CYBERARK SECRETS MANAGER

(Agentless Central Credential Provider CCP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Indeni

Website: www.indeni.com

Name of Product: Indeni

Version: 7.1

Date: 3 March 2021

INDENI SOLUTION OVERVIEW

The Indeni product is a Security Infrastructure Automation (SIA) Platform designed to auto-triage and identify infrastructure-related issues with firewalls and other security solutions for the Data Center.

Automation platform components:

- Indeni Server
- Indeni Insight
- Indeni Automation Elements
- Indeni Collector

The current release code for Indeni is v7.X (7.0.2 Release at the time of this publish).

KEY BENEFITS

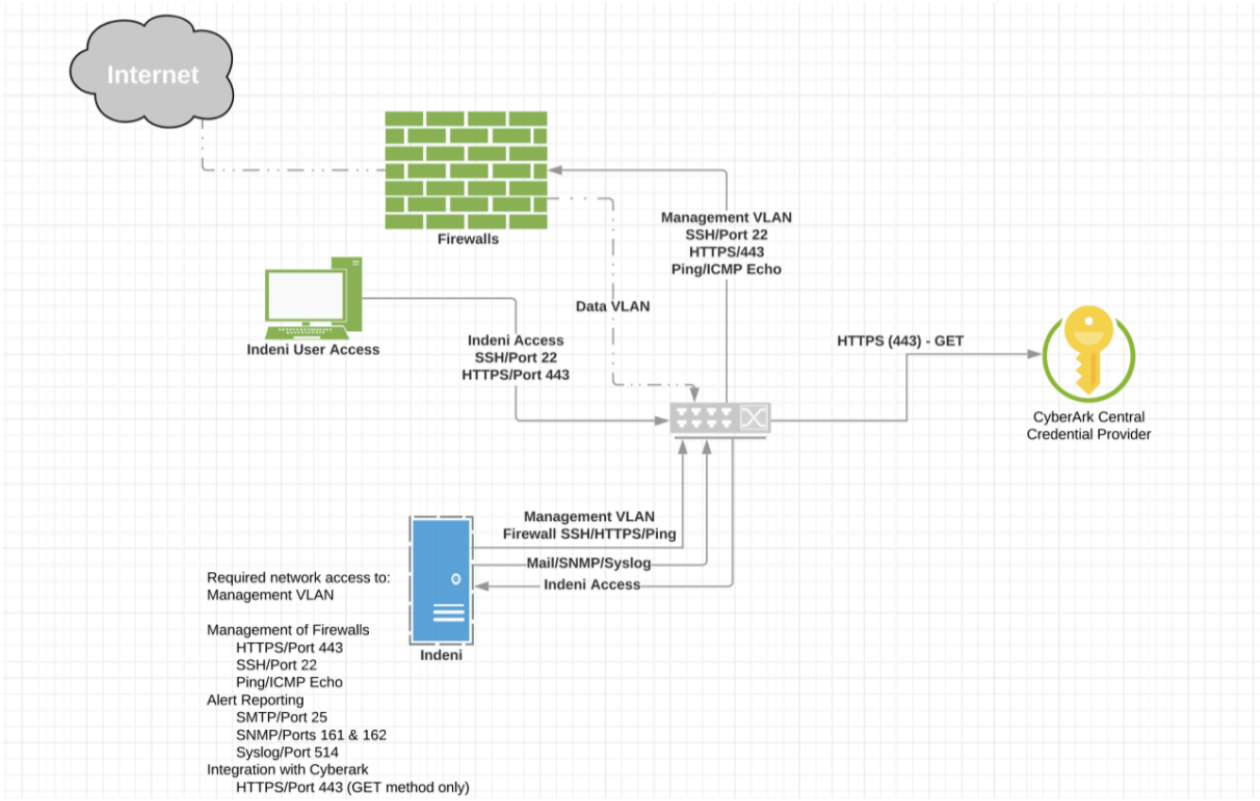
Benefits of Indeni:

- Real-time analysis of configuration drifts
- Best practice assessments
- Crowdsourcing of tribal operational knowledge of Data Center Security products (Firewalls, Proxies, WAF, Etc.)

Benefits of integrating Indeni with CyberArk Secrets Manager:

- Will allow customers to reduce their points of vulnerability by removing static service accounts for Indeni and using CyberArk Secrets Manager to use ephemeral service accounts.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER INTEGRATION

AAM integration is direct with the Indeni server (interacting with Indeni's Credential Database API). A regular call to the Central Credential Provider is made from the Indeni service every minute for state changes.

CREDENTIAL RETRIEVAL

Every minute, Indeni will poll the Central Credential Provider to capture the credentials associated with the target objects.

- If the password has been modified in the Vault, Indeni will reflect the changes locally in its credential DB.

These credentials are critical to Indeni as all Indeni's interactions with the target devices are through SSH or HTTPS

SECRETS MANAGER INSTALLATION

Refer to the "Credential Provider Implementation Guide" for CyberArk Agentless installation and configuration.

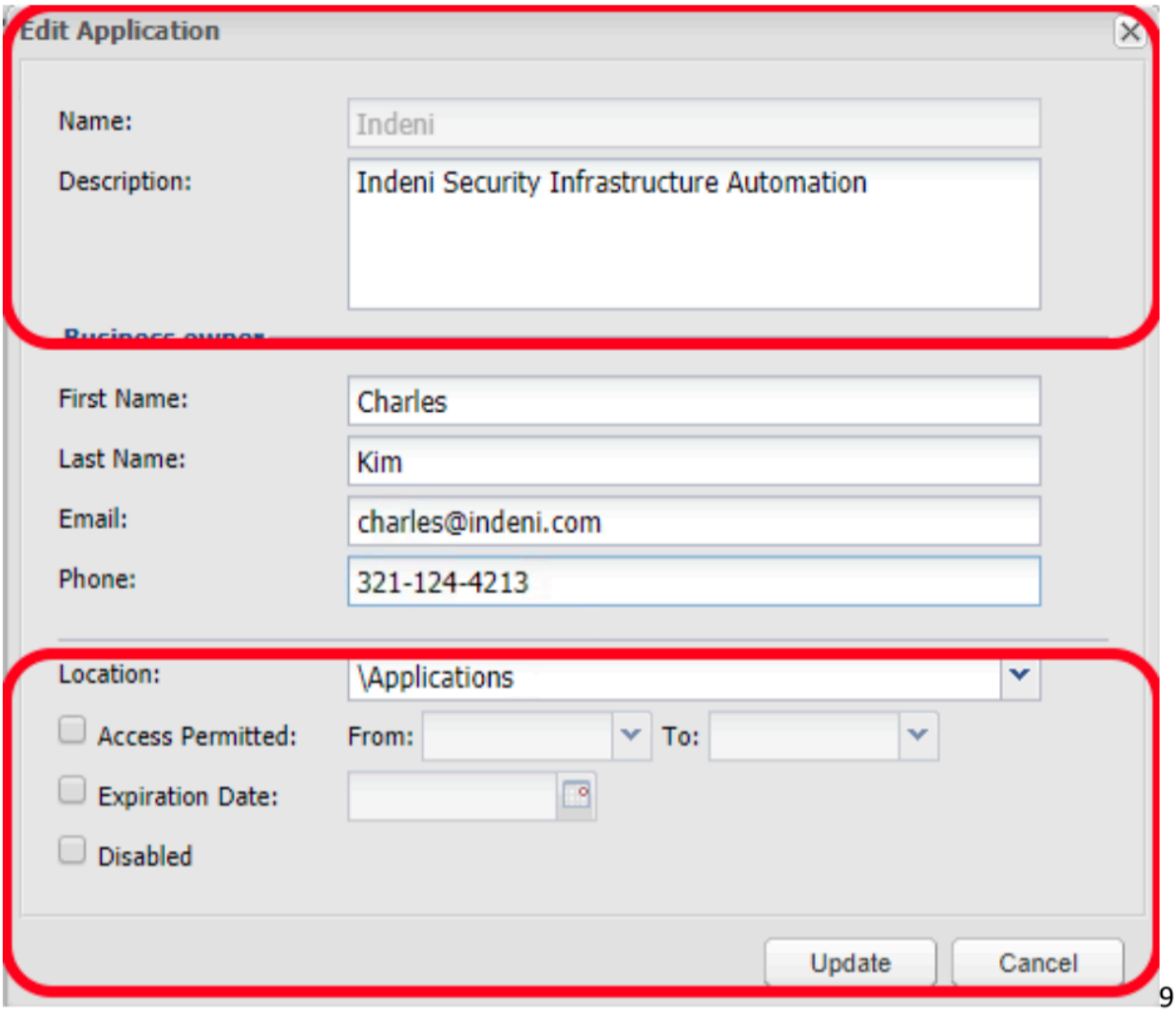
SECRETS MANAGER CONFIGURATION

The following sections provide details on Indeni 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.

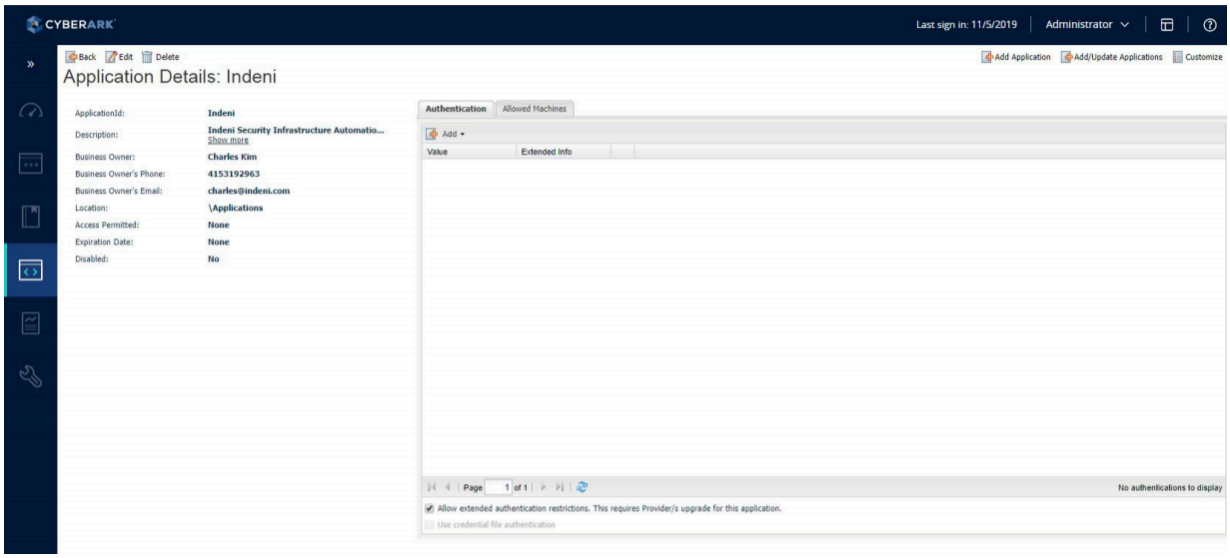


9

- ☐ Specify the following information:
  - In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: Indeni

- 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.



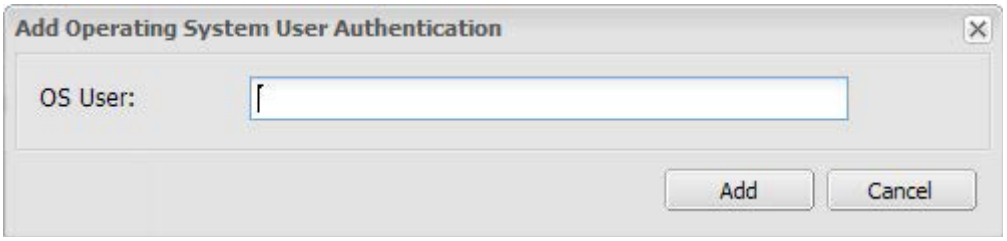
☐ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.

☐ Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password.

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

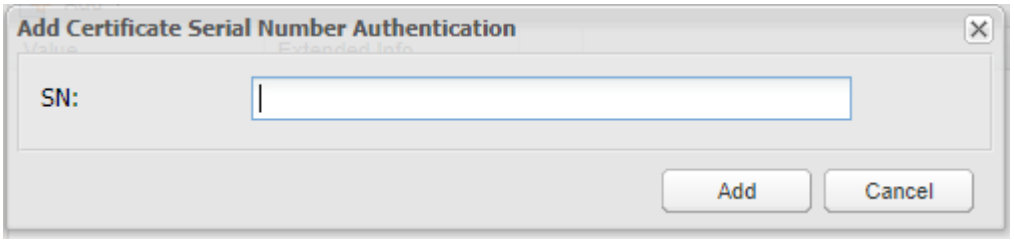
☐ Select the authentication characteristic to specify.

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



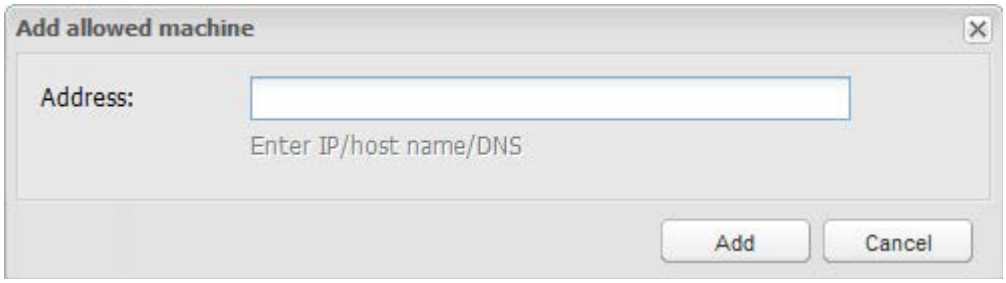
☐ Specify the name of the OS user who will run the application, then click **Add. T**he OS user is listed in the Authentication tab.

☐ Specify the Certificate Serial Number.



☐ Specify the application's Allowed Machines. This information enables Secrets Manager 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.

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.**

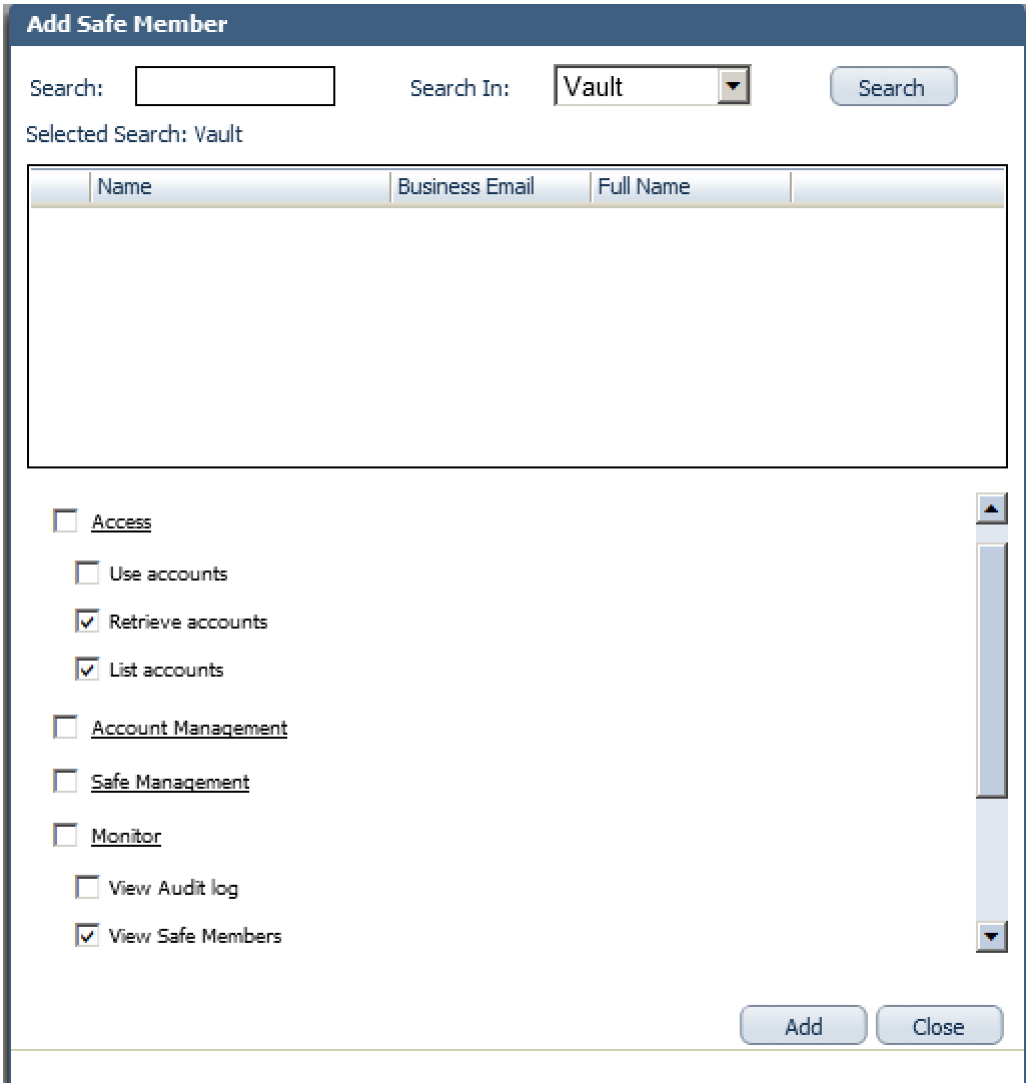
Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

Add the provider user (where the Central Credential Provider is installed) 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:

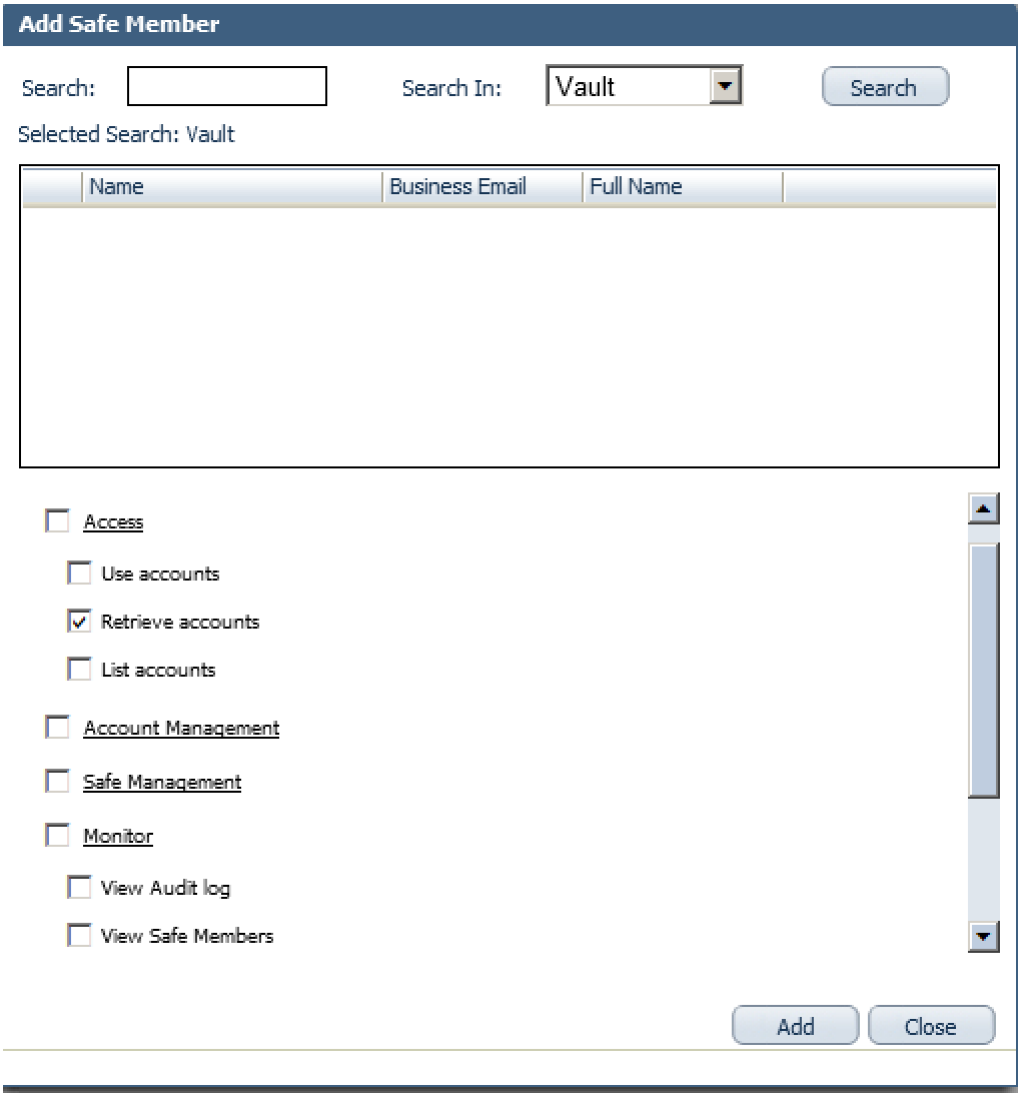
- List accounts
- Retrieve accounts
- View Safe Members

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.**

INDENI INSTALLATION & INTEGRATION CONFIGURATION

Refer to Indeni installation guide for Indeni installation.

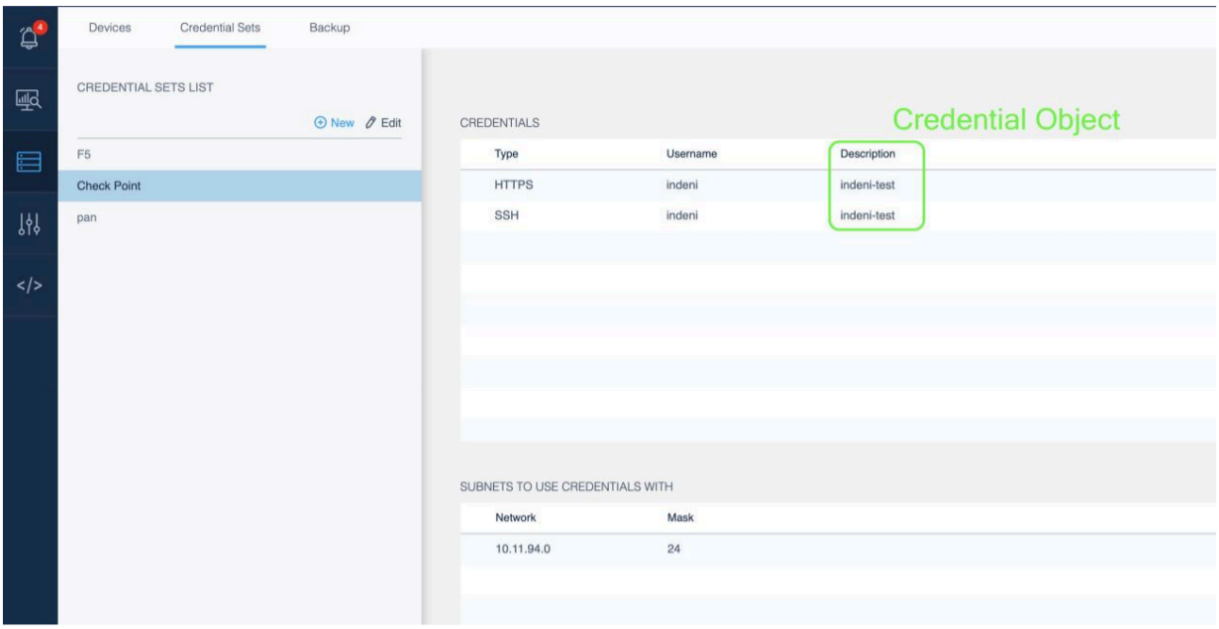
Requirements:

Indeni requires the following before proceeding with configuration:

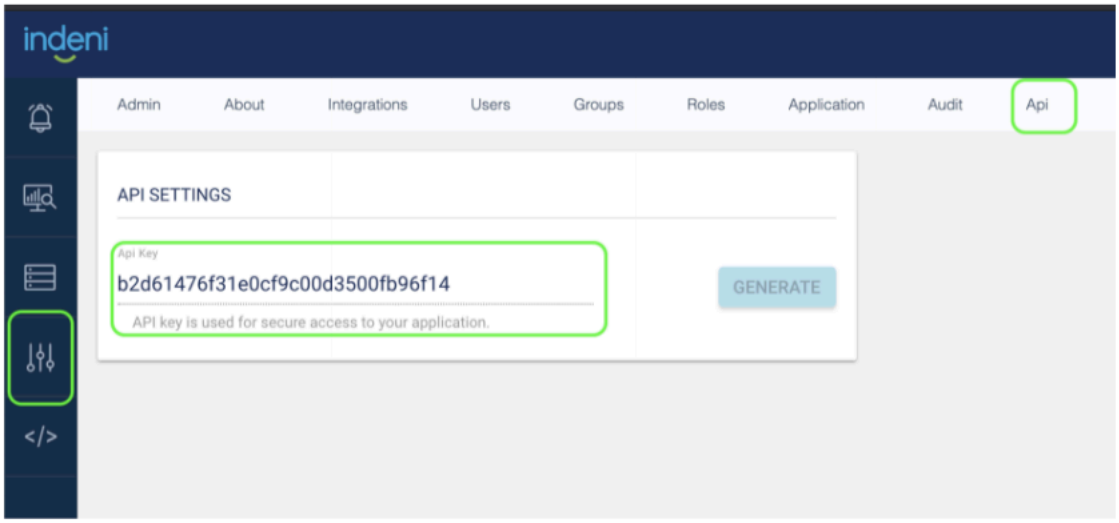
- User must have an available domain account which can be managed by CyberArk. All devices monitored by Indeni must connect to an AD through RADIUS. **PLEASE NOTE:** This mechanism will not be supported by F5 in 7.1. This integration may not suit your current deployment and you should contact your Indeni SE for further assistance.
- Domain Account must be configured as a Dual Account Object in CyberArk. The following link includes instructions to setup Dual Accounts: https://docs.cyberark.com/Product-Doc/OnlineHelp/AAM CP/Latest/en/Content/CP%20and%20ASCP/cv_Automatic_dual_account.htm?Highlight=dual%20accounts
- Indeni must have an AppID with necessary rights to the Safe where the Account Objects are stored.
- If User has a particular client certificate that should be used to authorize with Credential Provider, please have PEM certificate with both public/private key prepared. It should be transferred to the Indeni instance under the directory **/usr/share/indeni-services/bd-integrations/certs/**

Instructions:

1. Indeni does not support mixed use of credentials managed by CyberArk and self-managed credentials. Upon integrating with CyberArk, the customer must exclusively rely on CyberArk's Central Credential Provider to manage the credentials used for monitoring devices.
2. To properly configure Indeni with CyberArk, the end user must input the Cyberark Safe, Application ID, and corresponding Object Name for each credential Indeni will be synchronizing with.
3. Indeni strongly recommends that all accounts are under the same schedule for password rotation. This makes the integration easier by only requiring synchronization with one credential object. Otherwise, you will need to configure Indeni now with multiple credential sets.
4. The following instructions describes how to implement the integration with Central Credential Provider properly:
    a. Log into the **Indeni UI**:

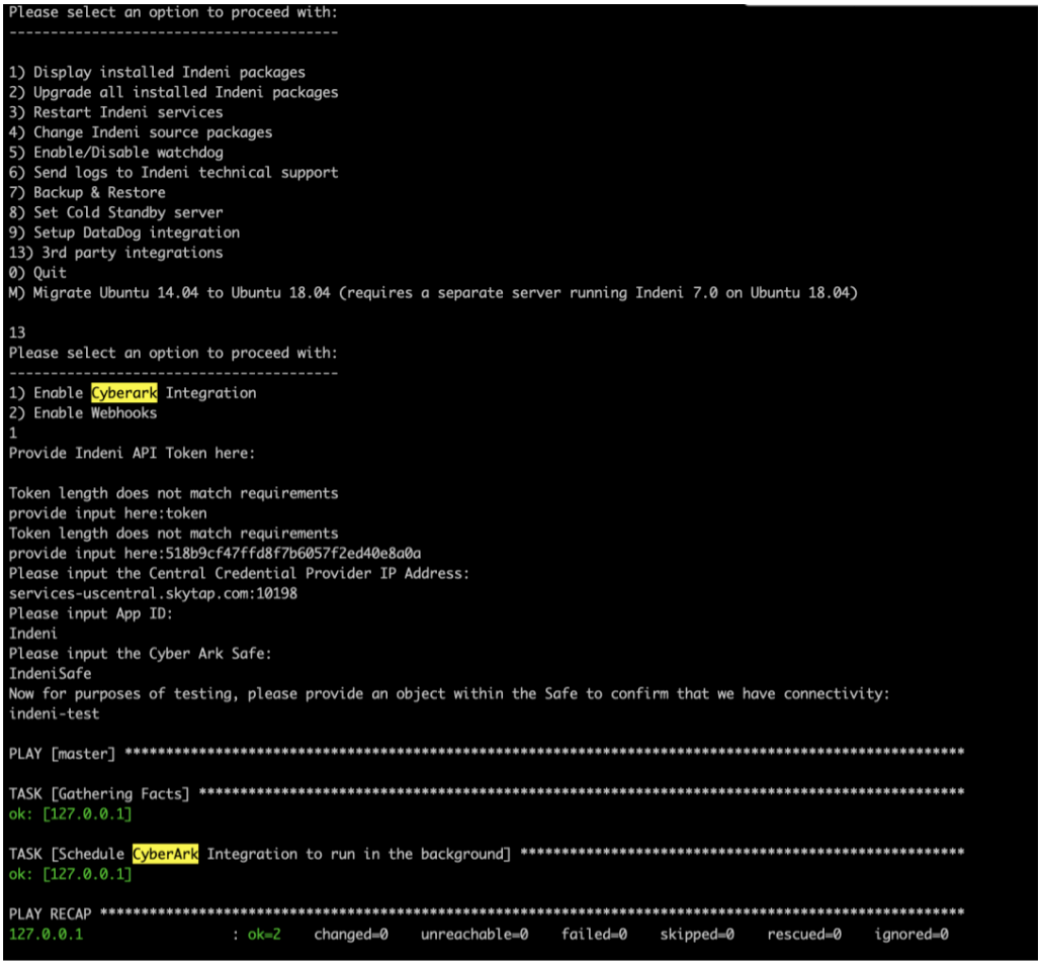


b. The user must create the correct credentials sets. This requires that the user maps the Credential Object to the Description Field found on Indeni.
    i. **Please note:** Indeni synchronizes with credentials stored in the CyberArk Vault at the Object level. That means that only specific objects will be synchronized based on how the credential sets are designed in Indeni. It's crucial to note that the credential set configurations may need to be different from previous deployment. For example, if the environment has 40 firewalls configured to rotate passwords at different points in time, you will want a separate credential for each unique CyberArk Object configuration.
c. End user must generate an API key (which can only be done with an account that has administrative privileges of Indeni):



d. Once the credential sets are mapped to the respective CyberArk objects and the API key is obtained, the user must login to the SSH terminal and must access imanage by typing "imanage".
e. Under imanage, type the respective number for the option "3rd party integrations". Follow the instructions provided in the terminal.
    i. You will need the following:
        - Indeni API key
        - Central Credential Provider IP address (custom ports are supported with the following syntax: **<ip-address>:<port number>**)
        - CyberArk Safe
        - CyberArk App ID
        - Vault Object Name
        - You will also be asked to provide a certificate - if needed, please specify the PEM file name under the directory **/usr/share/indeni-services/bd-integrations/certs/**

Once this is successful, you are now fully integrated with CyberArk. Example of interaction can be found here:


Please select an option to proceed with:
1) Display installed Indeni packages
2) Upgrade all installed Indeni packages
3) Restart Indeni services
4) Change Indeni source packages
5) Enable/Disable watchdog
6) Send logs to Indeni technical support
7) Backup & Restore
8) Set Cold Standby server
9) Setup DataDog integration
13) 3rd party integrations
0) Quit
M) Migrate Ubuntu 14.04 to Ubuntu 18.04 (requires a separate server running Indeni 7.0 on Ubuntu 18.04)
13
Please select an option to proceed with:
1) Enable Cyberark Integration
2) Enable Webhooks
1
Provide Indeni API Token here:
Token length does not match requirements
provide input here:token
Token length does not match requirements
provide input here:518b9cf47ffd8f7b6057f2ed40e8a0a
Please input the Central Credential Provider IP Address:
services-uscentral.skytap.com:10198
Please input App ID:
Indeni
Please input the Cyber Ark Safe:
IndeniSafe
Now for purposes of testing, please provide an object within the Safe to confirm that we have connectivity:
indeni-test
PLAY [master]
TASK [Gathering Facts]
ok: [127.0.0.1]
TASK [Schedule CyberArk Integration to run in the background]
ok: [127.0.0.1]
PLAY RECAP
127.0.0.1 : ok=2 changed=0 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0

PARTNER CONTACT INFO

Business Contact	Name	Ulrica de-fort Menares
	Email	ulrica@indeni.com
	Tel	
Technical Contact	Name	Charles Kim
	Email	charles@indeni.com
	Tel	415-319-2963
Support Contact	Name	
	Email	support@indeni.com
	Tel	