Splunk® Enterprise Securing Splunk Enterprise 7.3.0

Set up authentication with tokens

Generated: 11/17/2019 2:55 am
Set up authentication with tokens

Authentication tokens, also known as JSON Web Tokens (JWT), are a method for authenticating Splunk platform users into the Splunk platform. Tokens let you provide access to environments without having to provide the standard types of credentials. Instead of providing a username and password, you provide the token. As a Splunk platform user, you can use tokens to make calls to Representational State Transfer (REST) endpoints on Splunk platform instances. Tokens are credentials, so you must closely guard them, and not share them with anyone who does not explicitly need access to Splunk platform services.

Currently, Splunk Enterprise limits token support to web requests to REST endpoints. You cannot use tokens to log in interactively with the Splunk CLI or through Splunk Web.

Authentication tokens are different from other types of token that you can configure in Splunk Enterprise on forwarders and indexers for authenticated communication between those components, or HTTP Event Collector, though their function is similar.

As a Splunk platform administrator, you can control a number of authentication token properties:

- Who owns the token. A token is associated with a username on the instance
- Token audience. A label that indicates the token's purpose
- How long a token lasts
- When its validity begins. It does not have to become valid immediately when you create it
- Whether or not it is enabled, at any time

You can also delete the token if you no longer want the user to have access through the token. If you disable or remove a token, users of that token lose access to the instance unless they have standard credentials such as the username and password.

Supported Splunk deployment types and authentication schemes for tokens

You can create and assign tokens to various user types that can access a Splunk platform instance, based on the type of authentication system that the instance uses. At this time, tokens are supported in the following deployment types and
authentication schemes:

**Supported deployment types**

- Single-instance, on search heads only
- Search head cluster nodes

**Unsupported deployment types**

- Indexers
- Indexer cluster nodes
- Universal forwarders
- Splunk Cloud instances of any kind

**Supported authentication schemes**

- Native authentication
- Lightweight Directory Access Protocol (LDAP) authentication

**Unsupported authentication schemes**

- Single Sign-On (SSO) schemes that use Security Assertion Markup Language (SAML)
- Proxy SSO

**Prerequisites for activating tokens**

Before activating token authentication, confirm that you have performed the following tasks:

- Enable Transport Layer Security (TLS)/SSL on your Splunk platform instance. See About securing Splunk Enterprise with SSL for details.
- Confirm that you have enabled app key value store (KV Store). By default, KV store is enabled on search heads. See About app key value store in the *Admin Manual* for more information.

**Prerequisites for creating and configuring tokens**

Before you create and configure tokens, confirm that you have performed the following tasks:

- Logged in to the Splunk platform as a user that is either an administrator level or holds a role with at least one of the following Splunk platform
capabilities:

- `edit_tokens_settings`, which turns token authentication on or off
- `edit_tokens_all`, which lets you create, view, and manage tokens for any user on the instance
- `edit_tokens_own`, which lets you create, view, and manage tokens for yourself

- Completed all of the prerequisites for activating authentication tokens
- Enabled token authentication

**Information on the "list_*" capabilities**

If you have been assigned a role that includes only the following capabilities, you can view tokens, but cannot create them, or enable and disable token authentication:

- The `list_tokens_all` capability lets you see all tokens on the instance.
- The `list_tokens_own` capability lets you see your own tokens.

The `edit_tokens_*` capabilities include the ability to view tokens, as provided by the `list_tokens_*` capabilities.

**How authentication tokens work**

When you create a token, the Splunk platform picks an ID for the token. The token ID references the token information, which the platform stores securely in a KV store collection.

When you use tokens, you must provide the token with each REST request. If the Splunk platform uses its native authentication scheme, it does not cache authentication details.

When you present a token as part of a REST request (generally through a **curl** command or other REST client), the Splunk platform authentication system does the following:

- It checks to see if token authentication is enabled.
- It processes the token that it receives by validating its signature.
- If checks whether or not the token has expired, or if its validity has not yet started.
- If confirms that the token is available and has not been deleted.
- It checks whether or not the token is enabled.
- It confirms that the user that is associated with the token is authorized to use it.
If all checks pass, it authenticates the user and lets the submitted REST operation complete.

**Enable, create, manage, and use tokens**

See the following topics in this chapter for additional information on how to work with authentication tokens:

- Enable or disable token authorization
- Create authentication tokens
- Manage and delete authentication tokens
- Use authentication tokens