



KAPSTONE GATEWAY - CYBERARK IDENTITY INTEGRATION GUIDE

Name of Company: Kapstone Technologies LLC

Website: <http://www.kapstonellc.com/>

Name of Product: Kapstone Provisioning Gateway

Version: v1

Date: July 24, 2022

PARTNER SOLUTION OVERVIEW

About Kapstone Technologies

With over 20+ years of experience in the IAM industry, Kapstone is a leading provider of Identity & Access management solutions. With a focus on simplified user experience and business enablement through security, Kapstone has successfully architected and deployed Identity and access management solutions for various customers in North America.

Through Kapstone Provisioning Gateway, we continue to demonstrate our thought leadership in the Identity & Access Management market. We understand how multiple sources of truth, various Identity governance tools and multi-cloud environments are a reality for today's enterprises. In this complex identity eco-system, Kapstone Gateway acts as an abstraction layer which seamlessly integrates with multiple cloud and on-premise applications. Also Kapstone Gateway is capable of integration with multiple Identity providers (CyberArk, Sailpoint, Azure, Oracle etc.) and therefore helps organizations significantly consolidate their application integration efforts.

Kapstone Provisioning Gateway and CyberArk Identity

Kapstone and CyberArk have partnered to provide their customers a comprehensive, agile and scalable Identity Lifecycle management solution. CyberArk Identity customers can now onboard 100's of applications to the CyberArk Identity platform by leveraging Kapstone Provisioning Gateway. Identity lifecycle activities like user on-boarding, off-boarding, transfer and role change will be achieved through this joint integration. This solution enables our customers to rapidly achieve compliance and Identity automation objectives. Through this solution, we are providing pre-built connectors for various types of integrations (DB, LDAP, Unix, Web Services etc.). While allowing customers to rapidly onboard cloud and on-premise applications, we are also ensuring that there is no maintenance overhead on the customers with this solution. With Kapstone Gateway being offered as a SaaS service, it's a simple plug and play to enable increased integrations.

Kapstone Provisioning Gateway seamlessly integrates into CyberArk Identity through SCIM 2.0, providing deep provisioning capabilities without any disruption to your CyberArk identity deployment. Kapstone Provisioning Gateway is a cloud-native solution that requires only a few minor configuration settings within CyberArk, and does not require any coding. To get started, simply configure Kapstone Provisioning Gateway as a SAML 2.0 integration in your CyberArk Identity environment.

When an end-user requests access(provision/de-provision/role assignment) to an enterprise application through CyberArk Identity, the CyberArk Identity calls Kapstone Provisioning Gateway, which in turn connects with the application to perform the desired function.

KEY BENEFITS

Key Business Benefits of Kapstone Provisioning Gateway:

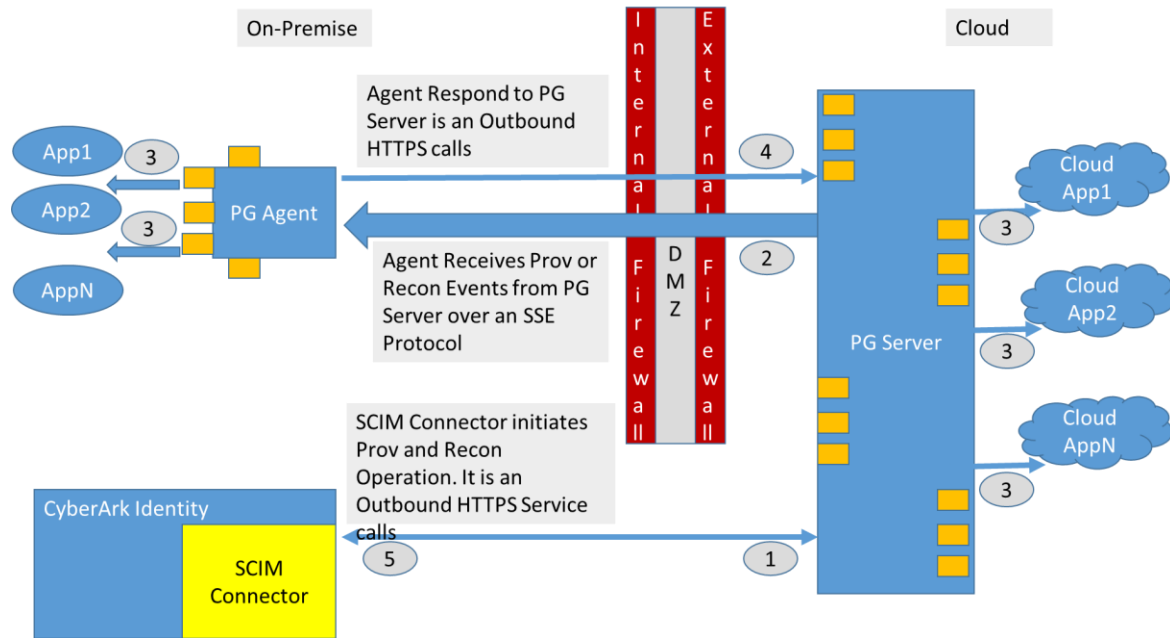
- **Rapid Application onboarding:** Integrate Applications faster by reducing application onboarding time by as much as 70% compared to traditional application onboarding methods

- **ZERO Maintenance:** As a SaaS solution, the customer has ZERO maintenance requirements. Additionally, Kapstone can also onboard and maintain applications for the customer
- **Delegation:** Promote a simplified application onboarding and maintenance process by delegating Application administration to App/IT owners, while centralized security is managed by IAM team(s)
- **Faster Product Upgrades:** Version upgrade/patching of IGA will not cause any issues to application integration
- **Interoperability:** Kapstone Gateway promotes interoperability by seamlessly integrating with all SCIM 2.0 enabled platforms. This feature drastically reduces your application migration costs.

Key Technical Features of Kapstone Gateway:

- Simplified excel driven **application enrichment:** Application owners can easily maintain their application specific attributes. This solution provides app/IT owners an interface where application details like description, entitlement tags, risk levels, entitlement description etc. can be easily maintained.
- **Logical Application** connector: In the case of multiple databases as well as multiple AD domains, the administrators are able to define a single connector that provides capability for multi-pronged back end integration. This greatly simplifies application management and helps business users easily understand and request business applications.
- **Ticketing System Integration:** The solution provides Intelligent, single click integration with Ticketing system for disconnected apps. The system will automatically create tickets in case of Identity related access request to disconnected applications.
- **Orphan account detection:** This integration also provides enhanced compliance capabilities by detecting and reporting on orphan application accounts.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



CYBERARK IDENTITY INTEGRATION

Kapstone Gateway acts as a user lifecycle management platform that enables Cyberark Identity to connect with 100's of applications. Through Kapstone Provisioning Gateway, Cyberark Identity customers can connect to 100's of applications to drive target/downstream user lifecycle management. Activities like user creation, providing access to applications, moving user access from one application to another and terminating/disabling user access can be automated through Cyberark.

Kapstone Gateway acts as an integration layer that is controlled through Cyberark Identity. Based on user's attributes, the Cyberark Identity system applies rules and access policies to determine which user should have access to which applications, and the level of access. Cyberark Identity then instructs Kapstone Gateway to perform the applicable user lifecycle activities.

All communication between Cyberark Identity and Kapstone Provisioning Gateway are secure HTTPS calls. Provisioning Gateway connects with cloud and on-premise applications with equal ease. All integration from Kapstone Provisioning Gateway to on-premise applications happens over HTTPS calls.

KAPSTONE PROVISIONING GATEWAY: LIST OF CONNECTORS

Trusted Connectors

- PeopleSoft
- Workday
- Oracle EBS
- Flat file / CSV
- Database – Oracle, MySQL, MSSQL
- Oracle HCM

- Azure AD
- SCIM Compliant Source(s)

Target Connectors

- Database User Management Collector (Single Connector for any number of DB instances) - Oracle, MySQL, MSSQL
- Database Application Connector - Oracle, MySQL, MSSQL
- LDAP
- Unix/Linux Server
- RSA IGL
- Active Directory Logical Application Connector
- Active Directory Multi Domain Connector
- Oracle E-Business Suite
- PeopleSoft User Management
- Azure Active Directory
- Office 365
- Sailpoint Identity Now
- Sailpoint IIQ
- AWS (Amazon Web Services)
- OCI (Oracle Cloud Infrastructure)
- OKTA
- Google Cloud Platform
- Box
- ServiceNow
- BMC Remedy
- GitLab
- Oracle Identity Manager (OIM)
- Oracle IDCS

INTRODUCTION

As outlined above, Kapstone Provisioning Gateway supports integration with 100's of applications. In order to demonstrate the ease of integration, we are going to integrate Kapstone Provisioning Gateway with PeopleSoft for user management. The integration with PeopleSoft (for user management/target application) is achieved through a simple 2 step process. The same process will be used for integration with any other target application.

- **Step 1:** Set up PeopleSoft (target application) in Kapstone Provisioning Gateway in order to enable user lifecycle management operations
- **Step 2:** Register Kapstone Provisioning Gateway as an integration agent with your CyberArk Identity environment.

PREREQUISITES

Ensure that you have a CyberArk Identity account with system admin privileges to:

- Create/Configure tenant.
- Create/Configure SAML 2.0 based application integration

KAPSTONE GATEWAY SERVER CONFIGURATION

Information provided by the Kapstone Gateway Server Admin Team:

Kapstone Gateway Admin Portal Login Credentials

- UserName
- Password

Kapstone Gateway User(App Owner) Portal Login Credentials

- UserName
- Password

Kapstone Gateway Server endpoint URLs:

- Portal Access : `https://<ManagedServer:port>/kpgateway/<TENANTID>`
- Issuer endpoint of an application :
`https://<ManagedServer:port>/scim/v2/<TENANTID>/<APPID>`
- Token endpoint of an application :
`https://<ManagedServer:port>/registeredapp/<APPID>/oauth2/v1/<TENANTID>/token`

SCIM Credentials of an Application:

- Client ID : [From Kapstone Gateway Server Admin Console]
- Client Secret : [From Kapstone Gateway Server Admin Console]
- Bearer Token : [From Kapstone Gateway Server Admin Console]
- Refresh Token : [From Kapstone Gateway Server Admin Console]

SCIM API endpoints :

- <https://<ManagedServer:port>/scim/v2/<TENANTID>/<APPID>/Users>
- <https://<ManagedServer:port>/scim/v2/<TENANTID>/<APPID>/Groups>

Step 1: Sign in as an administrator to Kapstone Provisioning Gateway (to register PeopleSoft application)

1a) Register PeopleSoft Application in Gateway

The screenshot shows the Kapstone Provisioning Gateway interface. At the top, there's a header with the Kapstone logo and a user profile 'xelsysadm'. Below the header, there's a navigation bar with tabs: Provisioning, Entitlements, Group Management, and Single Sign-on. The main content area is titled 'Application' and displays details for 'PSFTInstanceDemo'. The details include App Code (201CNF7H), App Name (PSFTInstanceDemo), App Description (Peoplesoft Instance for Demo), and Owner Group (RPONTING). Below this, there's a table with columns: APPLICATION NAME, TYPE, API TOKEN, APP URL, ACTIVE, and ACTIONS. The table shows one entry for 'PSFTInstanceDemo' with type 'PeopleSoftUM'. There are buttons for 'SHOW TOKEN' and 'SHOW URL'. The 'ACTIVE' status is toggled on. There are also icons for edit, refresh, and settings. A pagination bar at the bottom shows '1' of 1 items.

APPLICATION NAME	TYPE	API TOKEN	APP URL	ACTIVE	ACTIONS
PSFTInstanceDemo	PeopleSoftUM	SHOW TOKEN	SHOW URL	☒	Edit Refresh Settings

1b) Provide Peoplesoft Connection and Listener service details

The screenshot shows the Kapstone Provisioning Gateway interface with the application details for 'PSFTInstanceDemo'. The details are organized into two columns: Application Details and OAuth Details. The Application Details include fields for Create User Operation Method, Create Group Operation Method, Sender Node, Update User Operation Method, Default Role, Service URL, Get All Users Operation Method, Get All Groups Operation Method, Default Navigator Permission, Receiver Node, Delete Group Operation Method, Default Process Profile Permission, Get User Operation Method, Default Primary Permission, Host, and Default Row Security Permission. The OAuth Details include fields for OAuth Type, Admin ID, and Client ID. The interface also shows a pagination bar at the bottom with '1' of 1 items.

APPLICATION NAME	TYPE	API TOKEN	APP URL	ACTIVE	ACTIONS
PSFTInstanceDemo	PeopleSoftUM	SHOW TOKEN	SHOW URL	☒	Edit Refresh Settings

Application Details

Create User Operation Method: CI_SCIM_USERS_CV1.V1

Create Group Operation Method: CI_SCIM_ROLES_CV1

Sender Node: PSFT_HR

Update User Operation Method: CI_SCIM_USERS_UD.V1.V1

Default Role: FORM_USER

Service URL: http://cloud.kapstonellc.com:8000/PSIGW/HttpListeningConnector

Get All Users Operation Method: CI_SCIM_USERS_FV1.V1

Get All Groups Operation Method: CI_SCIM_ROLES_FV1

Default Navigator Permission: HCSPNAVHP

Receiver Node: KP_TEST

Delete Group Operation Method: CI_SCIM_DEL_ROLE_UD.V1

Default Process Profile Permission: HCSPPRFL

Get User Operation Method: CI_SCIM_USERS_CV1.V1

Default Primary Permission: HCPPPSUSI

Host: cloud.kapstonellc.com

Default Row Security Permission: HCDPPSUSI

OAuth Details

OAuth Type: KPOAUTH

Admin ID: RPONTING

Client ID: r1d97csSq54vt1fr3swwh6pc5t5zin

Activate Windows
Go to Settings to activate Windows.

1c) Provide OAuth Details to connect to Peoplesoft via Gateway

APPLICATION NAME	TYPE	API TOKEN	APP URL	ACTIVE	ACTIONS
PSFTInstanceDemo	PeopleSoftUM	SHOW TOKEN	SHOW URL	☒	Edit Refresh Settings

Application Name :

Application Details

Application Type: PeopleSoftUM

Create User Operation Method: CI_SCIM_USERS_C.V1.V1

Create Group Operation Method: CI_SCIM_ROLES_C.V1

Sender Node: PSFT_HR

Update User Operation Method: CI_SCIM_USERS_UD.V1.V1

Default Role: FORM USER

OAuth Details

OAuth Type: KPOAUTH

Admin ID: RPONTING

Client ID: r1c197cs5q54vt1fr3swwh6pc5t5zin

[Show Admin password](#)

[Show Client Secret](#)

1d) Verify and copy connection URL for the PeopleSoft Application through Gateway.
Click on Show URL button and copy the URL –

https://aep.kapstonellc.com/scim/v2/KPINSTANCE/201CNF7H

[Copy](#)

ACTIVE ☒

PeopleSoftUM

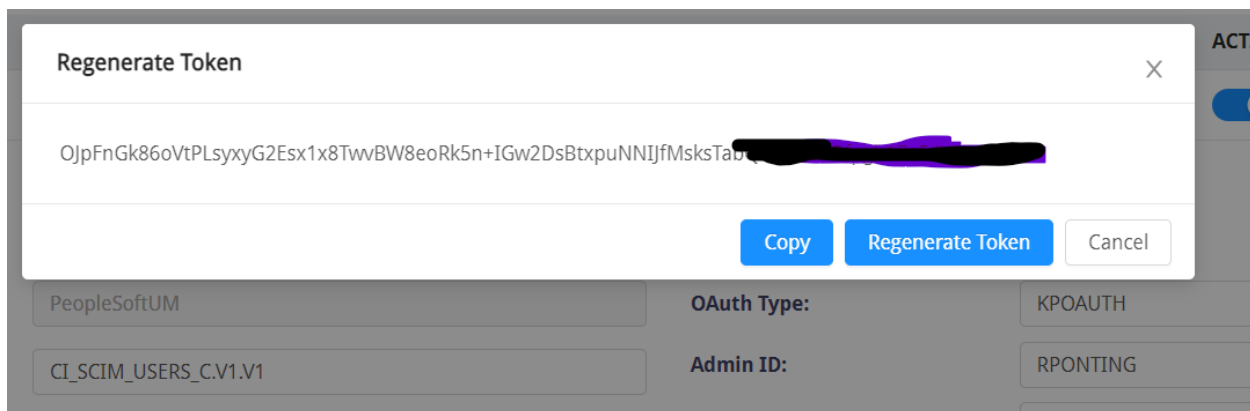
CI_SCIM_USERS_C.V1.V1

OAuth Details

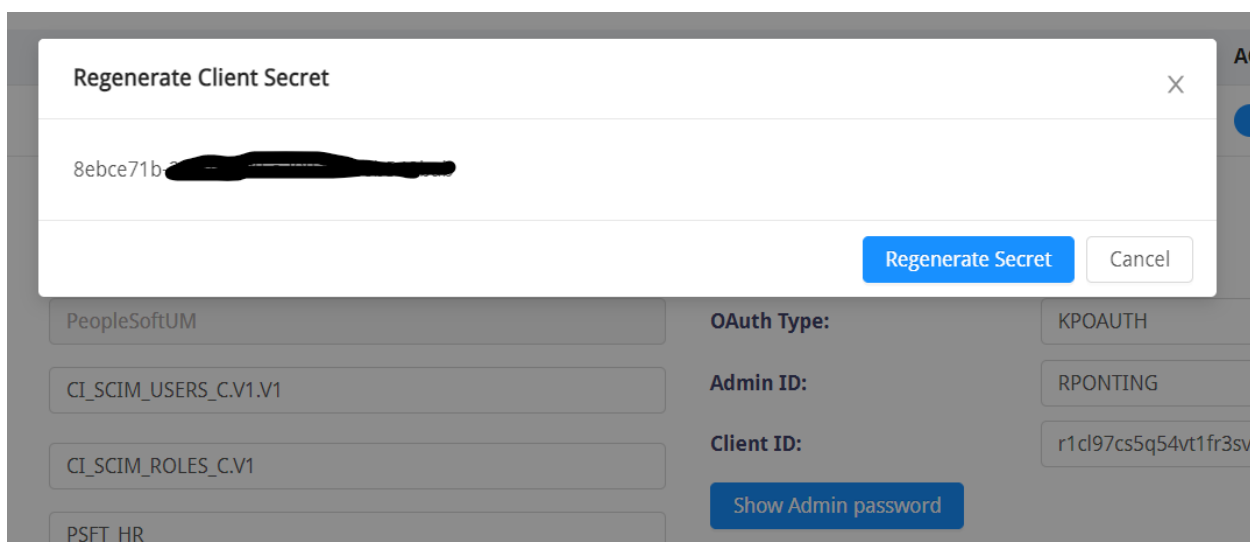
OAuth Type: KPOAUTH

Admin ID: RPONTING

1e) Click on Show Token to Copy the Bearer Token for the application



1f) Click on Show Client Secret Button to copy the Client Secret for the application



1g) Verify Schema Field Mappings: This is the mapping of Gateway Attributes and the Peoplesoft attributes for provisioning and Reconciliation operations.

Provisioning				Reconciliation	
Source Attribute	Target Attribute	Default Value	Action		
nickName	p_nickname				
emails.value[type:work]	p_email				
userName	p_username				
password	p_password				
enterpriseUser.manager.value	p_managerid				
id	id				

< 1 >

Save

Cancel

Add New Attribute

Mapping Type

Direct

Source Attribute [Help](#)

Target Attribute

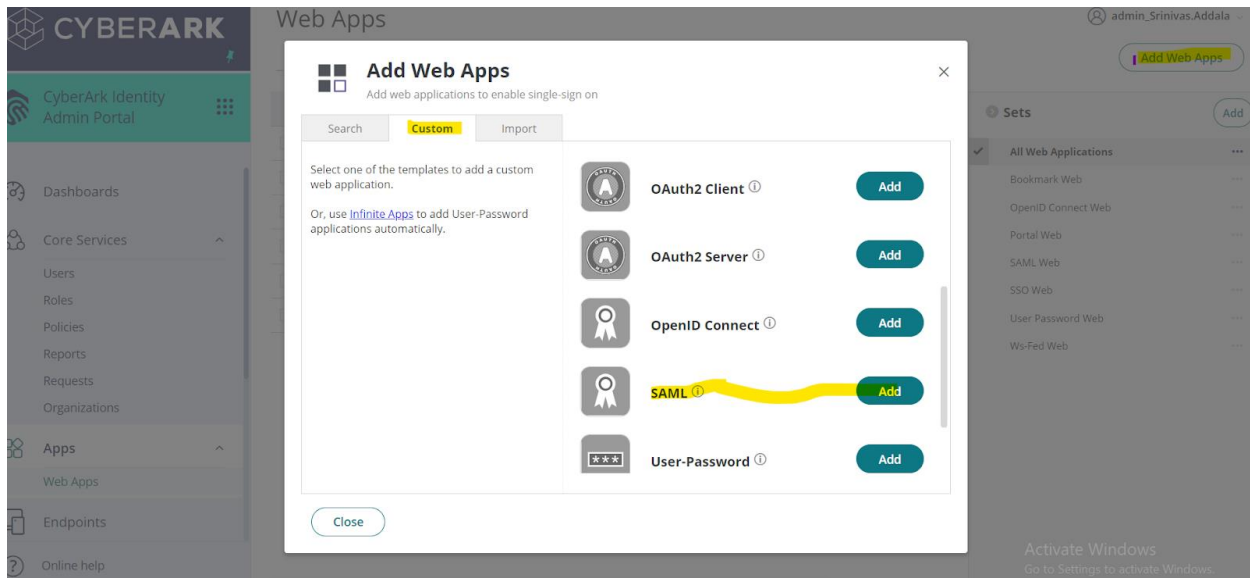
Default value (optional)

Add

Discard

Step 2: Registering Kapstone Provisioning Gateway with CyberArk Identity (to enable PeopleSoft Integration)

2a) Create a new Web Application in CyberArk, Add a new Custom SAML Template



SAML

Type: Web - SAML + Provisioning

Status: **Ready to Deploy**

[Application Configuration Help](#)

Actions ▾

Settings

- Trust
- SAML Response
- Permissions
- Policy
- Account Mapping
- Linked Applications
- Provisioning
- App Gateway
- Workflow
- Changelog

Settings

[Learn more](#)

Description

☐ Customize Name and Description for each language ①

Name *

PeopleSoft User Management

Description

This template enables you to provide single sign-on to a web application that uses SAML (Security Assertion Markup Language) for authentication.

Category *

SCIMGateway

Logo



[Browse](#)

Recommended image size is 100 x 100

Activate Windows

2b) Click on Provisioning Link and Enable provisioning -



PeopleSoft User Management

Type: Web - SAML + Provisioning

Status: Ready to Deploy

[Api](#)

Settings

Trust

SAML Response

Permissions

Policy

Account Mapping

Linked Applications

Provisioning

App Gateway

Workflow

Changelog

Provisioning

[Learn more](#)

☒ Enable provisioning for this application

Save

Cancel

Type: Web - SAML + Provisioning

Status: Ready to Deploy

Settings

Trust

SAML Response

Permissions

Policy

Account Mapping

Linked Applications

Provisioning

App Gateway

Workflow

Changelog

Provisioning

[Learn more](#)

- ☒ Enable provisioning for this application
☐ Preview Mode (changes will not be committed)
☒ Live Mode

SCIM Service URL *

Authorization Type ⓘ

- ☐ OAuth 2.0
☒ Authorization Header

Header Type

Bearer Token ▼

Bearer Token *

Verify

2c) Provide Details of the registered PeopleSoft application -
Copy and paste the SCIM Service URL and Bearer Token from the Gateway Server

Type: Web - SAML + Provisioning Status: **Ready to Deploy**

A

Settings

Trust

SAML Response

Permissions

Policy

Account Mapping

Linked Applications

Provisioning

App Gateway

Workflow

Changelog

Provisioning

[Learn more](#)

- ☒ Enable provisioning for this application
- ☐ Preview Mode (changes will not be committed)
- ☒ Live Mode

SCIM Service URL *

`https://aep.kapstonellc.com/scim/v2/KPINSTANCE/201CNF7H`

Authorization Type ⓘ

- ☐ OAuth 2.0
- ☒ Authorization Header

Header Type

Bearer Token

Bearer Token *

`OJpFnGk86oVtPLsyxyG2Esx1x8TtwvBW8eoRk5n+IGw2DsBtxpuNNIjfmMskstAbQtizUsUvOfj`

Verify

2d) Verify the configuration by Clicking the Verify Button and make sure that the status is Deployed.

Type: Web - SAML + Provisioning

Status: **Deployed**

Application

Settings

Trust

SAML Response

Permissions

Policy

Account Mapping

Linked Applications

Provisioning

App Gateway

Workflow

Changelog

Provisioning

[Learn more](#)

- ☒ Enable provisioning for this application
- ☐ Preview Mode (changes will not be committed)
- ☒ Live Mode

SCIM Service URL *

`https://aep.kapstonellc.com/scim/v2/KPINSTANCE/201CNF7H`

Authorization Type ⓘ

- ☐ OAuth 2.0
- ☒ Authorization Header

Header Type

Bearer Token

Bearer Token *

`OJpFnGk86oVtPLsyxyG2Esx1x8TtwvBW8eoRk5n+IGw2DsBtxpuNNIjfmMskstAbQtizUsUvOfj`

Verify

Once the above configuration is finished, we are now good to initiate Outbound provisioning from CyberArk for the PeopleSoft application through Kapstone Gateway.

PARTNER CONTACT INFO

Business Contact	Name	Saurabh Sharma
	Email	Saurabh.Sharma@kapstonelc.com
	Tel	+1-908-787-2303