CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Skybox Security

Website: https://www.skyboxsecurity.com

Name of Product: SPM

Version: 9

Date: 21 October 2018 (Revised 21 May 2021)

SKYBOX SOLUTION OVERVIEW

The Skybox suite is a powerful set of attack vector analytics that reduces response times and risks, bringing firewall, vulnerability, and threat management processes for complex networks under control. Skybox will reduce your attack surface and help contain cyberattacks fast. It's a cybersecurity management solution that gives you total visibility and actionable security intelligence.

The Skybox security suite is based on Security Policy Management (SPM) and Vulnerability and Threat Management (VTM).

Version: 9

Platform components:

SPM Components

- **Firewall Assurance**: Skybox Firewall Assurance brings all firewalls into one normalized view, continuously monitoring policy compliance, optimizing firewall rulesets and finding attack vectors that others miss
- **Network Assurance**: Skybox Network Assurance illuminates complex network security and policy compliance interactions, giving you visible insights to reduce attack vectors and network disruptions
- **Change Manager**: Skybox Change Manager ends risky changes with network-aware change planning and risk assessment, and speeds up firewall change processes with customizable workflows

VTM Components

- **Vulnerability Control**: Skybox Vulnerability Control eliminates blind spots and shows how vulnerabilities and threats could impact you, prioritizing remediation in a way that makes sense for your organization
- **Threat Manager**: Skybox Threat Manager keeps you on top of threat intelligence at all times. You'll know if a new advisory is important to your network, what assets are at stake, and where to start your response

KEY BENEFITS

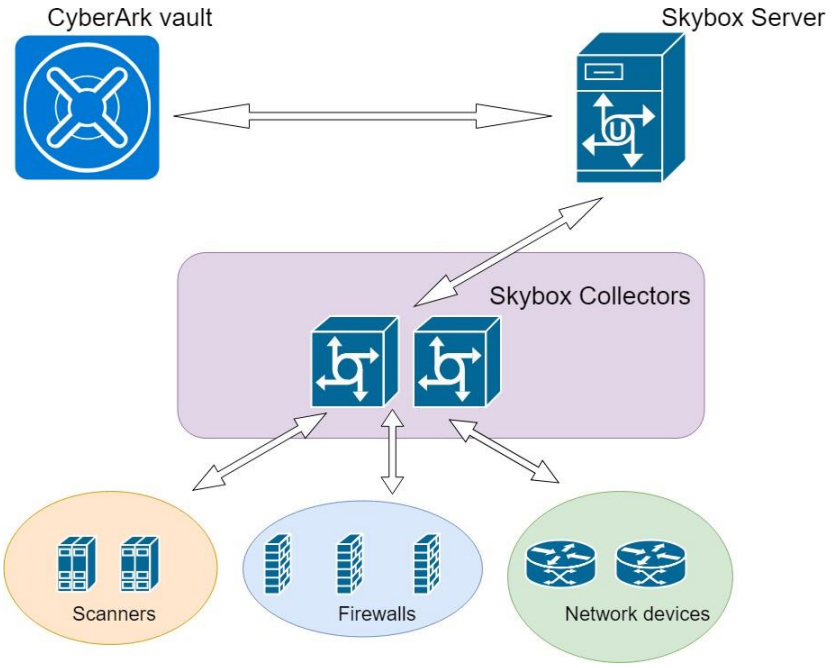
Benefits of Skybox:

- Combines firewall and network device data visibility with vulnerability management and threat intelligence
- Prioritizes security issues in the context of your unique environment

Benefits of integrating Skybox with CyberArk Secrets Manager:

- Allows Skybox to connect to network assets such as firewalls and scanners, in the most secure way, leaving password management and access control to be managed by CyberArk

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER INTEGRATION

Skybox analyses are based on data received from devices in your organizational network. A typical installation of Skybox within an organization is described in the diagram above: A Skybox Server, which runs all the analysis and manages all the collection tasks, and one or more Skybox Collectors (depending on the number and size of assets to collect from) that connect to the devices and retrieve their data.

CREDENTIAL RETRIEVAL

When a collection task runs, Skybox Server uses the CyberArk Vault and the application configured in Skybox. CyberArk creates a secure connection to the device without revealing the credentials to Skybox. The process in which Skybox Server requests CyberArk to connect to the device is made every time the task runs (either per a predefined schedule or on demand).

REQUIREMENTS

CyberArk integration works on Linux-based and Windows-based Skybox installations.

SECRETS MANAGER INSTALLATION

Refer to the "Credential Provider and ASCP Implementation Guide" for CyberArk Agent based installation and configuration.

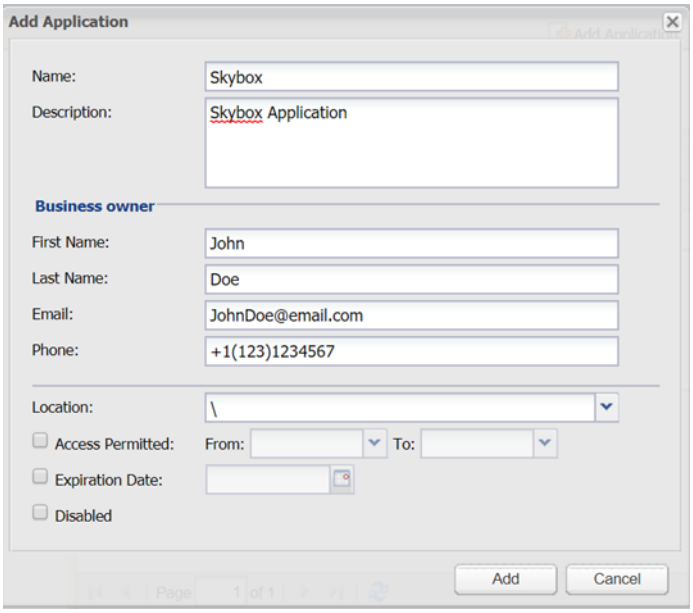
SECRETS MANAGER CONFIGURATION

The following sections provide details on Skybox configuration with CyberArk Secrets Manager.

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

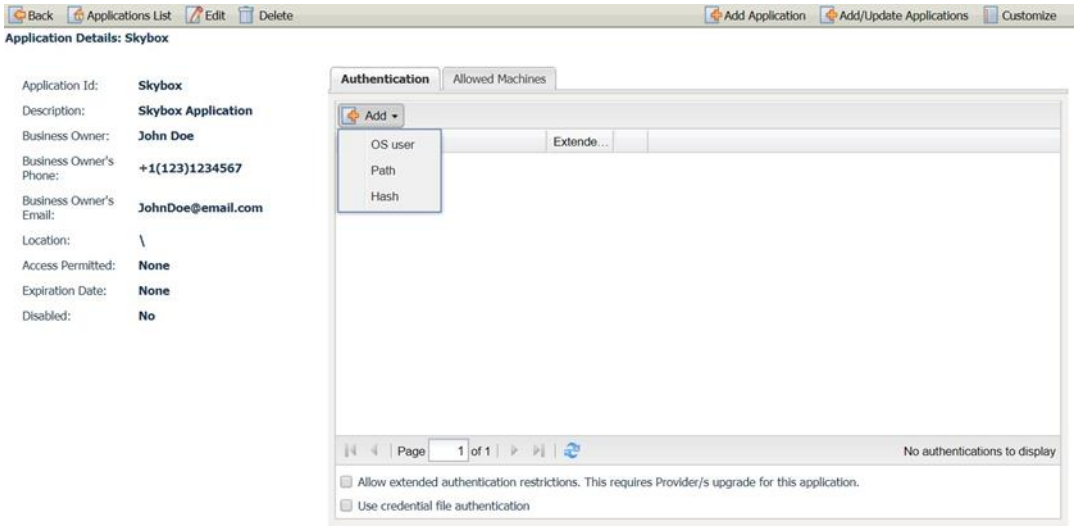
To define the application, define it manually through the CyberArk Password Vault Web Access (PVWA) interface:

- ☐ Log in as user allowed to manage applications (it requires Manage Users authorization)
- ☐ In the Applications tab, click **Add Application**. The Add Application page appears.



- ☐ Specify the following information:
  - In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: Skybox
  - In the **Description** box, specify a short description of the application that will help you identify it.
  - In the **Business owner** section, specify contact information about the application's business owner.
  - In the **Location** box, specify the location of the application in the Vault hierarchy. If a location is not selected, the application will be added in the same location as the user who is creating this application.

☐ Click **Add**. The application is added and is displayed in the Application Details page.



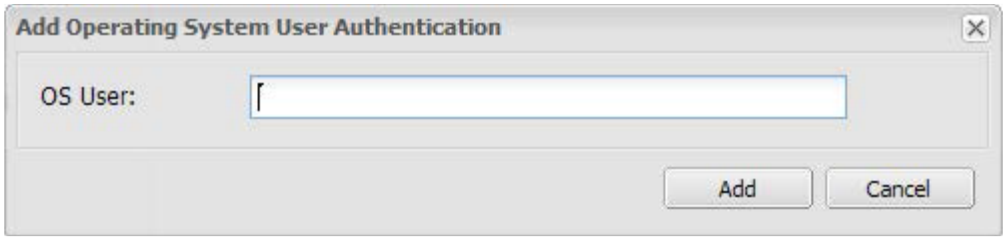
☐ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.

☐ Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password. For Skybox, select **OS user** and **Path**.

☐ In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.

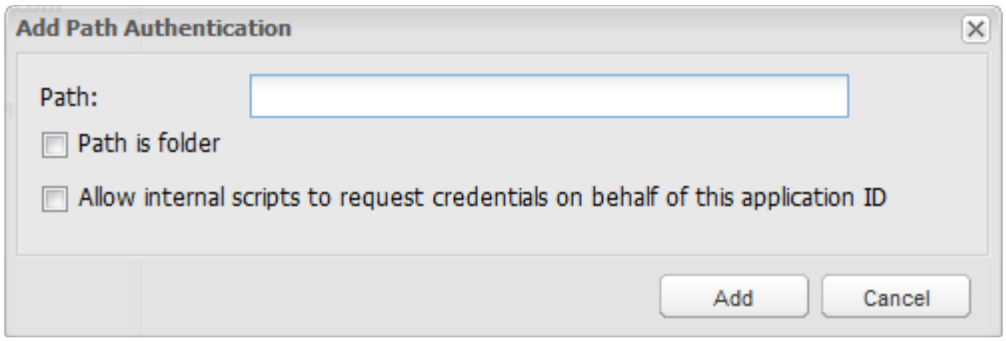
☐ Select the authentication characteristic to specify.

☐ Select **OS user**. The Add Operating System User Authentication window appears.



☐ Specify the name of the OS user who will run the application, then click **Add**. The OS user is listed in the Authentication tab.

☐ Select **Path**. The Add Path Authentication window appears.



☐ In the **Path** box, specify the path where the application will run. To indicate that the specified path is a folder, select **Path is folder**. To allow internal scripts to retrieve the application password for this application, select **Allow internal scripts to request credentials on behalf of this application ID**.

☐ Click **Add**. The Path is added as an authentication characteristic with the information that you specified.

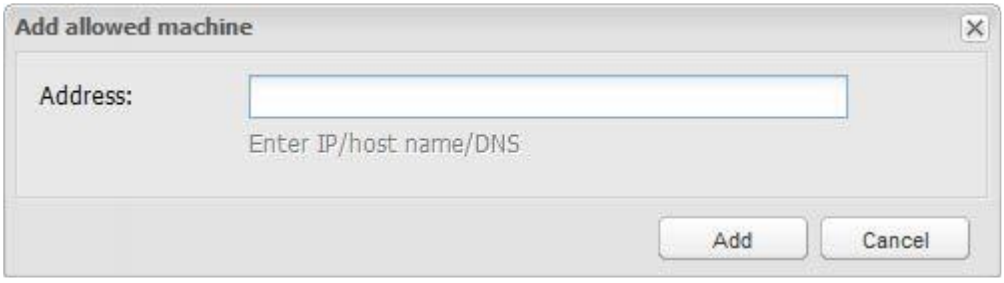
☐ Specify a hash:

- Run the AIMGetAppInfo utility to calculate the application's unique hash. Copy the hash value that is returned by the utility.
- In the PVWA, select **Hash**. The Add Hash window appears.

- In the Hash edit box, paste the application's unique hash value, or specify multiple hash values with a semi-colon. You can add additional information in a comment after each hash value specified for an application by specifying '#' after the hash value, followed by the comment. For example, OE883B7OD5B6E3EE37D37198049C9507C8383DB6 **#app2**
  Note: The comment must not include a colon or a semicolon.
- Click **Add**. The Hash is added as an authentication characteristic with the information that you specified.

☐ Specify the application's Allowed Machines. This information enables the Credential Provider to make sure that only applications that run from specified machines can access their passwords.

- In the Allowed Machines tab, click **Add**. The Add allowed machine window is displayed.



- In the **Address** box, specify the IP/hostname/DNS of the machine where the application will run and will request passwords, then click **Add**. The IP address is listed in the Allowed Machines tab.

  Make sure the servers allowed include all mid-tier servers or all endpoints where the Secrets Manager Credential Providers were installed.

PROVISIONING ACCOUNTS AND SETTING PERMISSIONS FOR APPLICATION ACCESS

For the application to perform its functionality or tasks, the application must have access to particular existing accounts, or new accounts to be provisioned in CyberArk Vault.

In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:

- **Manually** – Add accounts manually one at a time, and specify all the account details.
- **Automatically** – Add multiple accounts automatically using the Password Upload feature.

  For this step, you require the **Add accounts** authorization in the Password Safe.

For more information about adding and managing privileged accounts, refer to **the Privileged Access Security Implementation Guide.**

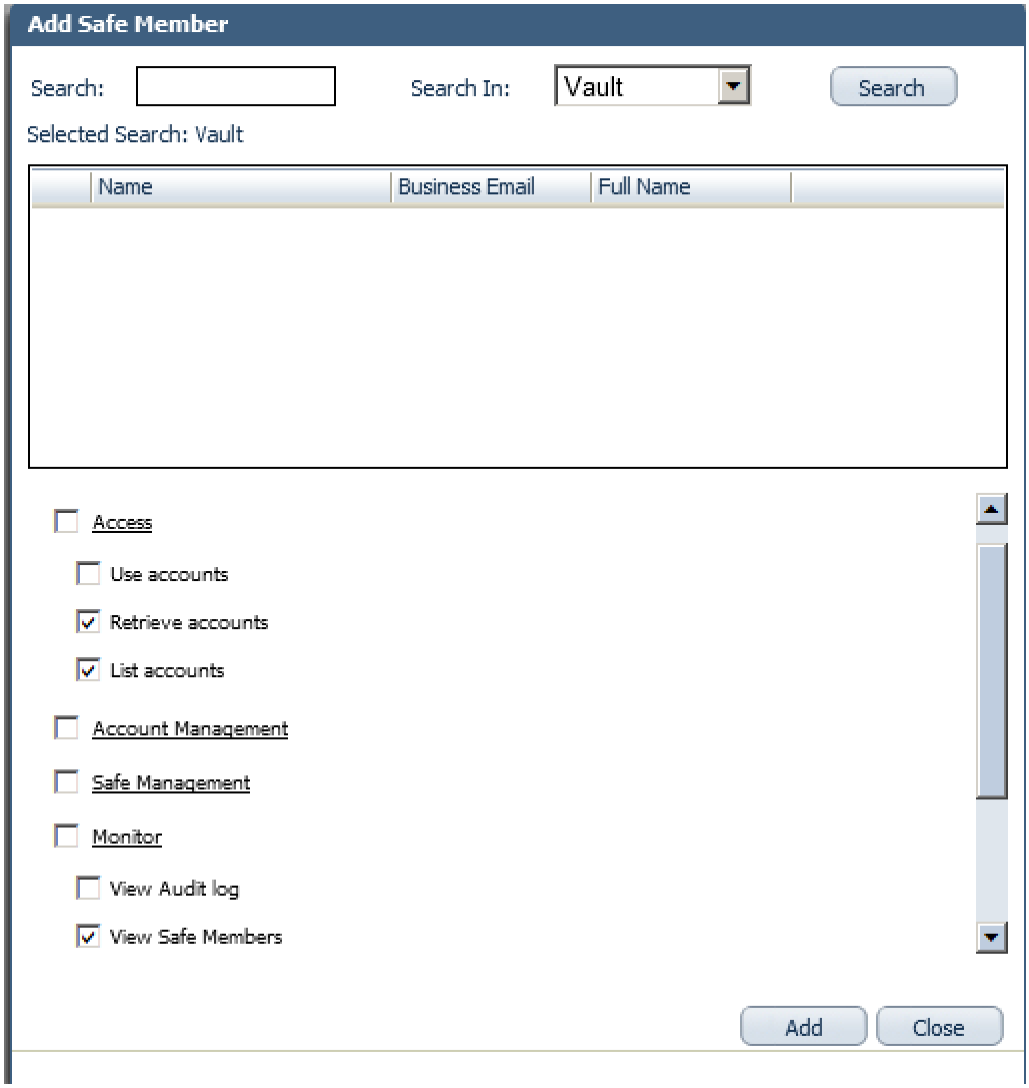
Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

Add the Credential Provider and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.

☐ Add the Provider user as a Safe Member with the following authorizations:

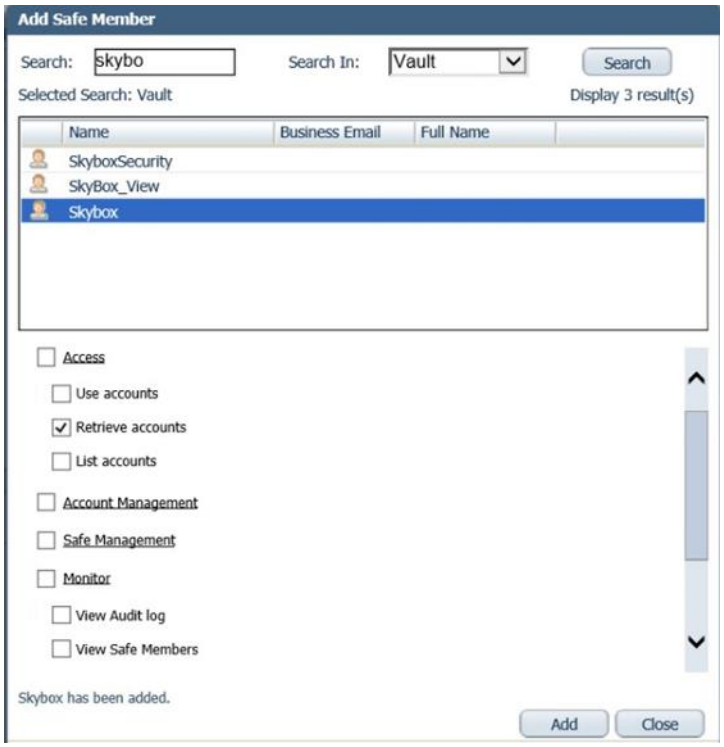
- List accounts
- Retrieve accounts
- View Safe Members

Note: When installing multiple Providers for this integration, it is recommended to create a group for them, and add the group to the Safe once with the above authorization.



☐ Add the application (the APPID) as a Safe Member with the following authorizations:

- Retrieve accounts



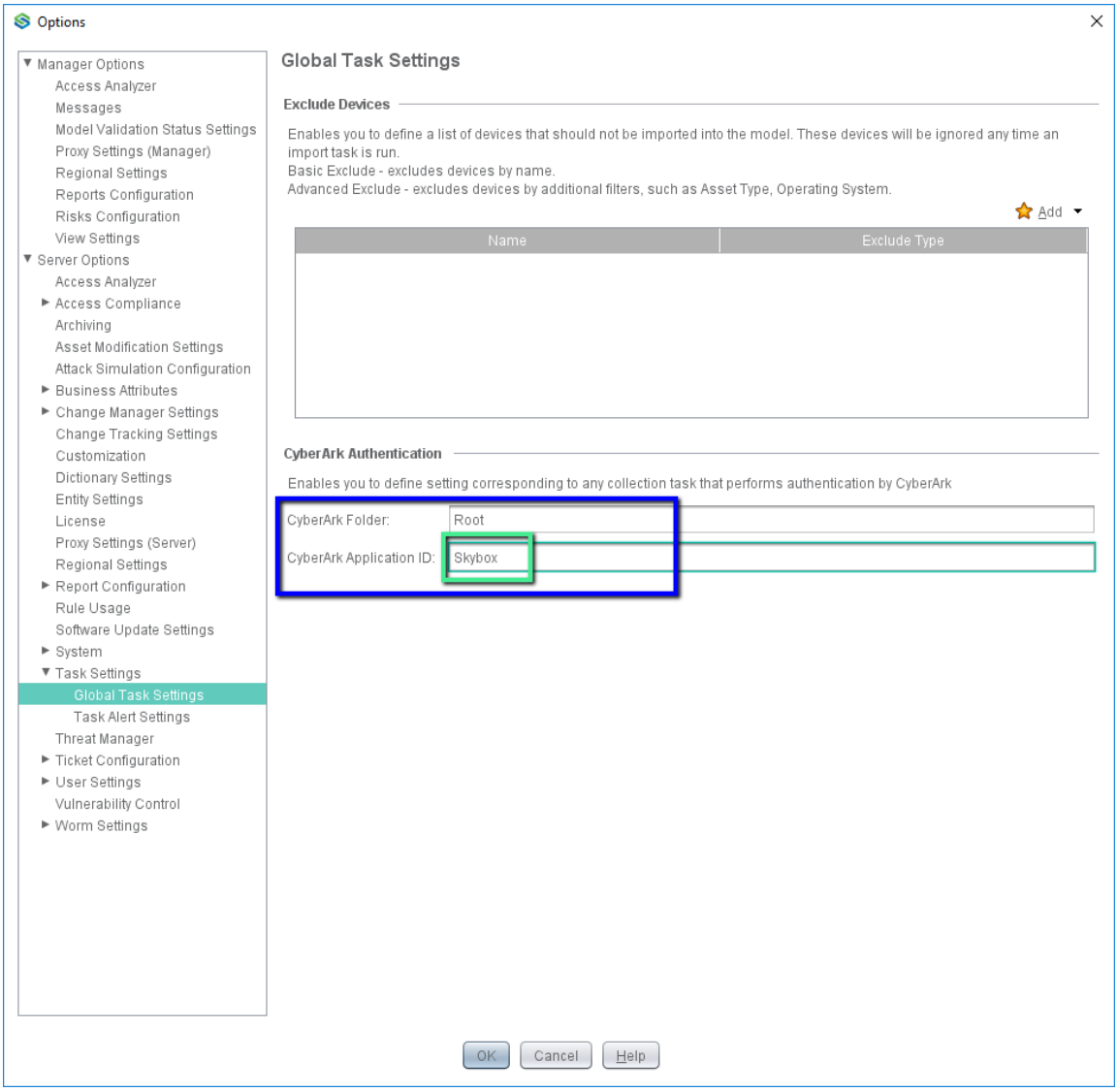
☐ If the Safe is configured for object level access, make sure that both the Provider user and the application have access to the password(s) to retrieve.

For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide.**

SKYBOX INSTALLATION & INTEGRATION CONFIGURATION

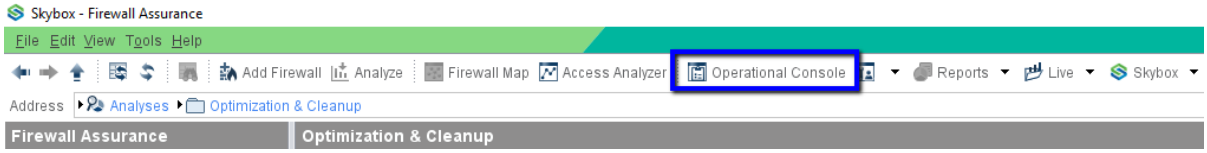
Refer to "Skybox_ReferenceGuide_V9_0_600.pdf" for Skybox installation.

1. Set the Application ID in Skybox as follows:
   a. From the Skybox application, go to **Tools** > **Options**.
   b. Under **Server Options** go to **Task Settings** > **Global Task Settings**.
   c. Add The default folder (Root) and the CyberArk application ID.

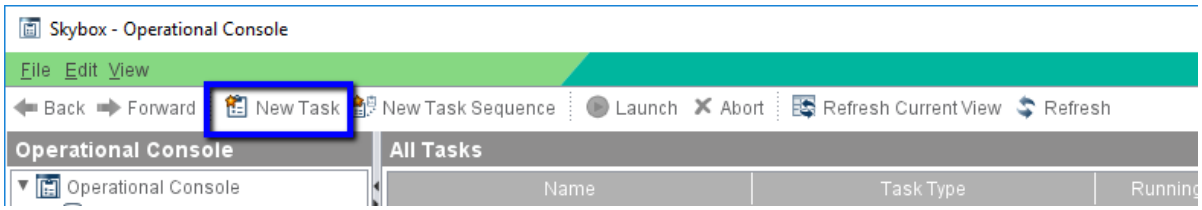

Options
Manager Options
Access Analyzer
Messages
Model Validation Status Settings
Proxy Settings (Manager)
Regional Settings
Reports Configuration
Risks Configuration
View Settings
Server Options
Access Analyzer
Access Compliance
Archiving
Asset Modification Settings
Attack Simulation Configuration
Business Attributes
Change Manager Settings
Change Tracking Settings
Customization
Dictionary Settings
Entity Settings
License
Proxy Settings (Server)
Regional Settings
Report Configuration
Rule Usage
Software Update Settings
System
Task Settings
Global Task Settings
Task Alert Settings
Threat Manager
Ticket Configuration
User Settings
Vulnerability Control
Worm Settings
Global Task Settings
Exclude Devices
Enables you to define a list of devices that should not be imported into the model. These devices will be ignored any time an import task is run.
Basic Exclude - excludes devices by name.
Advanced Exclude - excludes devices by additional filters, such as Asset Type, Operating System.
Add
Name
Exclude Type
CyberArk Authentication
Enables you to define setting corresponding to any collection task that performs authentication by CyberArk
CyberArk Folder:
Root
CyberArk Application ID:
Skybox
OK
Cancel
Help

2. Click **OK**.

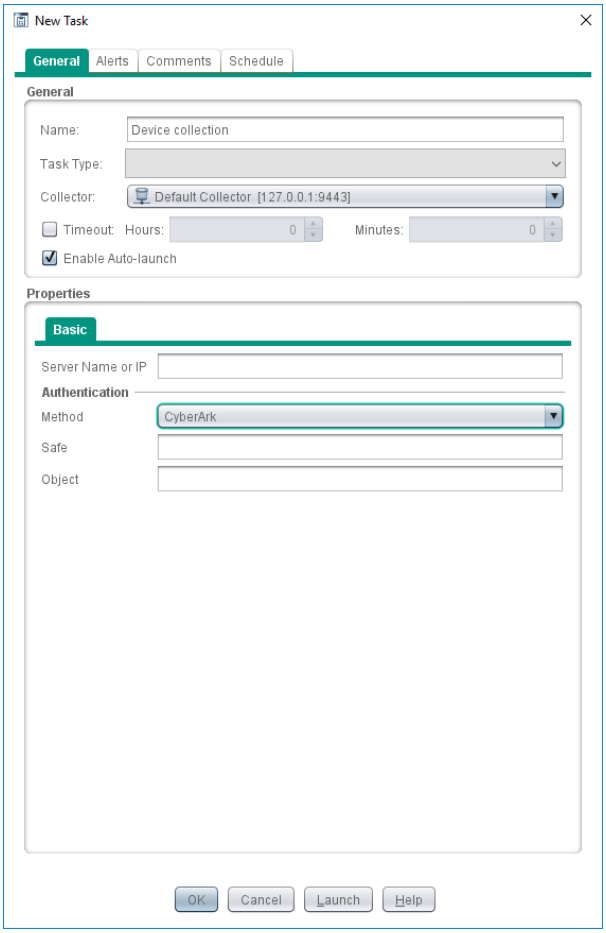
3. Open the Operational Console.



4. Create a new task.



5. Enter the task and device details and click **OK**.



PARTNER CONTACT INFO

Business Contact	Name	David Boardman
	Email	David.Boardman@skyboxsecurity.com
	Tel	805-452-9894
Technical Contact	Name	
	Email	
	Tel	
Support Contact	Name	
	Email	support@skyboxsecurity.com
	Tel	