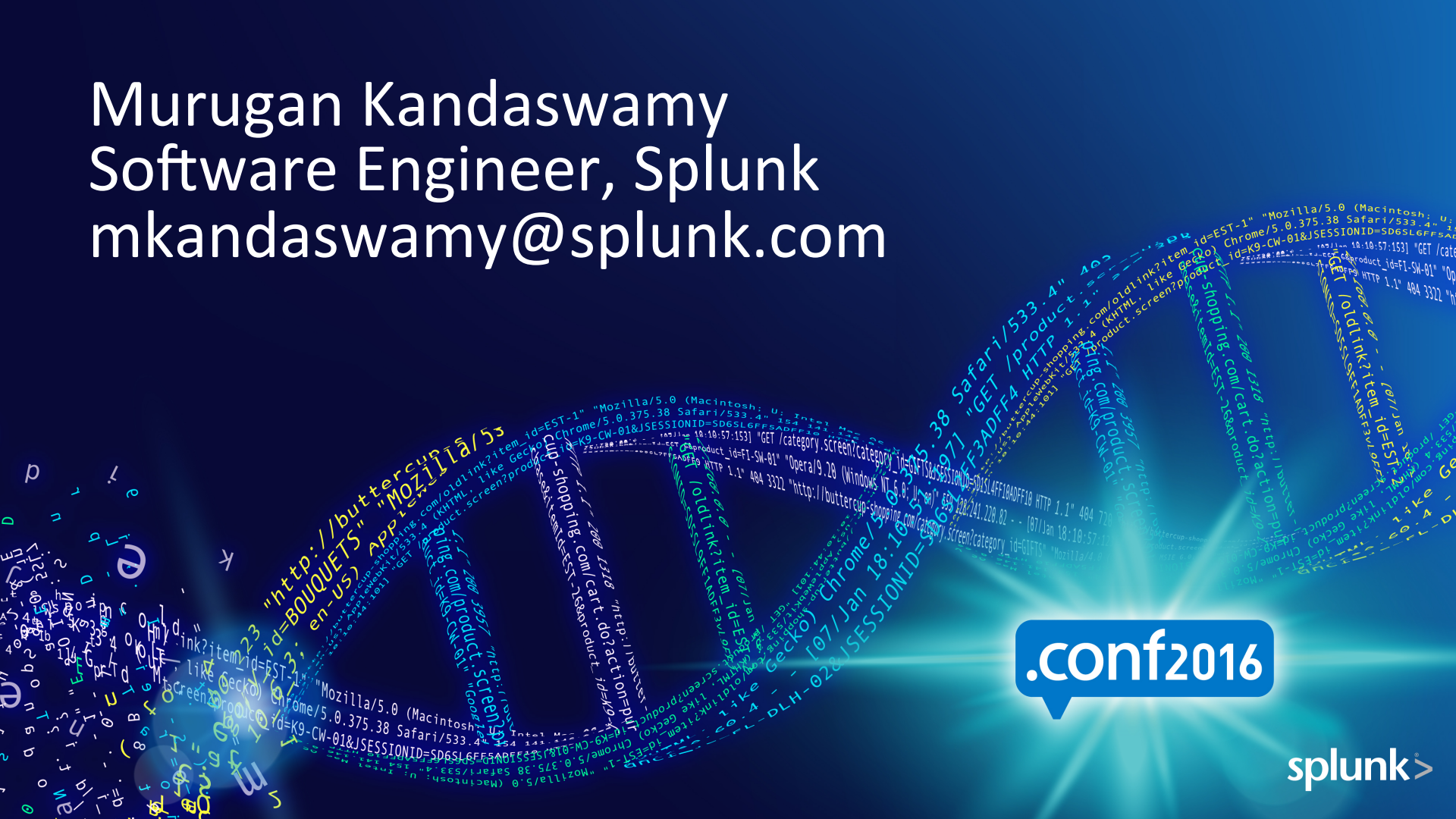
Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make. In addition, any information about 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. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Rama Gopalan
Principal Engineer at Splunk
rgopalan@splunk.com



Murugan Kandaswamy
Software Engineer, Splunk
mkandaswamy@splunk.com

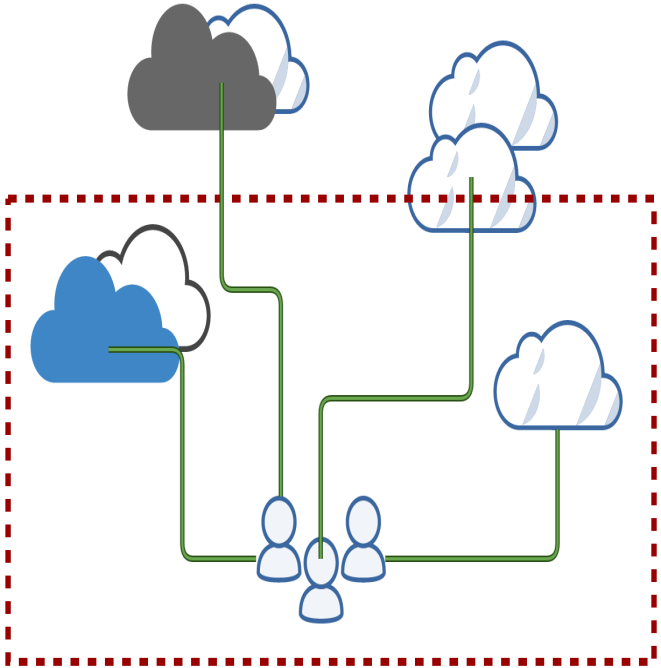


Agenda

- SSO
  - Proxy + LDAP
  - Proxy SSO
  - SAML 2.0
- MFA With Splunk, LDAP And Scripted Authentication

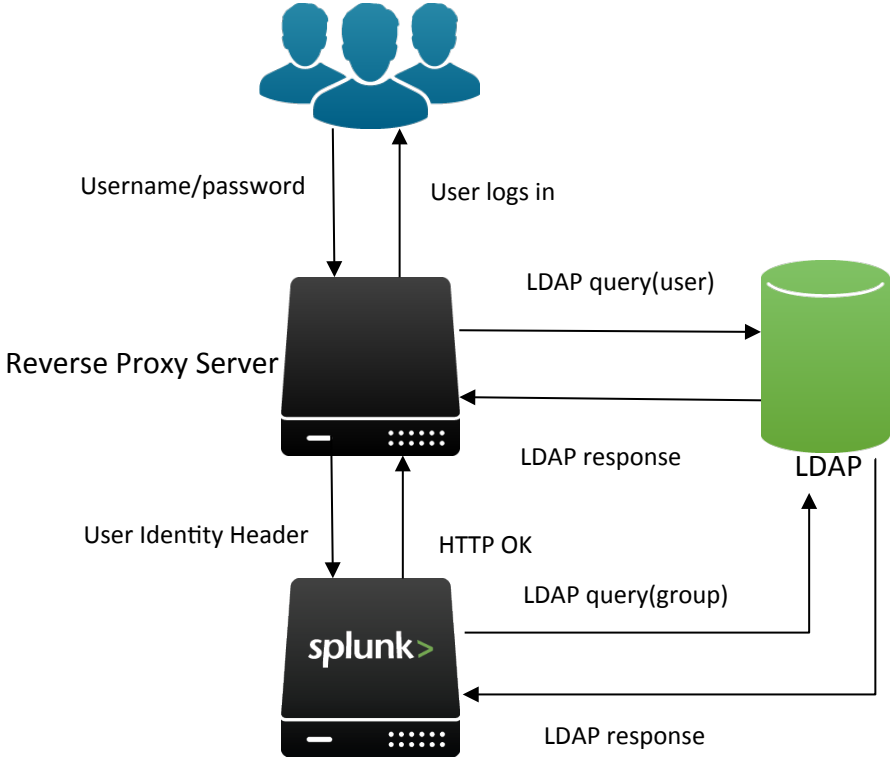
Why Single Sign On

- Reduce Administration
- Time Savings for Users
- Increase User Adoption
- Increased Security

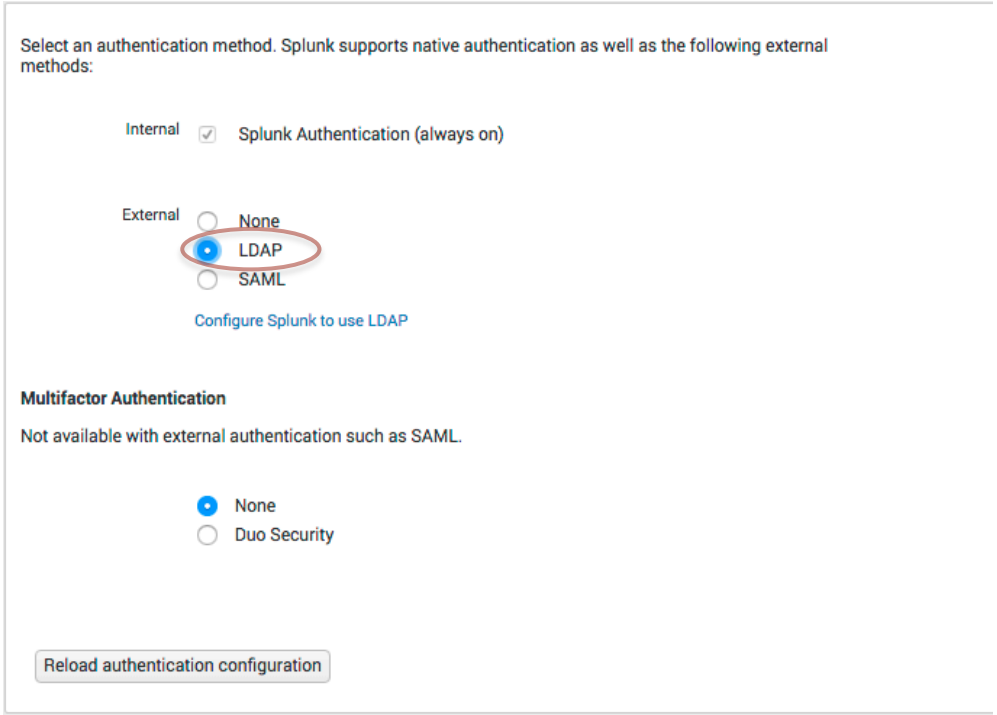


SSO With Proxy +LDAP

SSO With Proxy + LDAP



Configuring LDAP



Configuring Reverse Proxy - Apache

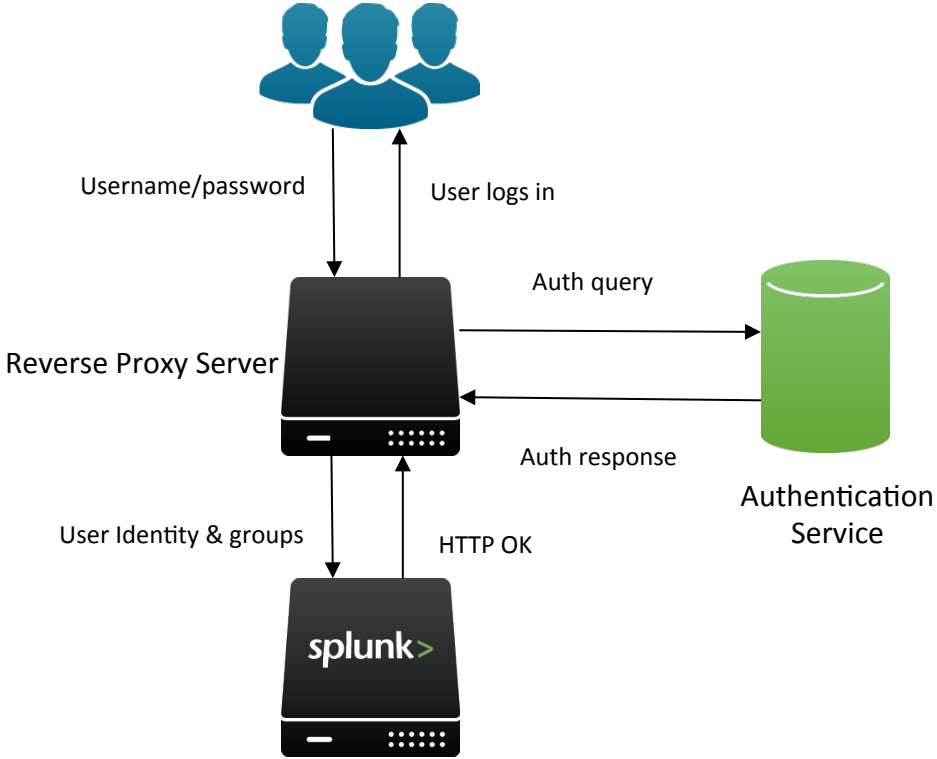
```
$ sudo a2enmod proxy_http


...
ProxyRequests off
ProxyPass / http://mysplunkhost:8000/
ProxyPassReverse / http://mysplunkhost:8000/
...
```

Proxy SSO

Proxy SSO

- Proxy SSO - a new authentication type, available from Splunk 6.5
- With Proxy SSO, Splunk need not communicate with the external authentication provider
- Combines authentication and authorization into single step
  - Reduce configuration steps
  - Streamline login process
- For Proxy SSO to work, reverse proxy server will add remote group HTTP header on top of remote user HTTP header sent for legacy SSO

Proxy SSO Workflow



How Do Saved Searches Run?

- In legacy SSO, Splunk queries the LDAP server to validate if user is authorized to run the search
- Proxy SSO removes the need to configure LDAP on Splunk
- Hence, saved searches will depend on the user to role map cache to validate the user

```
[authentication]
authType = ProxySSO
defaultRoleIfMissing = user

[roleMap_proxySSO]
admin = group1
user = group2
power = group3

[userToRoleMap_ProxySSO]
user2 = admin;power;user
```

Troubleshooting SSO

/debug/sso

SSO settings

SSO Enabled	Yes
splunkd trustedIP	
splunkweb trustedIP	10.75.7.67
splunkweb SSO Mode	strict

Splunkweb settings

Host Name	ronnie.sv.splunk.com
Host IP	10.1.42.3
Port	8013
Incoming request IP received by splunkweb	10.75.7.67
Is the incoming request IP in splunkweb's list of trustedIPs?	Yes. SSO will be used to authenticate this request.

Troubleshooting SSO

Remote user HTTP header

Remote User HTTP Header	REMOTE_USER
Value of REMOTE_USER	user2

Remote groups HTTP header

Remote Groups HTTP Header	REMOTE_GROUPS
Value of REMOTE_GROUPS	group1, group2, group3
Cookies Set	session_id_8013, splunkd_8013, splunkweb_csrf_token_8013

Other HTTP headers

Host	localhost:80
Cache-Control	max-age=0
Upgrade-Insecure-Requests	1
User-Agent	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.106 Safari/537.36
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding	gzip, deflate, sdch, br
Accept-Language	en-US,en;q=0.8
REMOTE-USER	user2
REMOTE-GROUPS	group1,group2,group3
X-Forwarded-For	::1
X-Forwarded-Host	localhost:80
X-Forwarded-Server	adhoke-mbpr15.sv.splunk.com
Connection	Keep-Alive

SAML 2.0

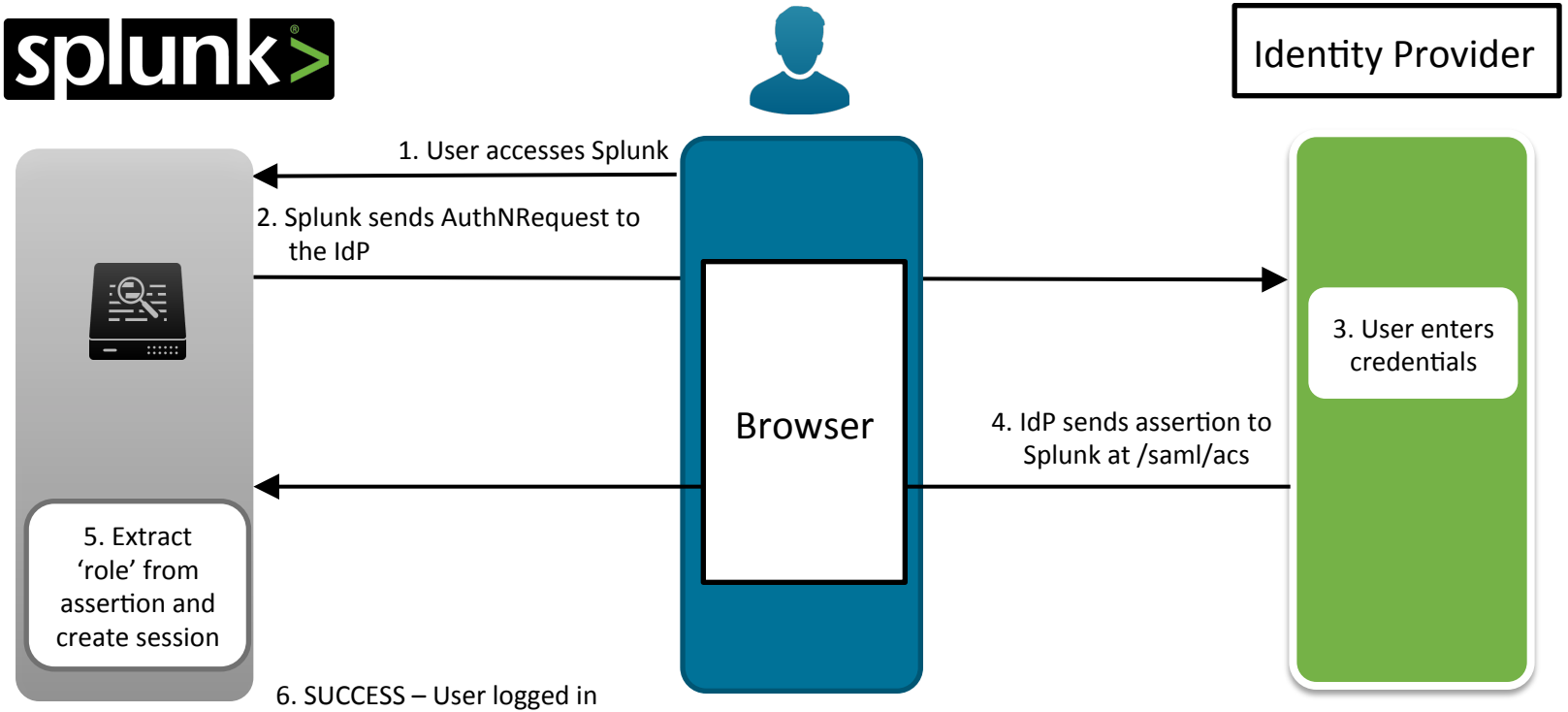
SAML 2.0

- Security Assertion Markup Language
- XML based standard for browser based SSO
- Multiple protocols and bindings
- IdP - Identity Provider - Trusted Authority, SP - Service Provider

Why SAML?

- Security
  - Credentials are not stored locally
  - Standard for Single Sign On
  - Multi-Factor authentication
  - Centrally managed Authentication & Authorization
  - Signed Saml payload
  - Especially useful on the Cloud

The Login Process



What Is New For 6.5?

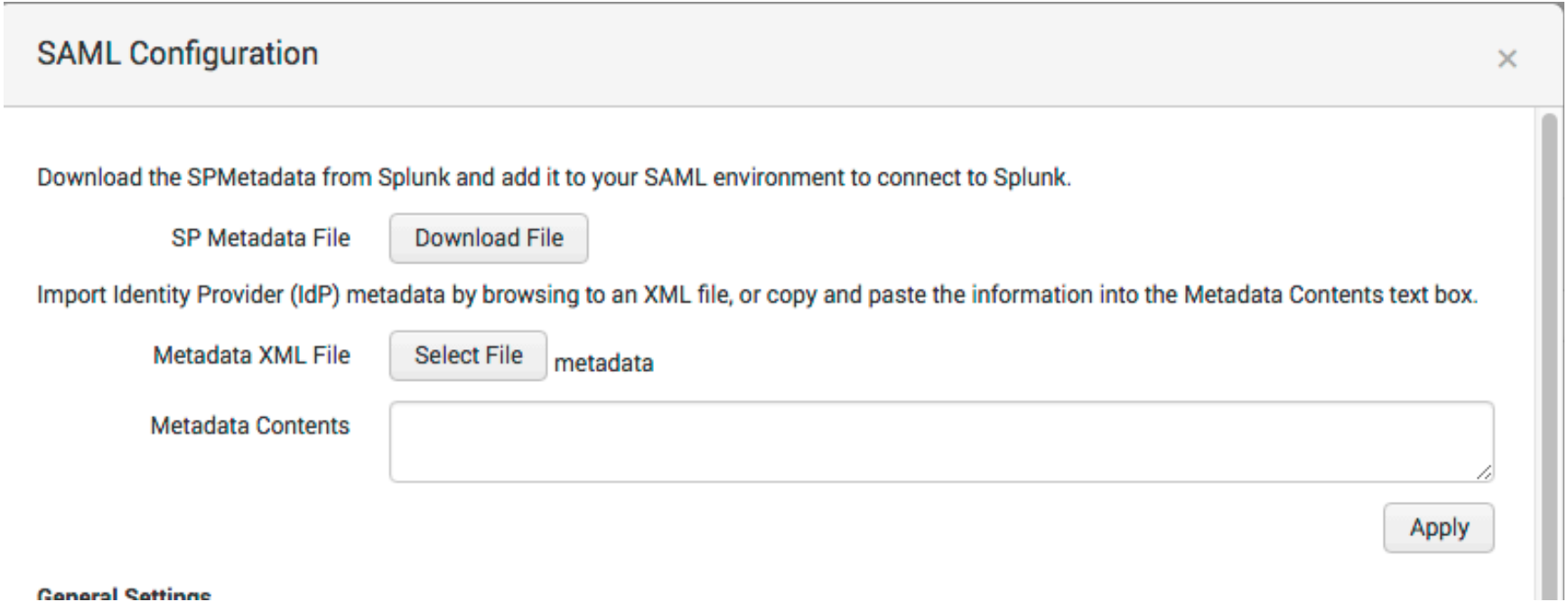
More supported IdPs

- Azure
- Okta
- Adfs
- OneLogin
- PingIdentity
- …

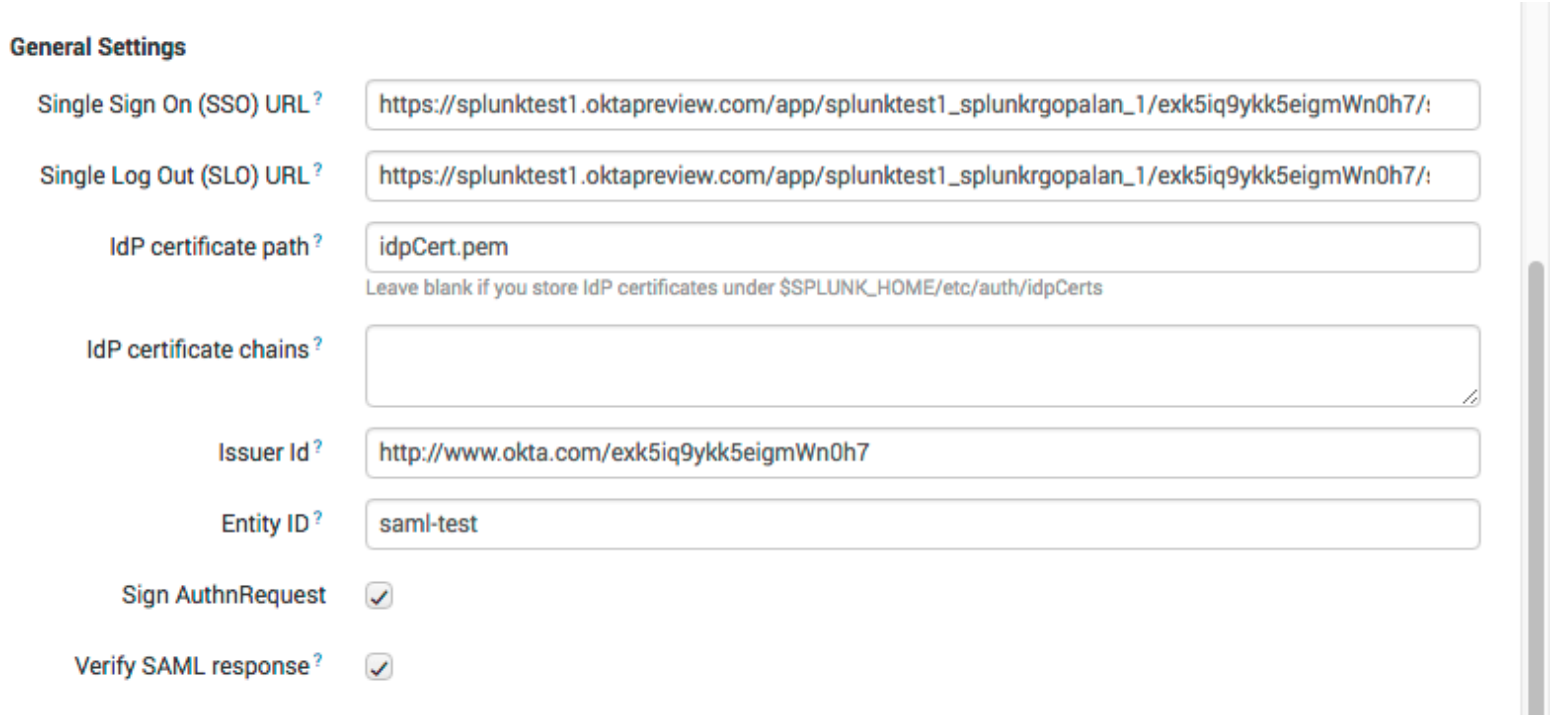
What Is New For 6.5 Cont'd…

- Attribute queries are optional
- Official Splunk app for Azure
- Support for additional bindings
- Support for aliases
- Improved UI

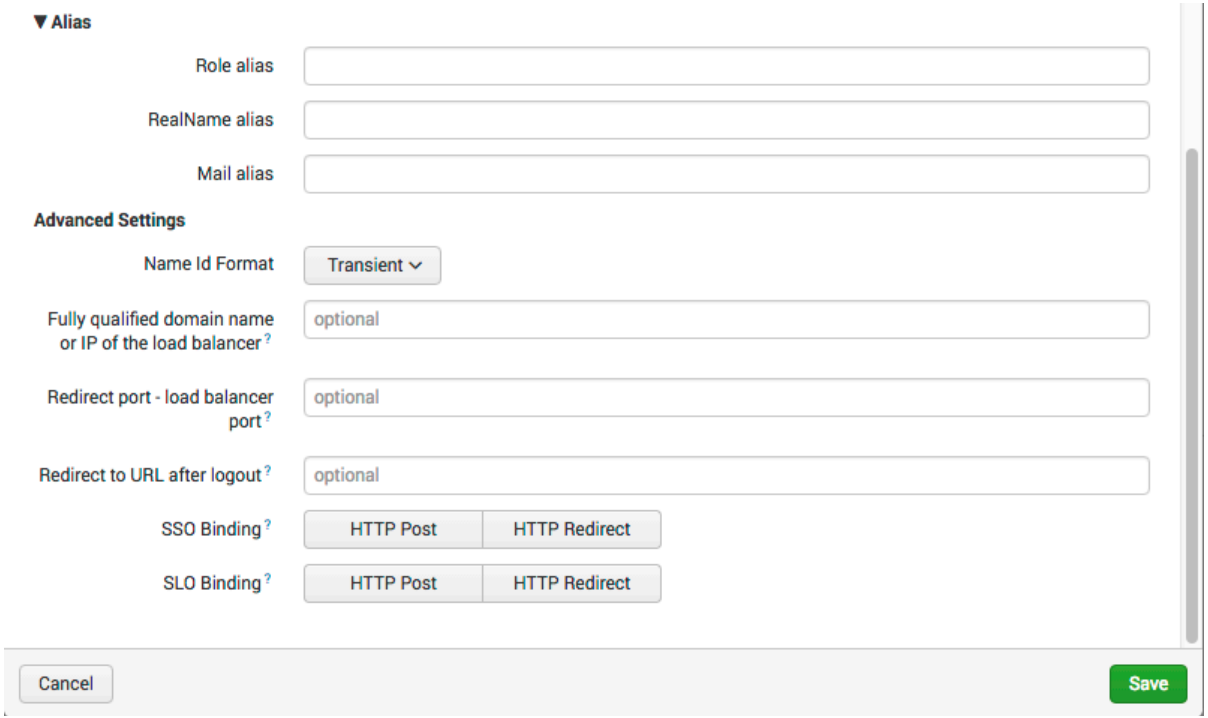
SAML 2.0 Configuration



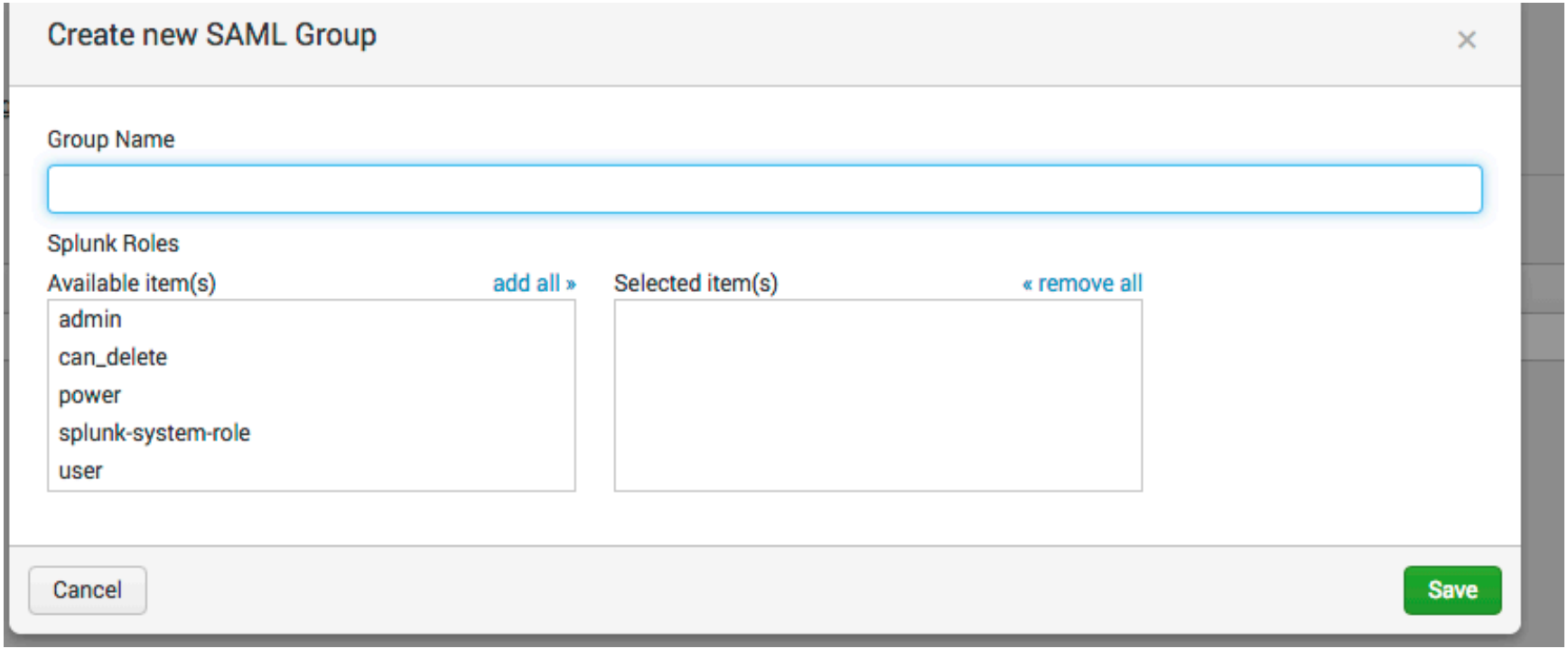
SAML 2.0 Configuration Cont'd…



SAML 2.0 Configuration Cont'd…



Add Role Mapping



How Do Saved Searches Work?

Attribute Query

- Configure Attribute Query
- PingIdentity, Novell Directory
- Splunk acts a http client and send a Attribute Query request to the IdP
- Runs at a configurable interval
- Always gets the latest and greatest AD groups for the user

How Do Saved Searches Work Cont'd?

Without Attribute Query

- Many IdPs do not support Attribute Query
- Okta, Adfs, Azure, Onelogin
- saved searches run using cached role information
- user-to-role information can be updated using an endpoint - services/admin/SAML-user-role-map/<user>

```
[authenticationResponseAttrMap_SAML]
mail = mail
realName = realName
role = http://schemas.microsoft.com/ws/2008/06/identity/claims/role

[authentication]
authSettings = saml
authType = SAML

[rolemap_SAML]
admin = domain admins
user = domain users
power = it admins

[userToRoleMap_SAML]
srv-adfs@qa.ad2008r2.com = admin
user1-adfs@qa.ad2008r2.com = user
pwruser-adfs@qa.ad2008r2.com = power
~
~
~
~
~
```

Tips For Troubleshooting

- SAML Tracer
- Verify that signed/unsigned requests for saml requests and response match Splunk and the IdP
- Enable DEBUG logging on Splunk
- IdP-specific DEBUG information – like Event viewer for Adfs
- Ensure nameId and ‘role’ attributes are present in the saml response
- Migrating users to SAML

Multi Factor Authentication

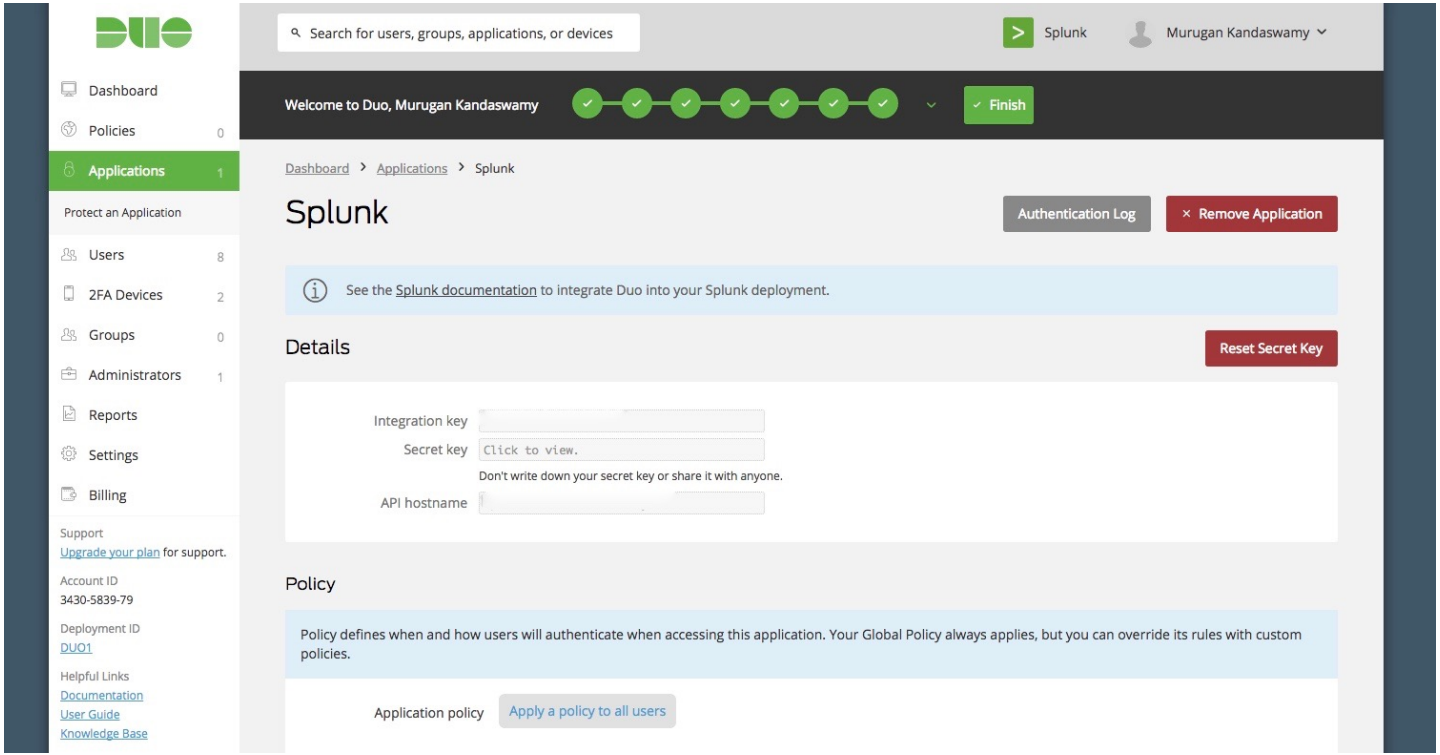
Why MFA?

- Multi Factor Authentication provides best protection against phishing attacks, credential exploitation and other attacks to compromise your system by combining what you know (user/password) with what you have (mobile/hardware token)

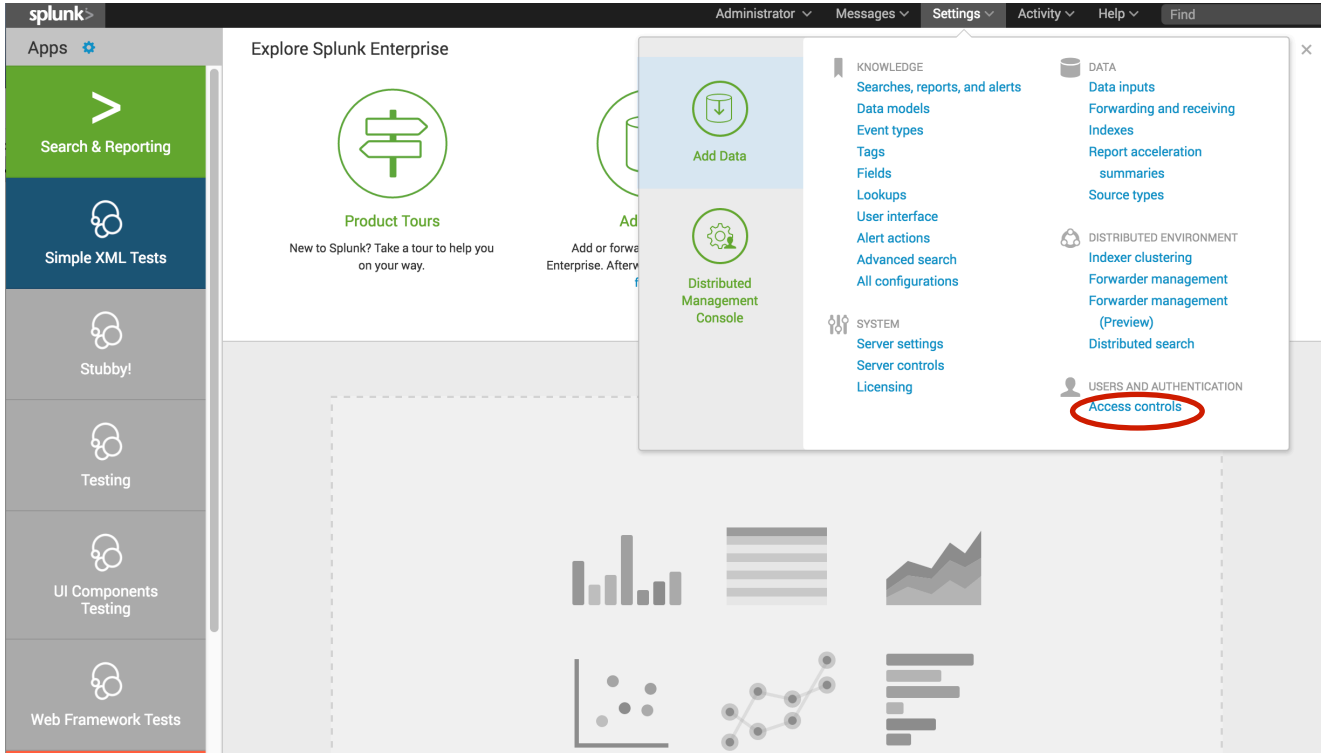
Splunk Support For MFA

- Splunk natively supports Multifactor Authentication only for local authentication methods like Splunk Auth, LDAP or Scripted Auth
- As of now, Duo Security is the only supported MFA vendor
- Customers using SSO solutions like SAML are expected to make use of MFA authentication service supported on the Identity Provider(IdP) platform

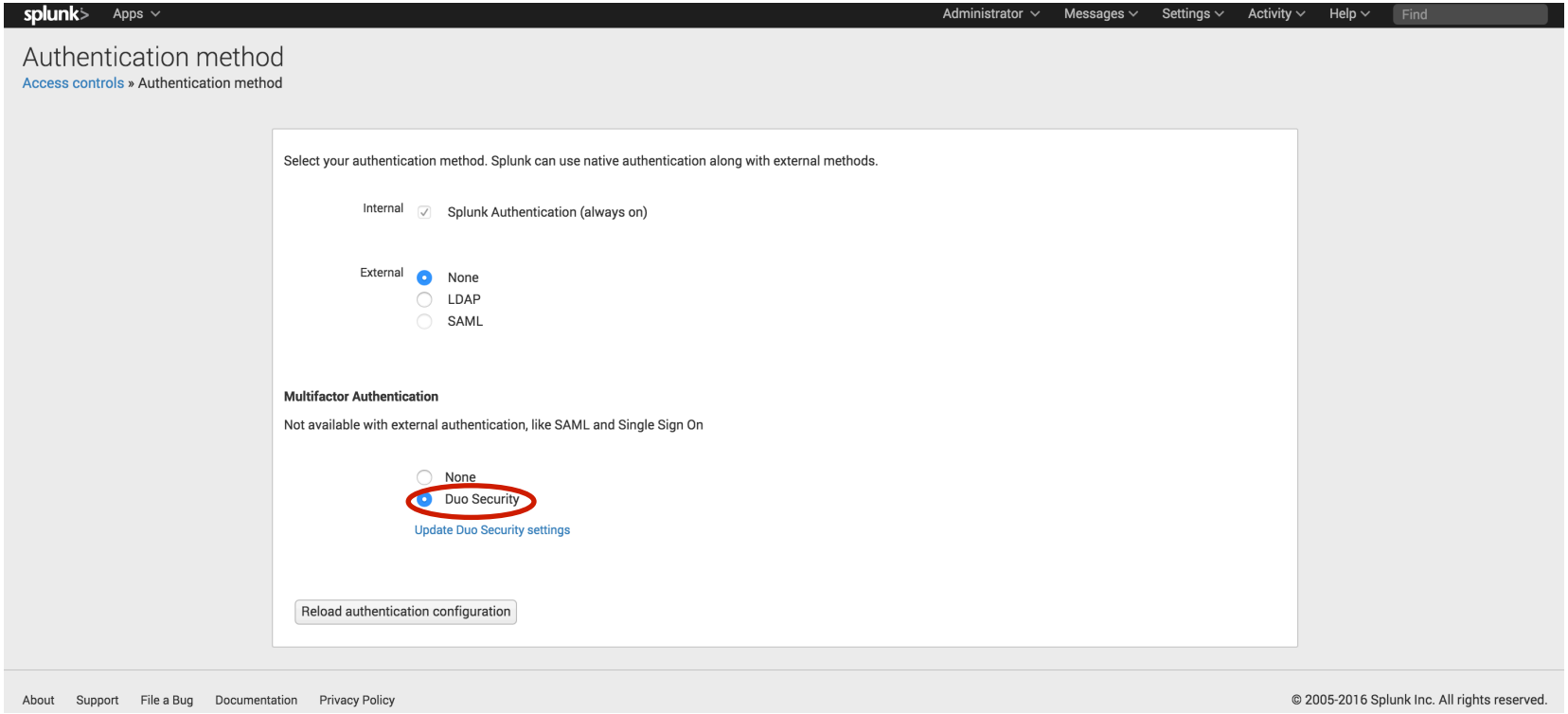
Configure Duo To Protect Splunk



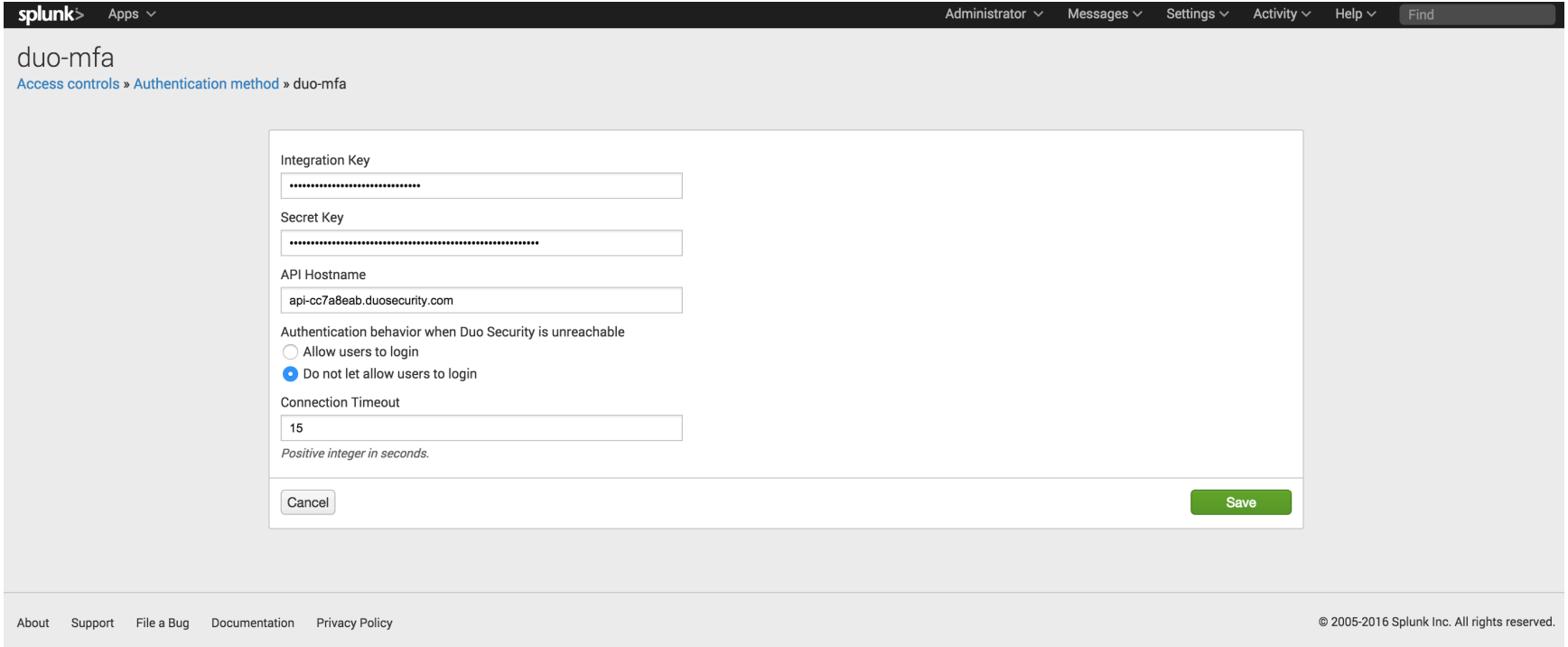
Configuring MFA in Splunk



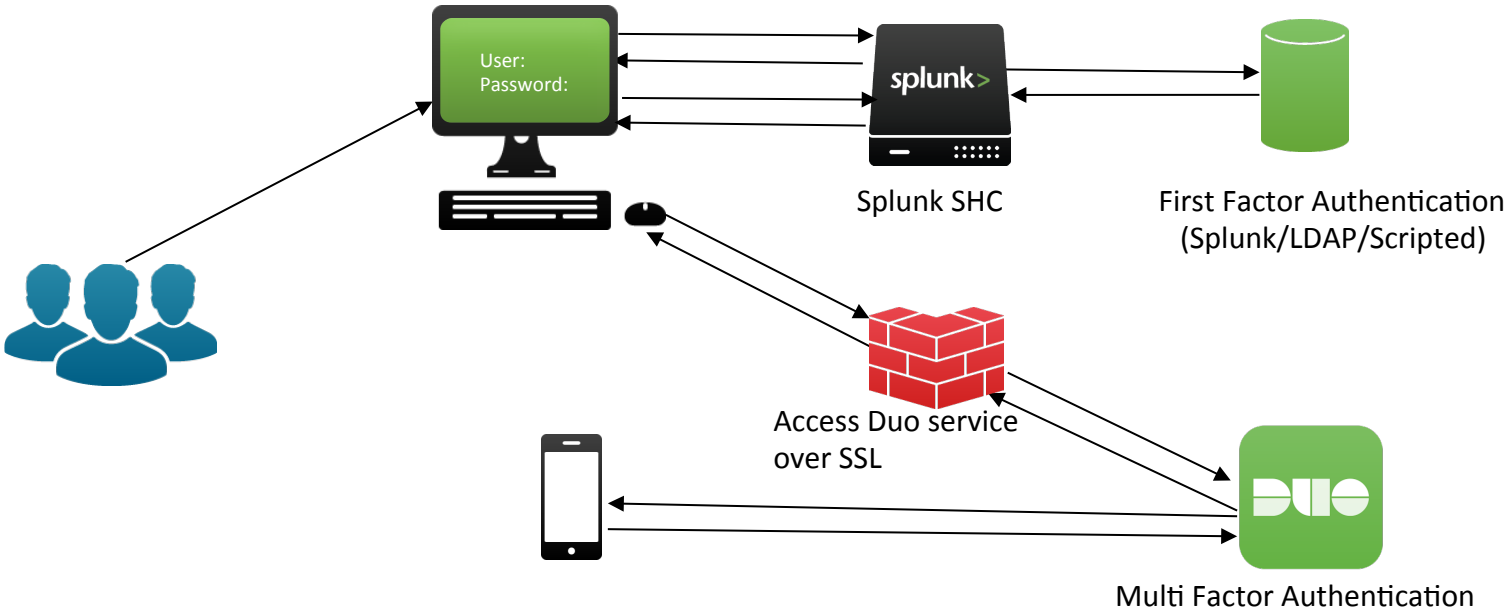
Configuring MFA In Splunk



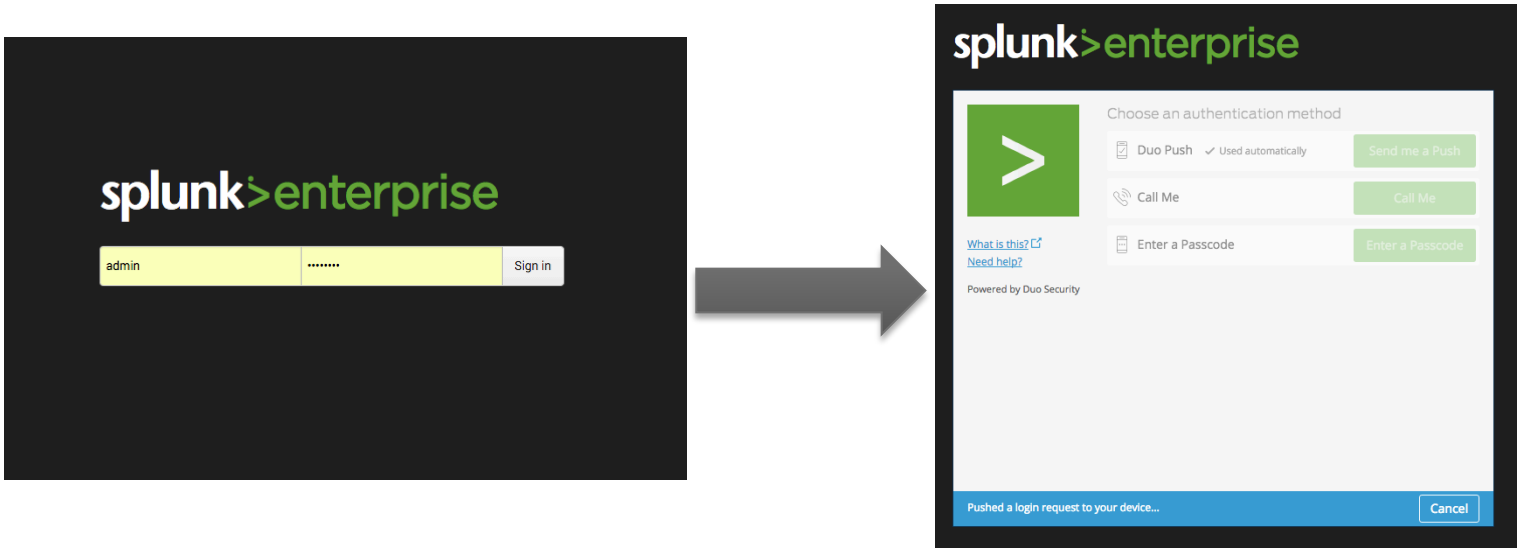
Configuring Duo MFA Service



Splunk Duo MFA Login Process

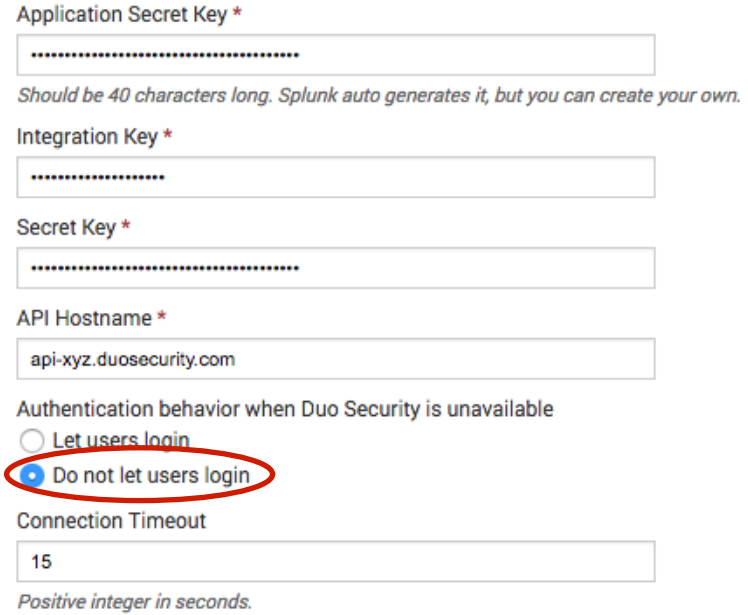


New Splunk Login Page With MFA



MFA Best Practices

- Synchronize Splunk server system time to a NTP server to avoid login failures
- When resetting secret key on Duo, have a Splunk session open to update the new secret key simultaneously to avoid lockout



Q & A

THANK YOU

splunk>