Securing the Splunk Cloud Platform

Splunk Cloud Platform has been designed to give organizations an enterprise, robust and scalable and secure Splunk Cloud Platform environment. The platform is built according to best practices and standards, and has more than 325 security controls built in.

Authentication

Every user of Splunk Cloud Platform must be authenticated and authorized, identifying themselves to gain access to their environment.

Splunk Cloud Platform offers several authentication methods for your organization:

<table>
<thead>
<tr>
<th>Authentication method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP</td>
<td>Supports authentication with your organizations existing LDAP server or Splunk’s own authentication</td>
</tr>
<tr>
<td>SAML</td>
<td>Supports integration with compliant identity providers</td>
</tr>
</tbody>
</table>

You can choose the authentication method you prefer in Splunk Cloud by navigating to Settings, then under Users and Authentication click Authentication Methods:

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
LDAP authentication

This diagram shows the LDAP authentication flow:

For users in cloud to authenticate using LDAP:

- Your organization should maintain read-only LDAP servers which are reachable over the internet
- You should use Distinguished Name (User) with attributes (Groups) that map to Splunk roles

SAML authentication

This diagram shows the SAML authentication flow:
For users in cloud to authenticate using SAML, users must maintain an Identity Provider that is reachable over the internet which has the following characteristics:

- Credentials exchanged in a browser session
- Currently limited to a single IDP

Authentication and authorization using SAML uses digitally signed XML certificates from an IDP. Some of the IDPs that are typically supported on Splunk Cloud Platform are:

- Okta
- OneLogin
- Ping Identity
- Azure AD or AD FS
- Optimal
- SecureAuth
- IdentityNow
- Oracle Open SSO
- Google SAML2 Provider

If you are using a mixture of native Splunk, LDAP or SAML users, Splunk native authentication takes precedence and local authorization may apply.

---

**Access and user management**

Splunk Cloud Platform supports Role-Based Access Control (RBAC), used for protecting the environment by restricting access based on a user’s role.

Users are able to hold multiple roles within Splunk Cloud Platform, and each role provides the user with specific access to resources or actions within the environment.

---

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Splunk Cloud Platform predefined roles are:

<table>
<thead>
<tr>
<th>Role</th>
<th>Role capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apps</td>
<td>Manage apps. Also has some admin capabilities</td>
</tr>
<tr>
<td>Power</td>
<td>Edit all shared objects and alerts, tag events</td>
</tr>
<tr>
<td>User</td>
<td>Create, edit and run searches and save searches. Can also edit its own preferences</td>
</tr>
<tr>
<td>Can_delete</td>
<td>Can delete by keyword</td>
</tr>
<tr>
<td>Sc_admin (Cloud-specific)</td>
<td>Create users and roles</td>
</tr>
<tr>
<td>Tokens_auth</td>
<td>Configure token-based authorization</td>
</tr>
</tbody>
</table>

If there are requirements for more granular access that the roles above, then Custom Roles would be a better solution.

**Encryption and key management**

Splunk Cloud Platform offers two options for encryption:

- Encryption in transit uses industry standard SSL/TLS 1.2+ encryption. This is used by forwarders and user sessions.
- Encryption at rest uses AES 256-bit advanced encryption. This service is available as a premium service enhancement.

Splunk Cloud Platform uses AWS KMS (Key Management Service), a fully managed service which helps to create and manage encryption. Essentially, Splunk is responsible for the overall management of all the keys, including their creation, rotation and revocation.

Splunk Cloud Platform also offers Enterprise Managed Encryption Keys (EMEK) as an option for encryption at rest. This gives you the option to bring your own primary encryption key.
Data isolation

In Splunk Cloud Platform each cloud stack is essentially physically separated. Your data is separated from our other customer's data, so your data integrity and performance will not be affected by any other customer who is using the platform.

Every customer's Splunk Cloud Platform stack is deployed into and runs in an extensively secured environment. Each service and component is secured, the OS layer is secured, and the hardened network is also secured and has a firewall policy with a default-deny. Each customer has their own instance(s).

Governance

Splunk Cloud Platform supports compliance with the following compliance regulations:

- SOC type 2
- ISO 27001
- PCI
- HIPAA
- FEDRAMP

You can read more about how Splunk products support compliance regulations [here](#).