Technology Partner Program Integration Guide

Author: Skybox Security Inc.

Revision History	
<Date>	<Description of the revision, changes - e.g. “Re - validated the integration on PAN - OS 9.1- added support for dynamic user groups”>

Partner Information	
Date	March 1st, 2020
Partner Name	Skybox security
Website	http://www.skyboxsecurity.com
Product Name	SPM, VTM
Partner Contact	support@skyboxsecurity.com
Support Contact	SPM
Product Description	Security Policy Management

Palo Alto Networks Products for Integration

Table 1: Integration Details by Product			
Palo Alto Networks Product	Integration Status	Palo Alto Networks Versions Tested	Skybox Versions Tested
AutoFocus			
Cortex XDR Prevent			
Cortex XDR Pro			
Next - Generation Firewall	Validated	PAN-OS 9.0	10.1.500-11.0.101
Panorama	Validated	PAN-OS 9.0	10.1.500-11.0.101
Prisma Access			
Prisma Cloud Compute			
Prisma Cloud Enterprise			
Prisma SaaS			
VM - Series			
WildFire			
Other			

Use Cases for Integration with the Palo Alto Networks Security Operating Platform

The Skybox Platform combines firewall and network device data visibility with vulnerability management and threat intelligence, prioritizing security issues in the context of your unique environment. To do that, Skybox needs to be able to connect to all your network assets including firewalls, scanners, and so on.

Use case #1 – Firewall Assurance

Skybox Security's firewall management capabilities enhance the more targeted security controls presented by Palo Alto Networks NGFW (next-generation firewalls). The Skybox Firewall Assurance module automatically verifies the use and effectiveness of user and application–specific network security controls in protecting against cyberthreats and misuse. Palo Alto Networks customers can establish next-generation firewall access and rule compliance policies by application and user levels, create firewall rule checks against these policies, track application changes, monitor network traffic for IPS policies, and verify that firewall configuration settings match best practice security guidelines.

The Skybox Platform in combination with Panorama combines firewall and network device data visibility with vulnerability management and threat intelligence, prioritizing security issues in the context of the customers unique environment.

Use case #2 – Network Assurance

Skybox Network Assurance provides total network visibility in the context of network devices and security controls including the Palo Alto Networks security platform, showing how they work together – or leave you exposed. With Network Assurance, you can find potential attack vectors, check the correct implementation of security zone policies that include user and application filters in addition to source and destination, or troubleshoot the root causes of network outages.

Use case #3 – Vulnerability Control

Skybox Vulnerability Control is a context-aware vulnerability management solution that goes beyond traditional vulnerability assessment and extends the visualization capabilities of Panorama. Vulnerability Control consolidates vulnerability sources and uses scanless vulnerability detection to fill in blind spots. It then applies attack simulation, superior vulnerability intelligence, and powerful analytics to quickly prioritize and eliminate attack vectors. Skybox Vulnerability Control has been optimized to support new intrusion detection devices and deployment options, allowing customers to take full advantage of active protection capabilities, including embedded IPS and L2 transparent deployments of the Palo Alto Networks security platform.

Integration Benefits

Skybox Security and Palo Alto Networks for network security configuration and compliance management offers:

- Complete support for next-gen access and rule compliance at the user and application level
- IPS signature management based on network context
- Full next-gen, on-demand policy compliance audits (PCI-DSS, NIST, best practices)
- Complete change tracking with application and user; shadowed and redundant rule analysis
- Comprehensive network modeling and access path analysis with patent-pending Access Analyzer to troubleshoot application and user connectivity issues — in seconds
- Automated network-wide assessments of stateful and next-gen security gaps with suggested remediation options

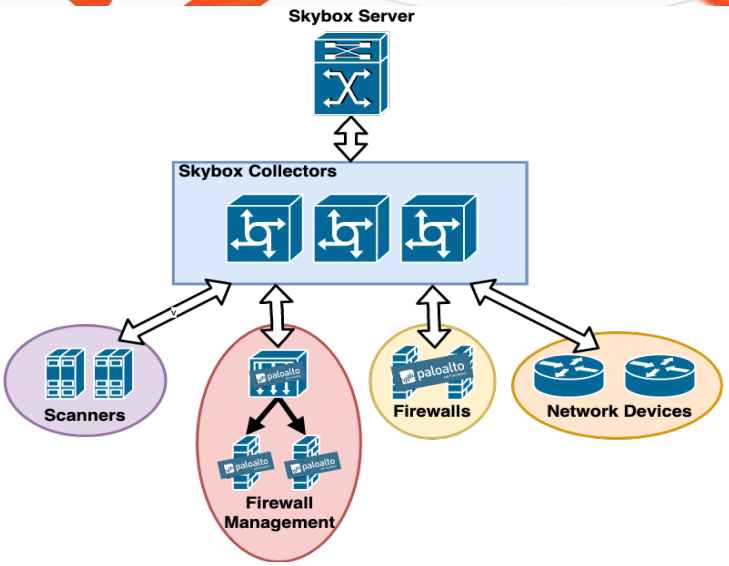
In addition, Skybox provides Integrated platform configuration checks for Palo Alto Networks including integration with the Panorama Management Platform

Skybox Security also includes provisioning capabilities for Palo Alto Network devices:

Device Support	Add Rule	Add Object	Modify Rule	Modify Object	Delete Rule / Disabled Rule	Global Rule	Global Object
Palo Alto Networks	Supported	Supported	Supported	Supported	TBD	TBD	Supported

Integration Diagram

- *The Skybox Collectors are responsible for connecting to the devices and collecting the needed data. Data is collected from the Palo alto Firewalls and Panorama using REST API calls and SSH commands.*
- *After the Data is collected the collector is transferring the data to the Skybox server for modeling, parsing and analyzing.*
- The data collected includes Rule base (local and panorama policies), Routing data, Objects etc.



Before You Begin

- Skybox data collection requires a Super User on the device; we recommend that you create a separate Super User Admin Account for this purpose.
- Configure the firewall to permit collection. (The Skybox Collector must have permission to connect to the firewall using HTTPS on port 443, and either SSH or Telnet(not-recommended).)

Palo Alto Networks Configuration

- Create a dedicated service account for Skybox to access Palo Alto Networks Firewall and Panorama via API and SSH.

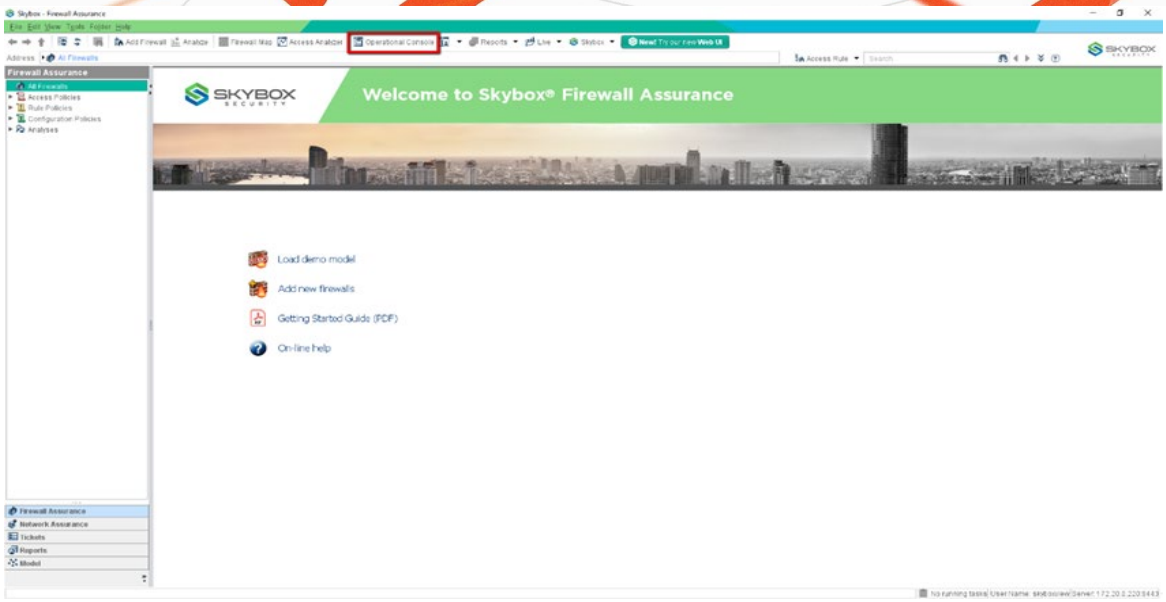
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-panorama-api/get-started-with-the-pan-os-xml-api/enable-api-access.html#ide6063ba8-2b0b-42eb-98c2-eb4914061722

- Configure Syslog forwarding to send Traffic and Configuration logs to Skybox Collector Syslog Server.

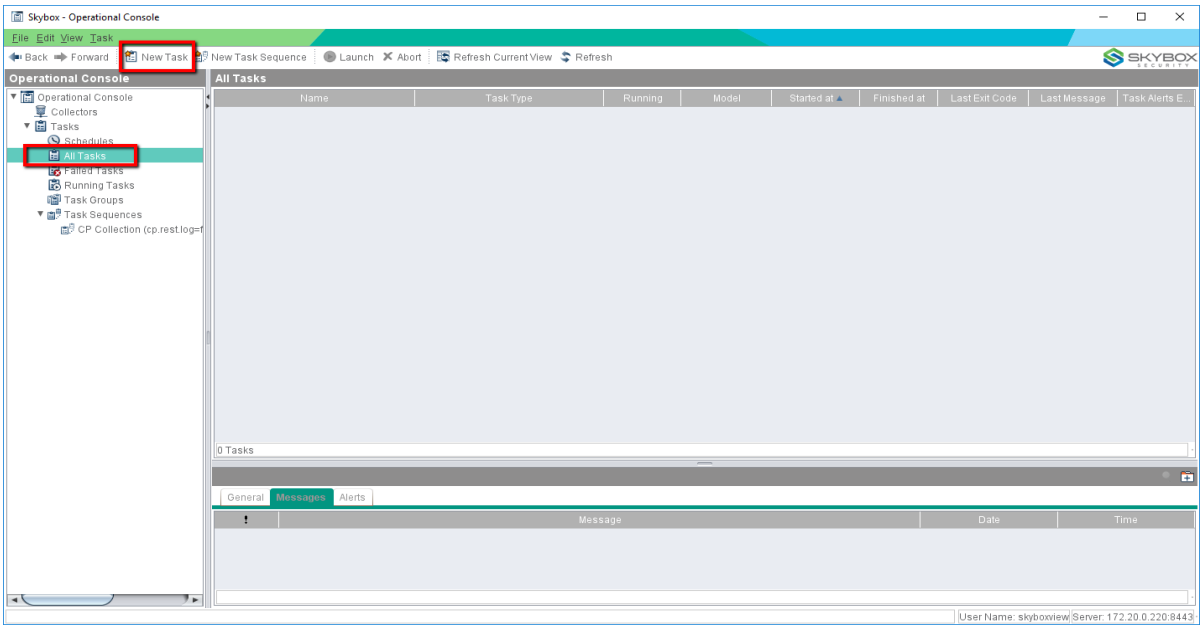
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/use-syslog-for-monitoring/configure-syslog-monitoring.html

Partner Product Configuration

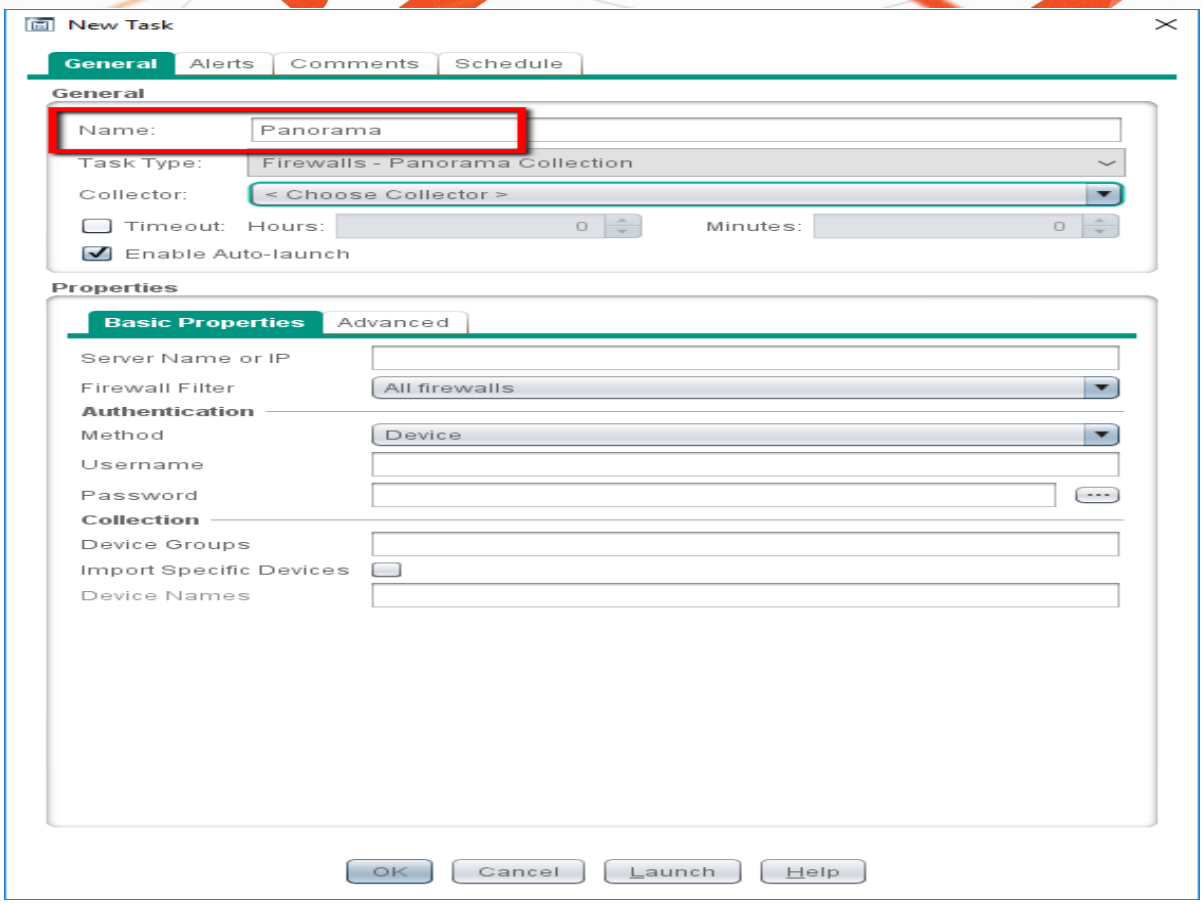
- Log in to Skybox Firewall Assurance
- Open “Operational console”



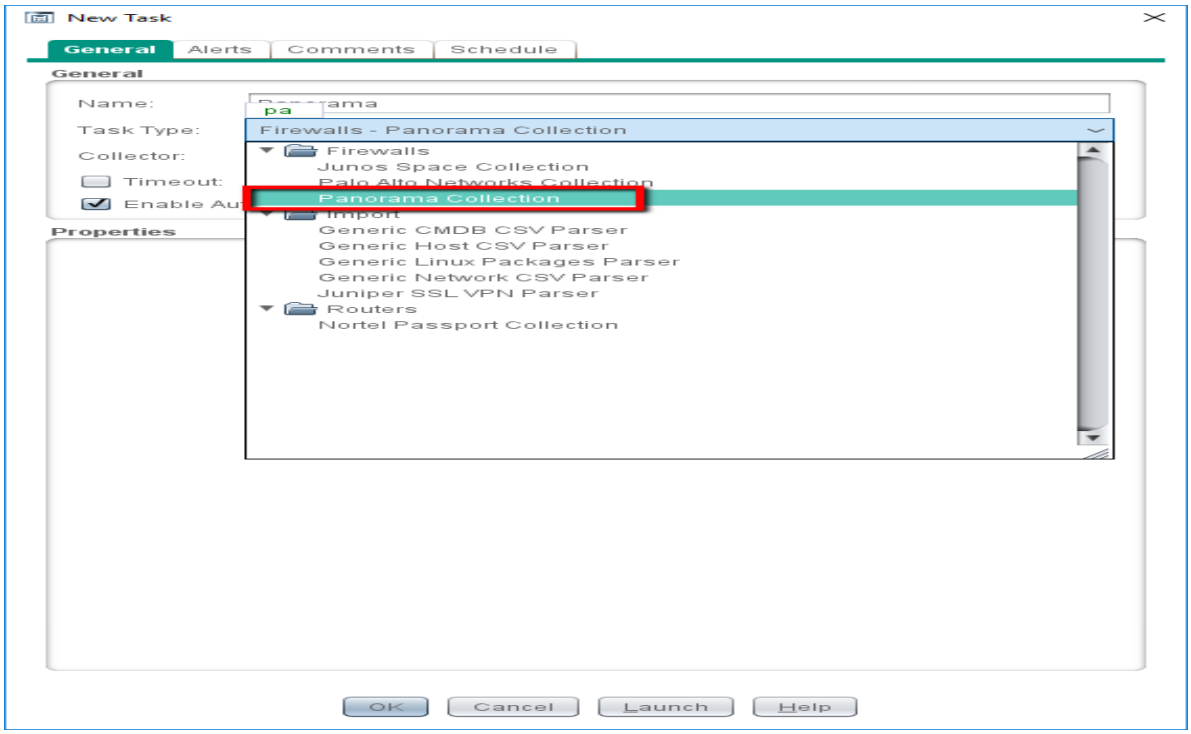
- Create a new collection task



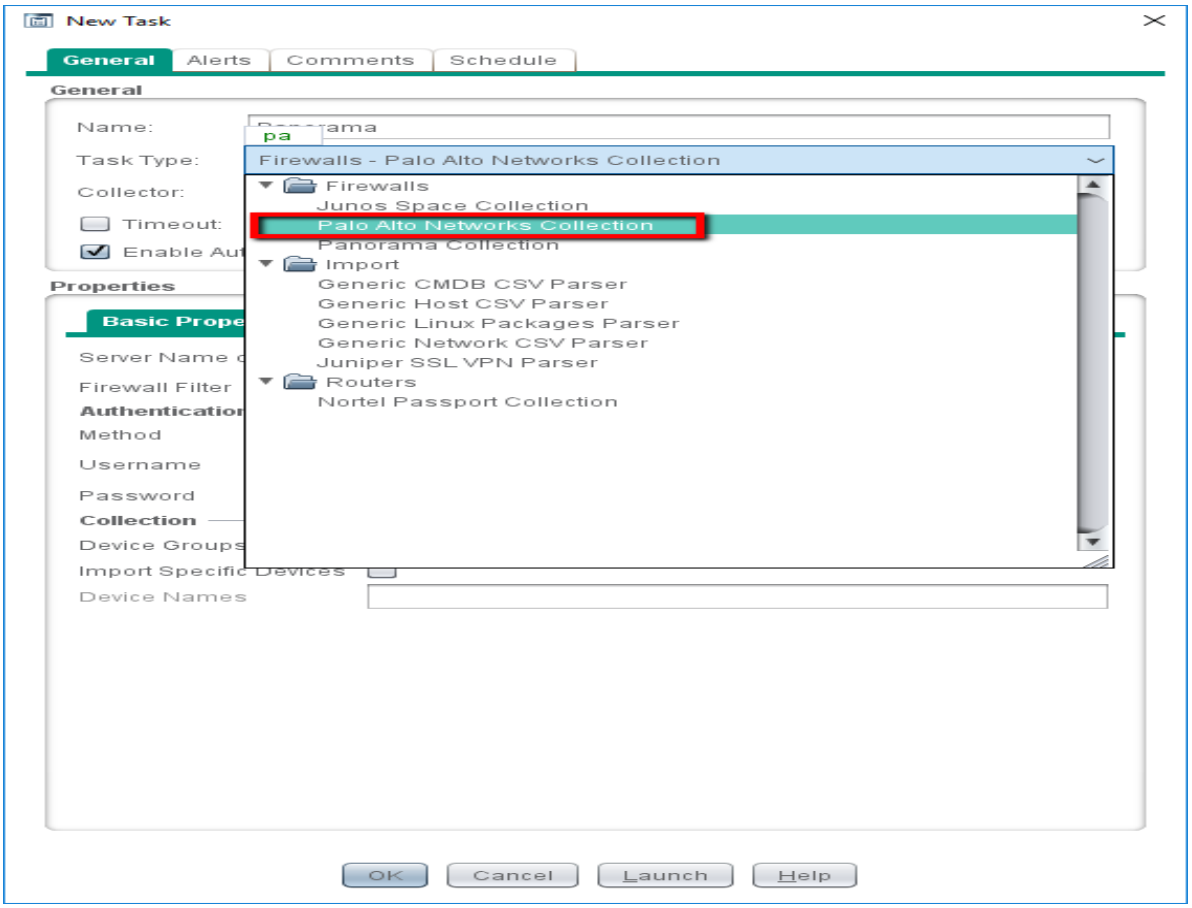
- Set task name



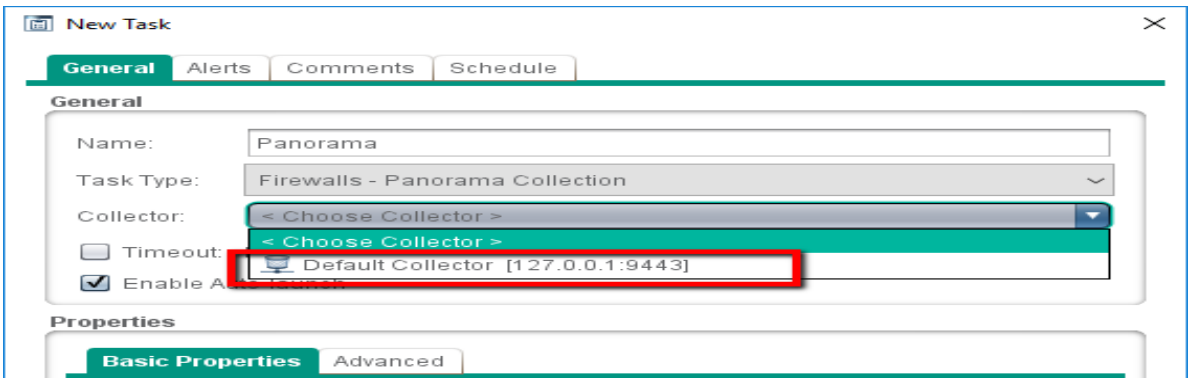
- For Panorama devices select “Panorama Collection”



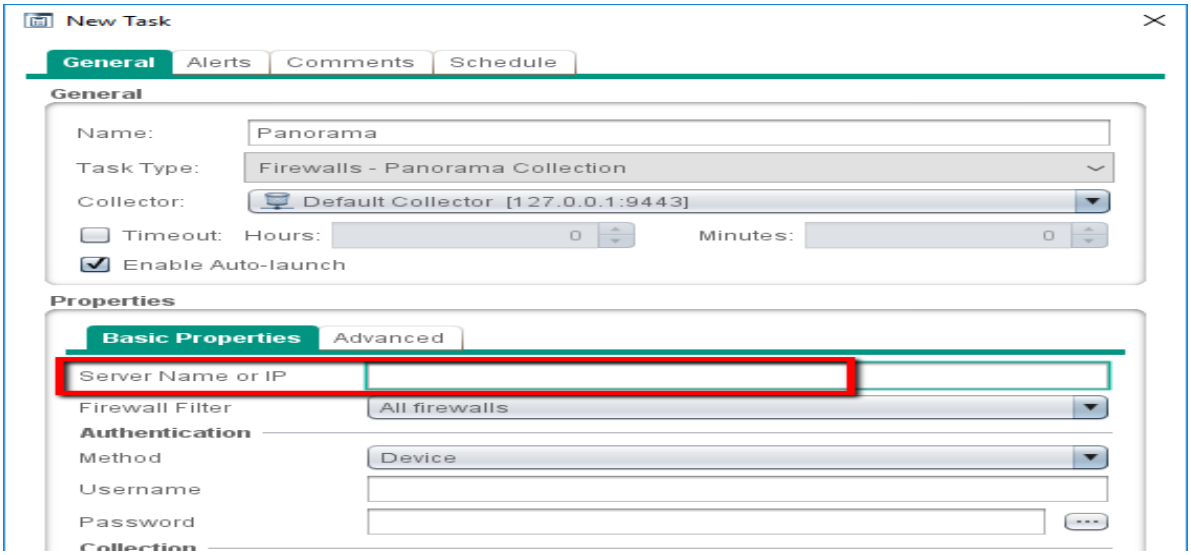
- For Palo Alto Firewall devices select “Palo Alto Networks Collection”

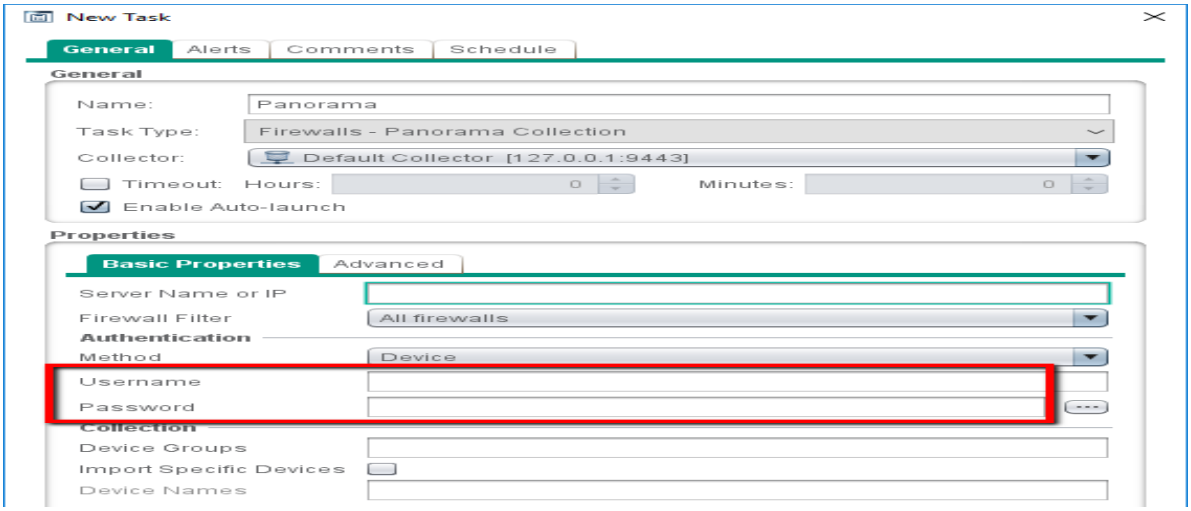


- Select the Collector that will run the task



- Enter the device IP, user & password

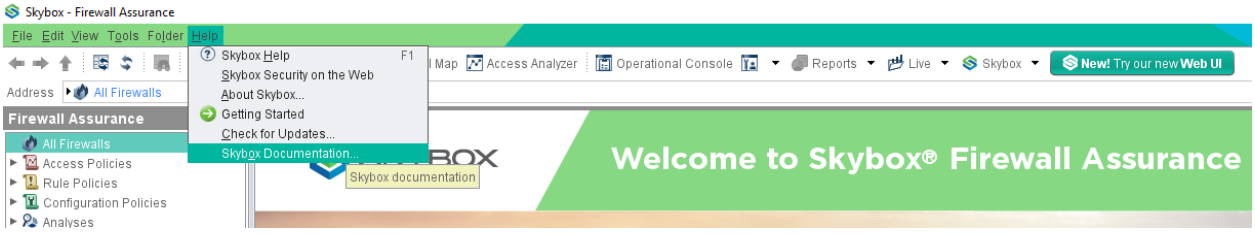




- Click Launch to begin the collection process

Troubleshooting

For troubleshooting problems or just to have a better understanding of Skybox capabilities you can use our documentation center



(OR via web browser - http://downloads.skyboxsecurity.com/files/Installers/Skybox_View/latestDocs/)

Please contact Skybox security support center for help by email support@skyboxsecurity.com.

Technical Details

- List of REST API calls used for collection:
  - https://<FW_IP>/api/?type=keygen&user=<admin name>&password=<password>
  - https://<FW_IP>/api/?type=config&action=show&key=<key>
  - https://<FW_IP>/api/?type=config&action=get&xpath=/config/predefined/application&key=<key>
  - https://<FW_IP>/api/?type=config&action=get&xpath=/config/devices/entry/vsys/entry/application-filter&key=<key>
  - https://<FW_IP>/api/?type=config&action=get&xpath=/config/devices/entry/vsys/entry/application-groups&key=<key>
  - https://<FW_IP>/api/?type=config&action=get&xpath=/config/predefined/service&key=<key>
  - https://<FW_IP>/api/?&type=op&action=get&cmd=<show><predefined><xpath>/predefined/threats/vulnerability</xpath></predefined></show>&key=<key>
  - https://<FW_IP>/api/?type=config&action=get&&xpath=/config/panorama&key=<key>
  - https://<FW_IP>/api/?type=op&action=get&cmd=<show><object><dynamicaddress-roup><all></all></dynamic-addressgroup></object></show>&key=<key>
  - https://<FW_IP>/api/?type=op&action=get&cmd=<show><highavailability><state></state></highavailability></sow>&key=<key>
  - https://<FW_IP>/api/?type=op&action=get&cmd=<show><system><info></info></system></show>&key=<key>
  - https://<FW_IP>/api/?type=op&action=get&cmd=<show><interface>all</interface></show>&target=<target>&key=<key>
- SSH commands used for collection:
  - get system info
  - Set cli pager off
  - Show routing route

- Syslog is used for Audit and Rule Usage Analysis