Skylight security app for Splunk

Installation manual

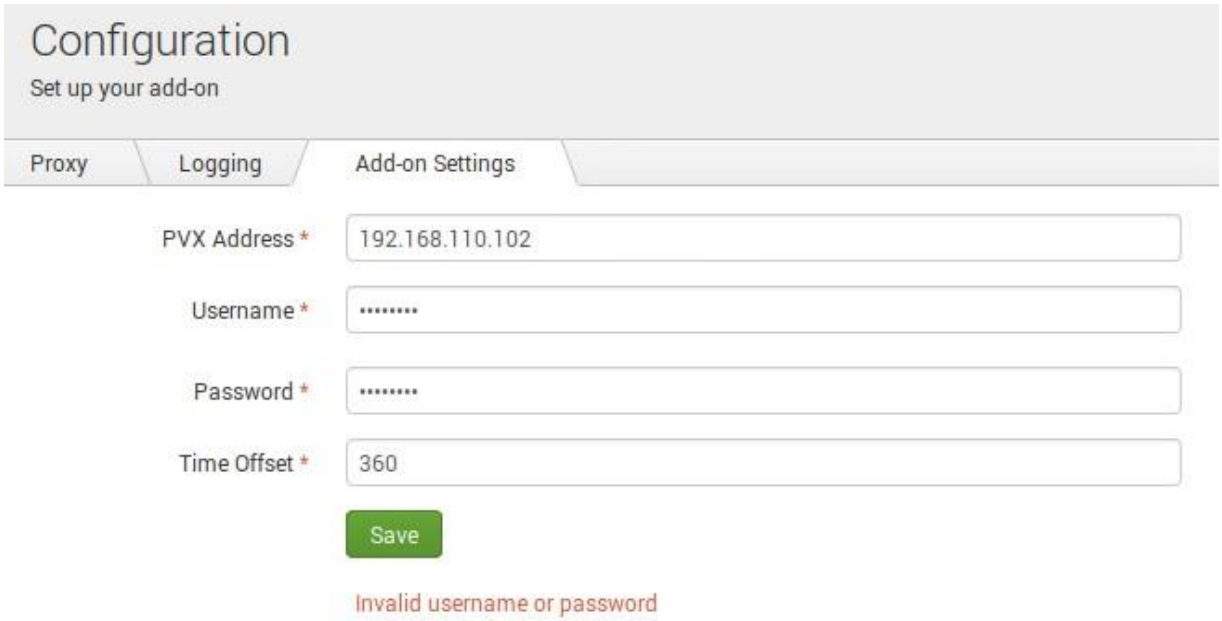
V1.3

Accedian | 2351 Blvd. Alfred Nobel | N-410 Saint-Laurent, QC H4S 2A9 | Tel: +1.514.331.6181 | NA Toll Free: +1.866.685.8181 accedian.com

Installation Procedures

1. Install the required apps
   - Download these applications: URL Toolbox, Parallel Coordinates, Sankey Diagram, Splunk CIM, Force Directed App For Splunk, Lookup File Editor, Punchcard from SplunkBase. To do this you should open the SplunkBase website and in the search field type, the app names one by one and download each of them.
   - Open your Splunk instance. Click on “App > Manage Apps - Install app from file - Select file” and select the app zip archive and click “Upload”. Repeat this action with the other ZIP archives. When you’ve installed all of the apps, restart Splunk.
2. Install the Skylight security for Splunk app and Skylight TA for Splunk
   - Go back to the SplunkBase website. Download the Skylight security app for Splunk and Skylight TA for Splunk the same way you did for the required apps.

   - After the ZIP archives are downloaded, go to your Splunk instance and Install app from file for Skylight Security for Splunk and Skylight TA for Splunk, the same way you did for the required apps.
3. Adjust the Settings
   - This solution works together with Skylight software. You need to build a connection to the server with Skylight. To configure this, go to Skylight TA for Splunk on the page “Configuration > Add-on Settings”.
     - § In the field “PVX Address”, enter the IP address to the Skylight server.
     - § In the “Username” text box, enter your username for Skylight.
     - § In the “Password” text box, enter your password for Skylight
     - § In the “Time Offset” text box, enter the time interval for connecting to the server.



- After you click 'Save', you should see an indicator representing the status of the Skylight connection below this menu. It should state 'Connection to PVX successful'.
- After ~15 minutes, you can check if the Skylight App is receiving data from Skylight.
- To do this, click on "App > Search & Reporting" and run the search *"index=pvx"*.
- If you see events listed, it means that the Skylight App is receiving data from Skylight.
- The Skylight Security for Splunk application is ready to use.