

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

.conf2016

splunk >

Murugan Kandaswamy
Software Engineer, Splunk
mkandaswamy@splunk.com

.conf2016

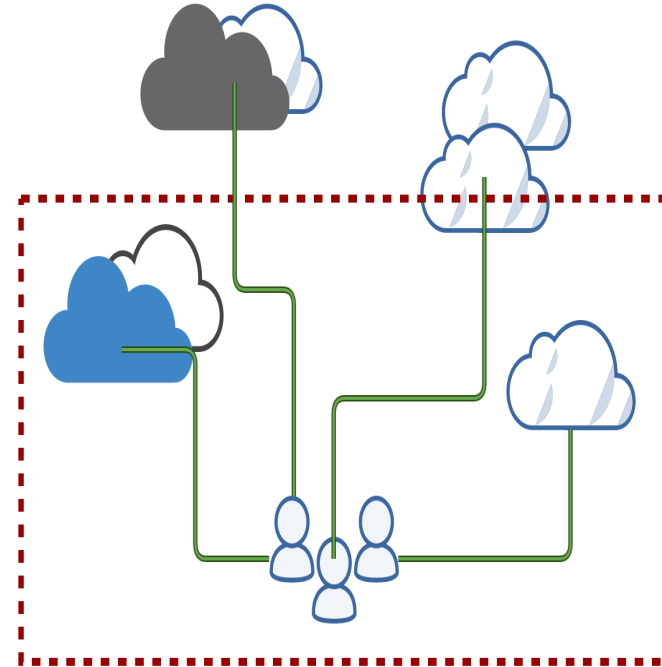
splunk >

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

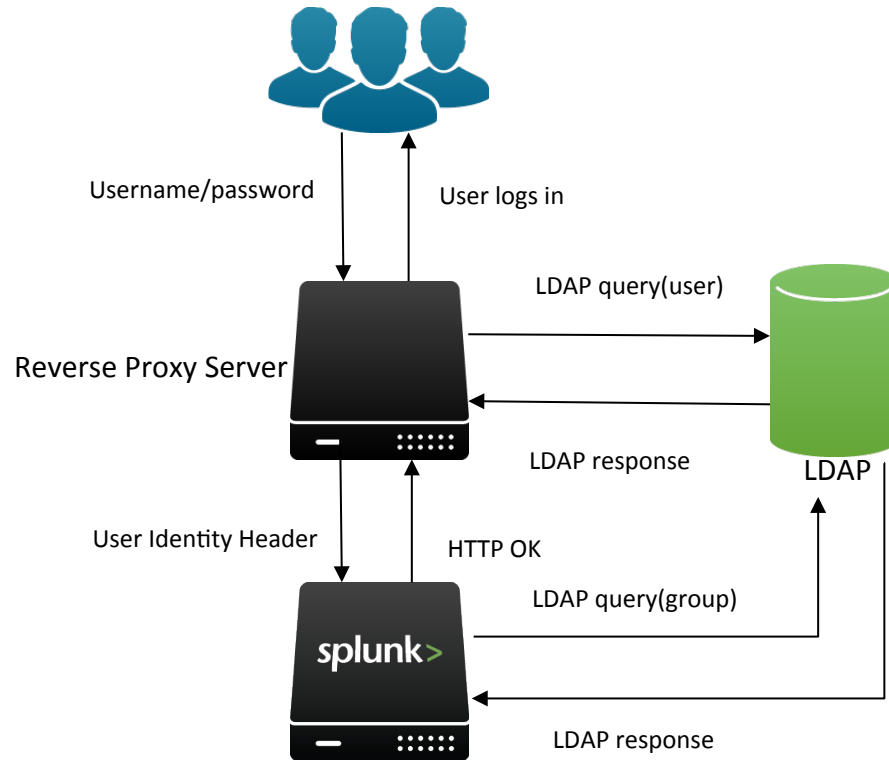


SSO With Proxy +LDAP

.conf2016

splunk >

SSO With Proxy + LDAP



Configuring LDAP

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

Internal Splunk Authentication (always on)

External None

LDAP

SAML

[Configure Splunk to use LDAP](#)

Multifactor Authentication

Not available with external authentication such as SAML.

None

Duo Security

Reload authentication configuration

Configuring Reverse Proxy - Apache

```
$ sudo a2enmod proxy_http  
  
...  
ProxyRequests off  
ProxyPass / http://mysplunkhost:8000/  
ProxyPassReverse / http://mysplunkhost:8000/  
  
...
```

Proxy SSO

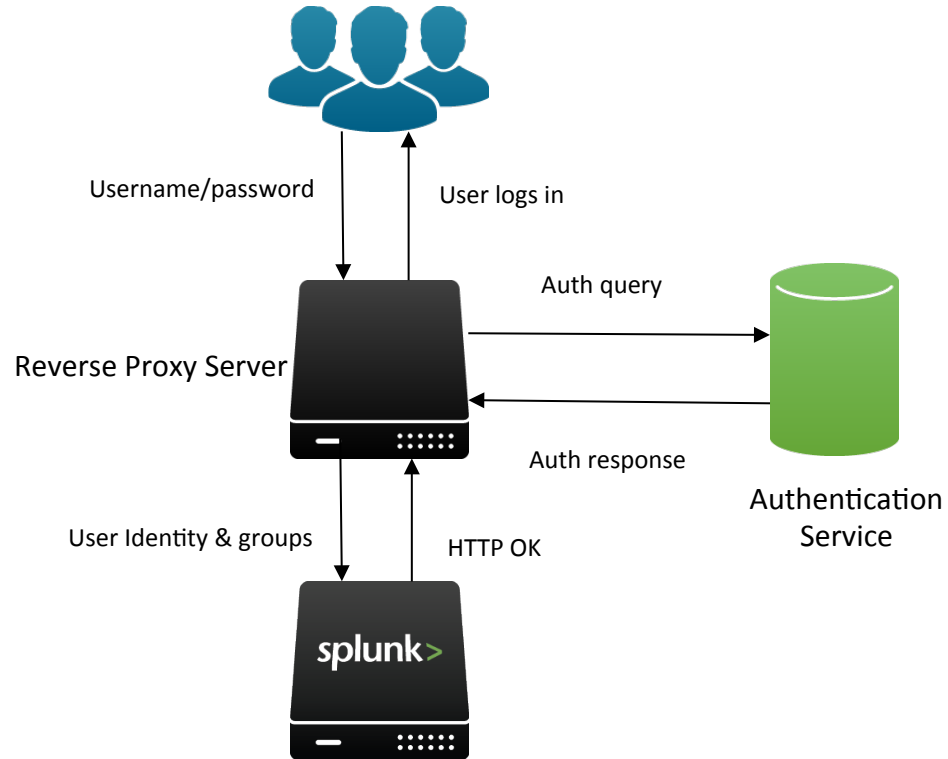


.conf2016

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

```
1 [authentication]
2 authType = ProxySSO
3 defaultRoleIfMissing = user
4
5 [roleMap_proxySSO]
6 admin = group1
7 user = group2
8 power = group3
9
10 [userToRoleMap_ProxySSO]
11 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



.conf2016

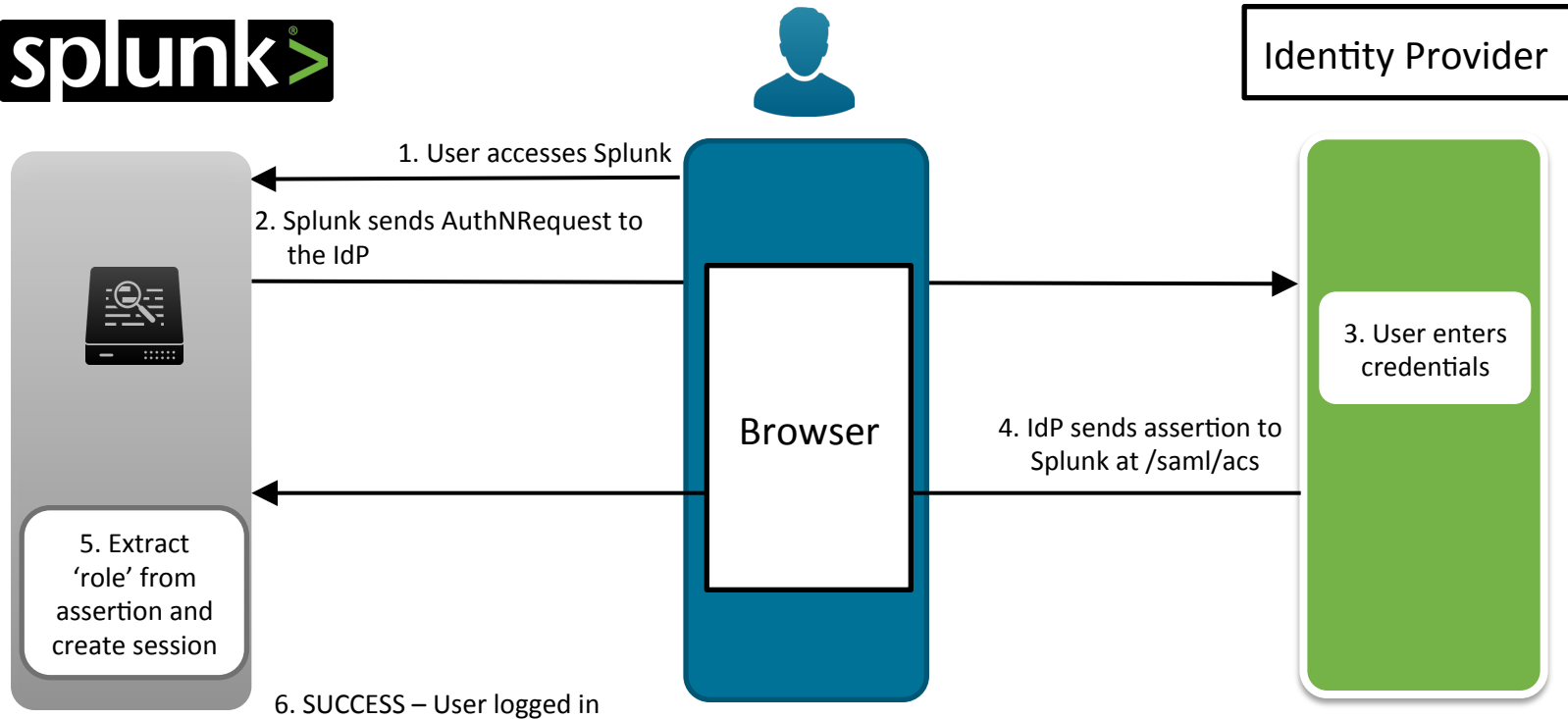
SAML 2.0

- 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 Configuration ×

Download the SPMetadata 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

Metadata Contents

General Settings

SAML 2.0 Configuration Cont'd...

General Settings

Single Sign On (SSO) URL ?

Single Log Out (SLO) URL ?

IdP certificate path ?

Leave blank if you store IdP certificates under \$SPLUNK_HOME/etc/auth/idpCerts

IdP certificate chains ?

Issuer Id ?

Entity ID ?

Sign AuthnRequest

Verify SAML response ?

SAML 2.0 Configuration Cont'd...

▼ Alias

Role alias

RealName alias

Mail 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?

SSO Binding?

SLO Binding?

Add Role Mapping

Create new SAML Group ✕

Group Name

Splunk Roles

Available item(s) add all »	Selected item(s) « remove all
admin can_delete power splunk-system-role user	

Cancel Save

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-adsf@qa.ad2008r2.com = admin
user1-adsf@qa.ad2008r2.com = user
pwruser-adsf@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 nameld and 'role' attributes are present in the saml response
- Migrating users to SAML

Multi Factor Authentication



.conf2016

splunk >

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

The screenshot displays the Duo Admin Console interface. On the left is a navigation sidebar with the Duo logo at the top and menu items: Dashboard, Policies (0), Applications (1), Protect an Application, Users (8), 2FA Devices (2), Groups (0), Administrators (1), Reports, Settings, and Billing. Below the sidebar are support links: Upgrade your plan, Account ID (3430-5839-79), Deployment ID (DUO1), and Helpful Links (Documentation, User Guide, Knowledge Base). The main content area has a search bar at the top, a user profile for Murugan Kandaswamy, and a progress indicator with seven green checkmarks and a Finish button. The breadcrumb trail is Dashboard > Applications > Splunk. The page title is 'Splunk' with buttons for Authentication Log and Remove Application. A light blue information box contains a link to Splunk documentation. The 'Details' section includes a Reset Secret Key button and input fields for Integration key, Secret key (with a Click to view button), API hostname, and a warning not to share the secret key. The 'Policy' section has a light blue box explaining that a policy defines authentication rules, with an 'Apply a policy to all users' button.

Configuring MFA in Splunk

The image shows the Splunk web interface. At the top, the navigation bar includes 'splunk >', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. On the left, the 'Apps' sidebar lists: Search & Reporting, Simple XML Tests, Stubby!, Testing, UI Components Testing, and Web Framework Tests. The main content area is titled 'Explore Splunk Enterprise' and features a 'Product Tours' card. A 'Settings' dropdown menu is open, displaying a tree structure of configuration categories. The 'Access controls' option under 'USERS AND AUTHENTICATION' is circled in red. The menu items are as follows:

- KNOWLEDGE
 - Searches, reports, and alerts
 - Data models
 - Event types
 - Tags
 - Fields
 - Lookups
 - User interface
 - Alert actions
 - Advanced search
 - All configurations
- DATA
 - Data inputs
 - Forwarding and receiving
 - Indexes
 - Report acceleration summaries
 - Source types
- DISTRIBUTED ENVIRONMENT
 - Indexer clustering
 - Forwarder management
 - Forwarder management (Preview)
 - Distributed search
- SYSTEM
 - Server settings
 - Server controls
 - Licensing
- USERS AND AUTHENTICATION
 - Access controls

Configuring MFA In Splunk

splunk> Apps ▾ Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Authentication method

[Access controls](#) » Authentication method

Select your authentication method. Splunk can use native authentication along with external methods.

Internal Splunk Authentication (always on)

External None
 LDAP
 SAML

Multifactor Authentication
Not available with external authentication, like SAML and Single Sign On

None
 Duo Security
[Update Duo Security settings](#)

[Reload authentication configuration](#)

About Support File a Bug Documentation Privacy Policy

© 2005-2016 Splunk Inc. All rights reserved.

Configuring Duo MFA Service

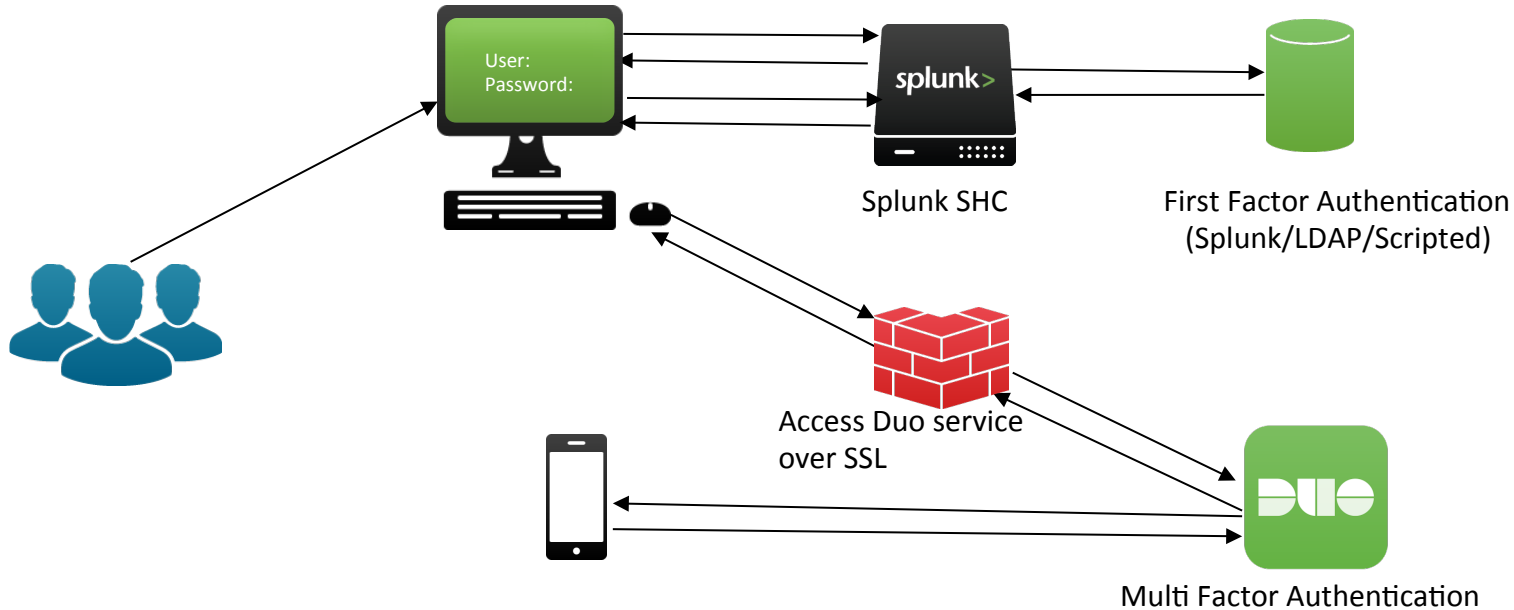
The screenshot shows the Splunk Admin UI for configuring Duo MFA. The breadcrumb trail is: [Access controls](#) » [Authentication method](#) » duo-mfa. The configuration form includes the following fields and options:

- Integration Key:** A text input field containing a series of asterisks.
- Secret Key:** A text input field containing a series of asterisks.
- API Hostname:** A text input field containing the value `api-cc7a8eab.duosecurity.com`.
- Authentication behavior when Duo Security is unreachable:** Two radio button options:
 - Allow users to login
 - Do not let allow users to login
- Connection Timeout:** A text input field containing the value `15`.

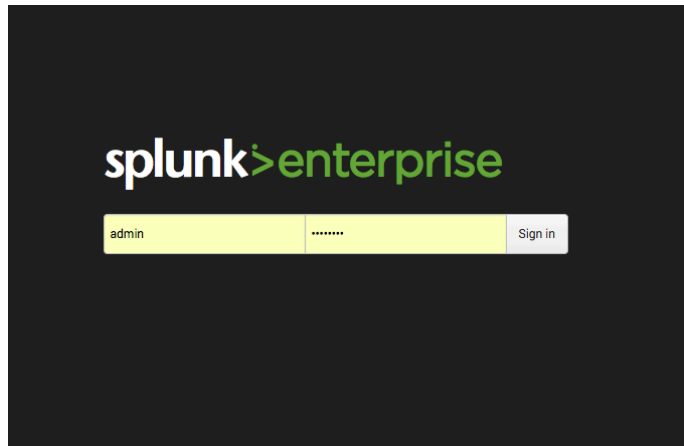
Below the form, there is a note: *Positive integer in seconds.* At the bottom of the form are two buttons: **Cancel** and **Save**.

At the bottom of the page, there is a footer with links: [About](#), [Support](#), [File a Bug](#), [Documentation](#), and [Privacy Policy](#). On the right side of the footer, it says: © 2005-2016 Splunk Inc. All rights reserved.

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

Application Secret Key *

Should be 40 characters long. Splunk auto generates it, but you can create your own.

Integration Key *

Secret Key *

API Hostname *

Authentication behavior when Duo Security is unavailable

Let users login

Do not let users login

Connection Timeout

Positive integer in seconds.

Q & A

.conf2016

splunk >

THANK YOU

.conf2016