Splunk® Enterprise Securing Splunk Enterprise 7.3.1

Configure Single Sign-On with reverse proxy

Generated: 10/17/2019 7:05 pm
Configure Single Sign-On with reverse proxy

Before you configure reverse proxy-based SSO with Splunk Enterprise, make sure you have the following:

- A Proxy Server (Splunk Enterprise supports IIS or Apache) configured as a reverse proxy to authenticate to external systems.
- An LDAP Server or other external authentication system provisioned with appropriate groups and users for your proxy to authenticate against.
- A working Splunk Enterprise configuration that is either configured to use the same external authentication system as your proxy (usually LDAP) or that has native Splunk Enterprise users that match the user and group IDs contained in your external authentication system.

Configuring SSO with reverse proxy requires the following steps:

1. Edit the properties on your proxy server to authenticate against your external authentication system.

2. Edit the Splunk Enterprise `server.conf` file.

3. Edit the Splunk Enterprise `web.conf` file.

**Note**: For optimal security, any HTTP header-based solutions should be implemented over a TLS/SSL enabled deployment.

**Configure server.conf**

Edit the trustedIP in the `general settings` stanza to add the IP address that will make secure authentication requests to splunkd. This is typically Splunk Web and therefore the localhost. You can only enter one IP address per splunkd instance.

```
trustedIP=127.0.0.1
```

If no IP addresses are provided in the trustedIP list, Splunk SSO is disabled by default.

**Configure web.conf**

To enable SSO, configure the following in the `[settings]` stanza in `web.conf` (SPLUNK_HOME/etc/system/local):

```
SSOMode = strict
trustedIP = 127.0.0.1,10.3.1.61,10.1.8.81
remoteUser = Remote-User
tools.proxy.on = False

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Default</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSOMode</td>
<td>no</td>
<td>The SSOMode attribute determines whether the Splunk Web SSO operates in strict or permissive mode. Strict mode restricts authentication to identities that match the IP addresses listed in trustedIP property. If the IP attempting to connect does not match any IP address, an error page appears to the user. Strict mode is recommended for SSO. Permissive mode also restricts authentication to requests from IPs found in the trustedIP list. In permissive mode, if the IP attempting to connect does not match any IP address, a login page is displayed to allow the user to re-authenticate.</td>
</tr>
<tr>
<td>trustedIP</td>
<td>n/a</td>
<td>Set this to the IP address of the authenticating proxy or proxies. Specify a single address or a comma-separated list of addresses; IP ranges and netmask notation are not supported.</td>
</tr>
<tr>
<td>remoteUser</td>
<td>REMOTE_USER</td>
<td>The remoteUser attribute determines the authenticated identity’s attribute that is passed by the proxy server via the HTTP request header. This value defaults to REMOTE_USER but any LDAP attribute can be passed in this request header as long as the proxy sets this attribute properly after authentication. When you configure your remoteUser attribute, you must also configure the RequestHeader property in your proxy configuration to pass the identity’s attribute to Splunk software. This process is described in &quot;About Splunk Single Sign-On&quot;. The default Splunk header used is REMOTE_USER, but if your proxy uses a different</td>
</tr>
<tr>
<td>Attribute</td>
<td>Default</td>
<td>Value</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>tools.proxy.on</td>
<td>false</td>
<td>For apache 1.x proxy this value should be set to True. For later versions this value should be set to False.</td>
</tr>
</tbody>
</table>

If you host Splunk Web behind a proxy that does not place Splunk Web at the proxy’s root, you may also need to configure the `root_endpoint` setting in `$SPLUNK_HOME/etc/system/local/web.conf`.

For example if your proxy hosts Splunk Web at "yourhost.com:9000/splunk", `root_endpoint` should be set to `/splunk`.

For example:

```
root_endpoint=/lzone
```

In the above example, Splunk Web is accessed via


You would next make it visible to the proxy by mapping it in `httpd.conf`:

```
ProxyPass /lzone http://splunkweb.splunk.com:8000/lzone
ProxyPassReverse /lzone http://splunkweb.splunk.com:8000/lzone
```

**Session management**

Since there is no simple log out for a session and Splunk Enterprise will preserve a session as long as the correct header information is contained in the proxy header, you should set your proxy’s session timeout value with this in mind.

If you need to end a session before the timeout has occurred, you can use the REST end point along with the session identifier to destroy the session:

```
curl -s -u admin:changeme -k -X DELETE
https://localhost:8089/services/authentication/httpauth-tokens/990cb3e61414376554a39e390471fff0
```