Integration Guide

Cyberark <-> Nexpose Integration

Vulnerability -> Credentials workflow

Partner Name:	CyberArk
Website:	http://www.cyberark.com
Product Name:	Application Identity Manager
Version:	8.5.0
Action Type:	Automated via API and CyberArk SDK Java

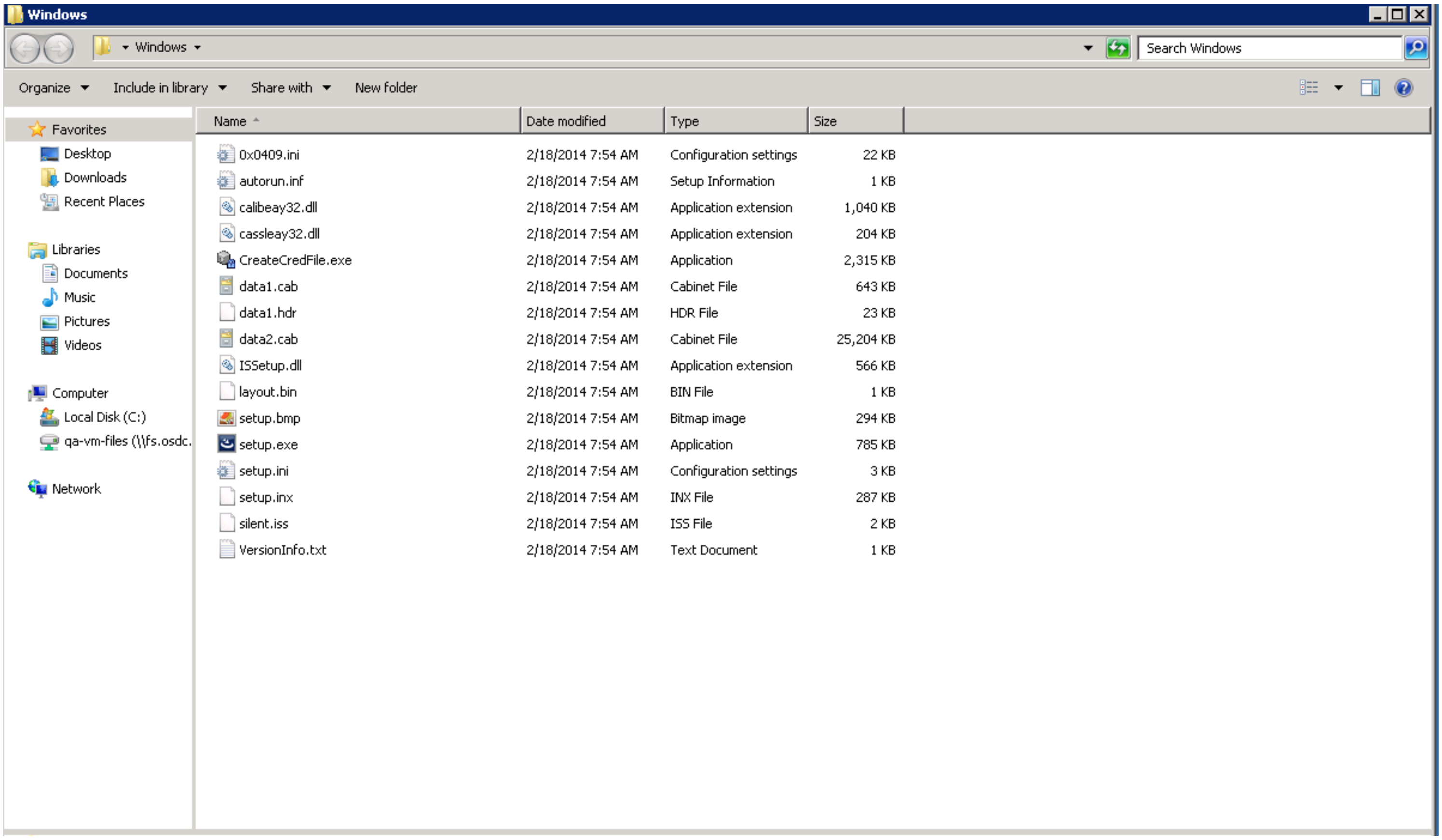
Last Revised: June 25th, 2014

Solution Summary

Application Identity Manager is designed to randomize and store the passwords for accounts on target systems on a regular recurring basis. Because these passwords are stored and managed by the vault, they can be retrieved via an integrated Java SDK.

Partner Product Configuration

The CyberArk Password Java SDK component should be installed beforehand and it's available through the CyberArk support channels; in this example it should be installed and configured using the vault information:



Name	Date modified	Type	Size
0x0409.ini	2/18/2014 7:54 AM	Configuration settings	22 KB
autorun.inf	2/18/2014 7:54 AM	Setup Information	1 KB
calibeay32.dll	2/18/2014 7:54 AM	Application extension	1,040 KB
cassleay32.dll	2/18/2014 7:54 AM	Application extension	204 KB
CreateCredFile.exe	2/18/2014 7:54 AM	Application	2,315 KB
data1.cab	2/18/2014 7:54 AM	Cabinet File	643 KB
data1.hdr	2/18/2014 7:54 AM	HDR File	23 KB
data2.cab	2/18/2014 7:54 AM	Cabinet File	25,204 KB
ISSetup.dll	2/18/2014 7:54 AM	Application extension	566 KB
layout.bin	2/18/2014 7:54 AM	BIN File	1 KB
setup.bmp	2/18/2014 7:54 AM	Bitmap image	294 KB
setup.exe	2/18/2014 7:54 AM	Application	785 KB
setup.ini	2/18/2014 7:54 AM	Configuration settings	3 KB
setup.inx	2/18/2014 7:54 AM	INX File	287 KB
silent.iss	2/18/2014 7:54 AM	ISS File	2 KB
VersionInfo.txt	2/18/2014 7:54 AM	Text Document	1 KB

Please refer to CyberArk documentation for installation and configuration of the Password SDK

Once installed and configured we must go to our Vault and make sure that the assets to be managed have the following characteristics:

- The Object name should match the name of the asset, for example, if the server is named in Nexpose as “server45.mydomain.com”, the Object property in CyberArk should also be “server45.mydomain.com”. Any discrepancies and the integration will not be able to pull the Object name and therefore the credential. Please refer to CyberArk documentation for how to set this.

- The Policy ID of the Object should have a description of the operating system. For example ‘Unix’ or ‘Windows’.

Introduction

This document will guide you through all the steps necessary to configure the CyberArk Gem to successfully import CyberArk credentials into the Nexpose vulnerability management system.

Before you begin

The script was created using JRuby, as such, a JRuby interpreter must be installed on the system where it's going to run. The following link shows the different options for installing Ruby in several platforms:

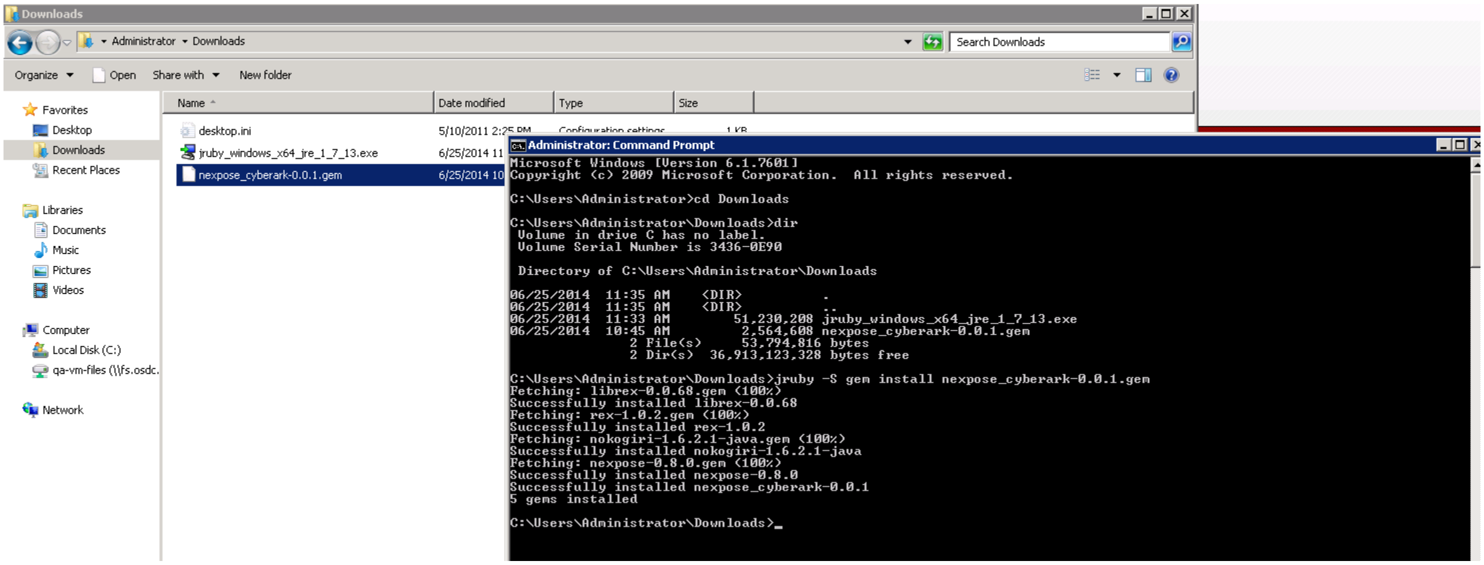
http://jruby.org/

Please install the most appropriate for your need.

Once installed, the following Ruby Gems must also be installed:

- nexpose_cyberark (http://rubygems.org/gems/nexpose_cyberark)

This can be downloaded through the GEM application repositories, or manually if provided by Rapid7 like this:

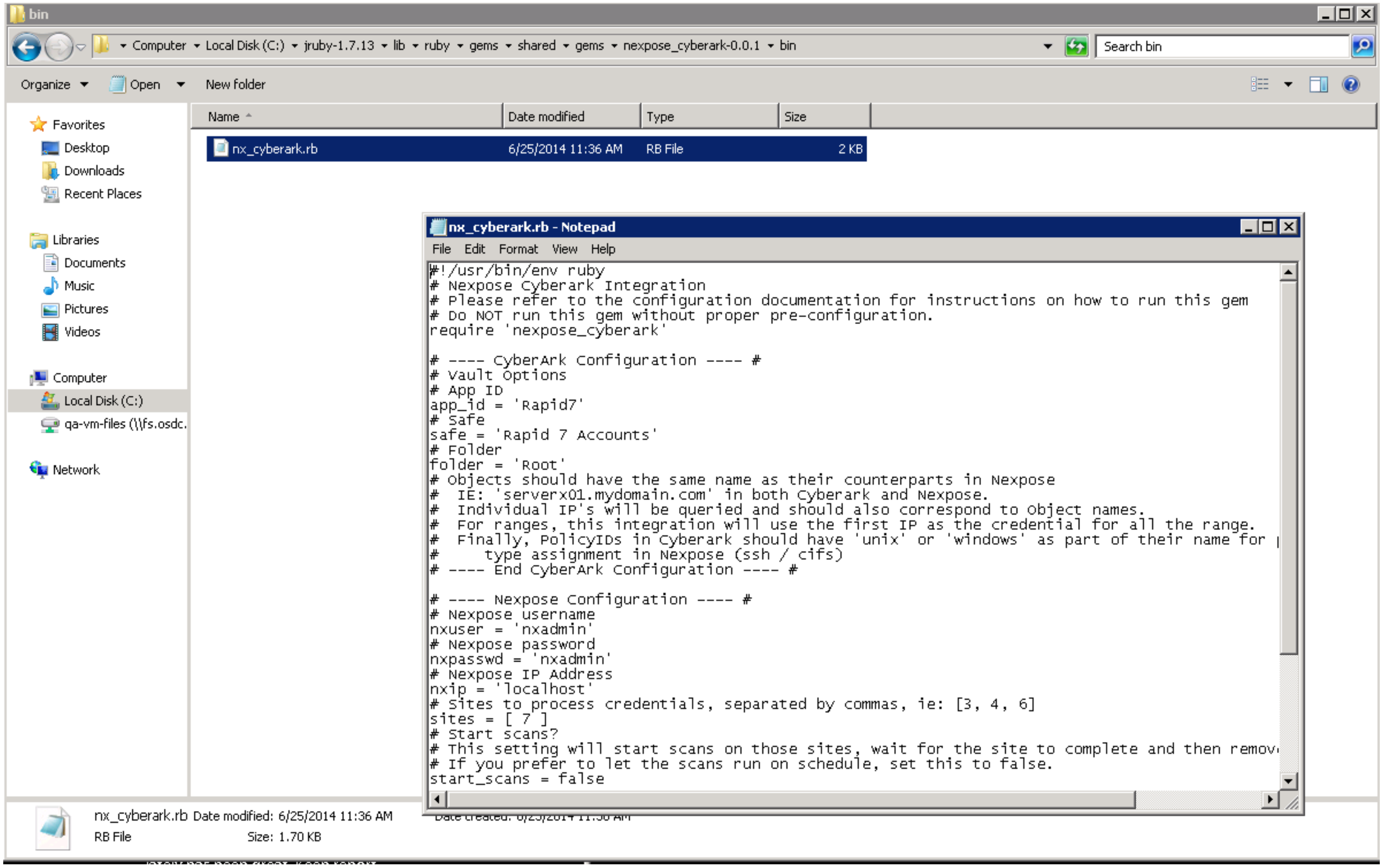


Name	Date modified	Type	Size
desktop.ini	5/10/2011 2:25 PM	Configuration settings	1 KB
jruby_windows_x64_jre_1_7_13.exe	6/25/2014 11		
nexpose_cyberark-0.0.1.gem	6/25/2014 10		

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>cd Downloads

C:\Users\Administrator\Downloads>dir
 Volume in drive C has no label.
 Volume Serial Number is 3436-0E90

 Directory of C:\Users\Administrator\Downloads

06/25/2014  11:35 AM    <DIR>          .
06/25/2014  11:35 AM    <DIR>          ..
06/25/2014  11:33 AM        51,230,208 jruby_windows_x64_jre_1_7_13.exe
06/25/2014  10:45 AM         2,564,608 nexpose_cyberark-0.0.1.gem
               2 File(s)     53,794,816 bytes
               2 Dir(s)  36,913,123,328 bytes free

C:\Users\Administrator\Downloads>jruby -S gem install nexpose_cyberark-0.0.1.gem
Fetching: librex-0.0.68.gem (100%)
Successfully installed librex-0.0.68
Fetching: rex-1.0.2.gem (100%)
Successfully installed rex-1.0.2
Fetching: nokogiri-1.6.2.1-java.gem (100%)
Successfully installed nokogiri-1.6.2.1-java
Fetching: nexpose-0.8.0.gem (100%)
Successfully installed nexpose-0.8.0
Successfully installed nexpose_cyberark-0.0.1
5 gems installed

C:\Users\Administrator\Downloads>_
```

Configuring the script

Once all dependencies have been installed, the script should now be configured. To configure, open the file nx_cyberark.rb found in the nexpose_cyberark JRuby gem bin folder. Usual paths include c:\jruby-<version>\lib\ruby\gems\shared\nexpose_cyberark-<version>\bin



Name	Date modified	Type	Size
nx_cyberark.rb	6/25/2014 11:36 AM	RB File	2 KB

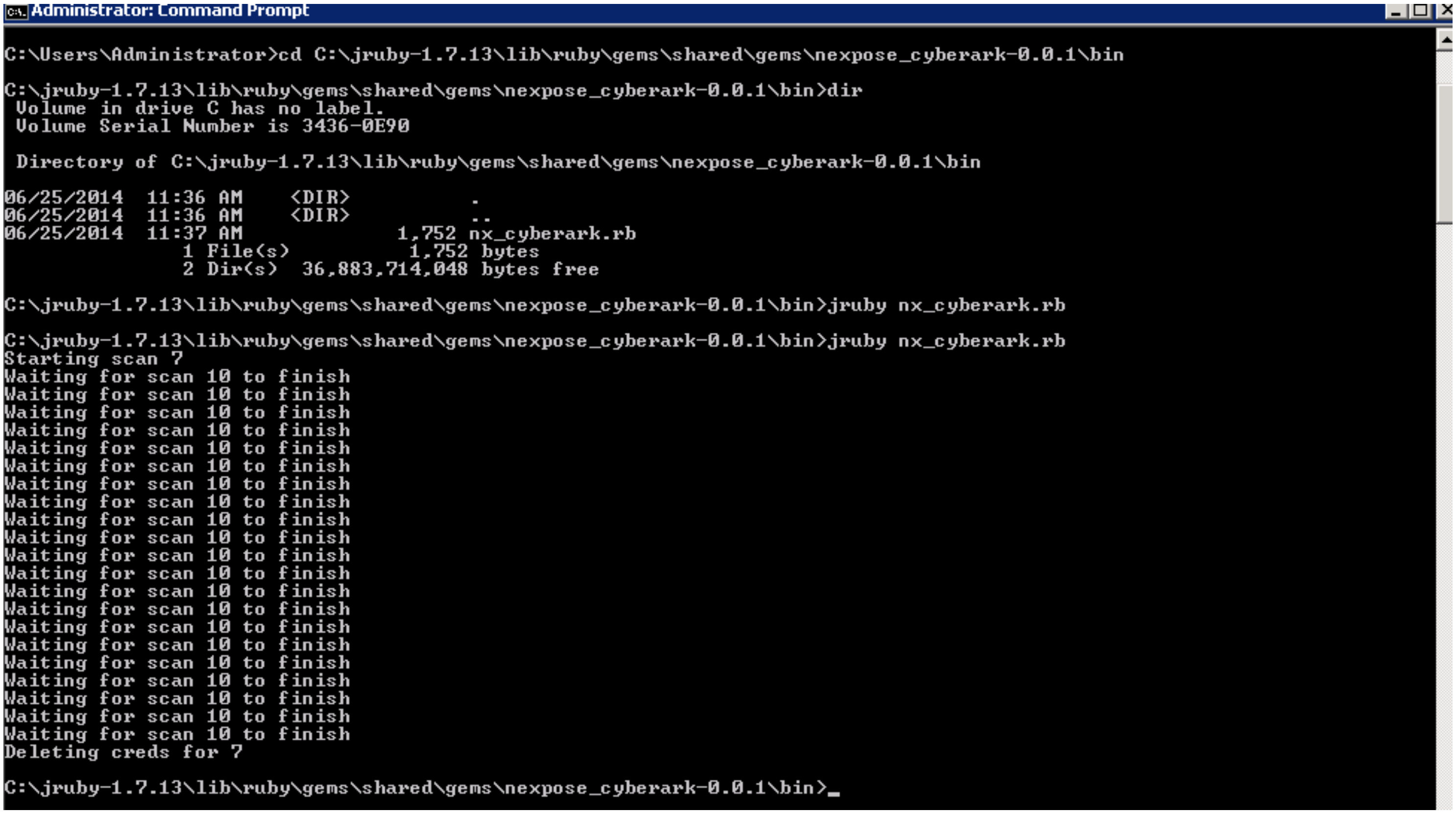
```
#!/usr/bin/env ruby
# Nexpose Cyberark Integration
# Please refer to the configuration documentation for instructions on how to run this gem
# Do NOT run this gem without proper pre-configuration.
require 'nexpose_cyberark'

# ---- CyberArk Configuration ---- #
# Vault Options
# App ID
app_id = 'Rapid7'
# Safe
safe = 'Rapid 7 Accounts'
# Folder
folder = 'Root'
# Objects should have the same name as their counterparts in Nexpose
#  IE: 'serverx01.mydomain.com' in both Cyberark and Nexpose.
#  Individual IP's will be queried and should also correspond to Object names.
#  For ranges, this integration will use the first IP as the credential for all the range.
#  Finally, PolicyIDs in Cyberark should have 'unix' or 'windows' as part of their name for
#     type assignment in Nexpose (ssh / cifs)
# ---- End CyberArk Configuration ---- #

# ---- Nexpose Configuration ---- #
# Nexpose username
nxuser = 'nxadmin'
# Nexpose password
nxpasswd = 'nxadmin'
# Nexpose IP Address
nxip = 'localhost'
# Sites to process credentials, separated by commas, ie: [3, 4, 6]
sites = [ 7 ]
# Start scans?
# This setting will start scans on those sites, wait for the site to complete and then remov
# If you prefer to let the scans run on schedule, set this to false.
start_scans = false
```

nx_cyberark.rb Date modified: 6/25/2014 11:36 AM
RB File Size: 1.70 KB

- Configure Vault settings:
  - APP ID, Safe, Folder properties from CyberArk. Please refer to CyberArk documentation.
- Configure Nexpose settings:
  - A valid nexpose user, password, ip address and sites to manage.
  - The start scan variable. If set to true, once updated the gem will trigger a scan of the site, wait until it's finished and deletes the credentials stored. If set to false, it'll not kick a scan and will run on scheduled.
- Run the script for the first time.
  - The script can be run using the command from the command line:

    ```
    > jruby nx_cyberark.rb
    ```

  - The script will run and perform the queries, if the start scan variable is set to false, the script will exit silently; otherwise the script will output the status of each scan
  - **Note: Passwords stored in Cyber Ark can be rotated before a scan is initiated. Make sure you synchronize properly the scanning window with your password rotations.**



```
C:\Users\Administrator>cd C:\jruby-1.7.13\lib\ruby\gems\shared\gems\nexpose_cyberark-0.0.1\bin

C:\jruby-1.7.13\lib\ruby\gems\shared\gems\nexpose_cyberark-0.0.1\bin>dir
 Volume in drive C has no label.
 Volume Serial Number is 3436-0E90

 Directory of C:\jruby-1.7.13\lib\ruby\gems\shared\gems\nexpose_cyberark-0.0.1\bin

06/25/2014  11:36 AM    <DIR>          .
06/25/2014  11:36 AM    <DIR>          ..
06/25/2014  11:37 AM             1,752 nx_cyberark.rb
               1 File(s)          1,752 bytes
               2 Dir(s)  36,883,714,048 bytes free

C:\jruby-1.7.13\lib\ruby\gems\shared\gems\nexpose_cyberark-0.0.1\bin>jruby nx_cyberark.rb

C:\jruby-1.7.13\lib\ruby\gems\shared\gems\nexpose_cyberark-0.0.1\bin>jruby nx_cyberark.rb
Starting scan 7
Waiting for scan 10 to finish
Waiting for scan 10 to finish
Waiting for scan 10 to finish
Waiting for scan 10 to finish
Waiting for scan 10 to finish
Waiting for scan 10 to finish
Waiting for scan 10 to finish
Waiting for scan 10 to finish
Waiting for scan 10 to finish
Waiting for scan 10 to finish
Waiting for scan 10 to finish
Waiting for scan 10 to finish
Waiting for scan 10 to finish
Waiting for scan 10 to finish
Waiting for scan 10 to finish
Waiting for scan 10 to finish
Waiting for scan 10 to finish
Waiting for scan 10 to finish
Waiting for scan 10 to finish
Waiting for scan 10 to finish
Waiting for scan 10 to finish
Deleting creds for 7

C:\jruby-1.7.13\lib\ruby\gems\shared\gems\nexpose_cyberark-0.0.1\bin>_
```

What if something goes wrong?

The most common errors when running the script are configuration based, users without permission to update sites, or query credentials from CyberArk

1. Make sure the objects have the same name in Nexpose and in CyberArk.

2. Make sure the username of Nexpose can save sites and kick scans

3. Check that the CyberArk Folder, App id and safe settings are properly configured.

4. If anything else fails, please email us to integrations_support@rapid7.com with the information about the issue.