



CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Tata Consultancy Services

Website: www.tcs.com

Product Website: www.digitate.com

Name of Product: ignio™

Version: 2.x (Cheetah)

Date: 8 August 2019 (25 November 2020)

IGNIO™ OVERVIEW

ignio™ is an enterprise cognitive automation solution for IT Operations. ignio™ brings unprecedented levels of contextual intelligence to transforming enterprises. ignio™ binds together disparate yet interconnected business applications and their underlying infrastructures to perform actions autonomously and drive smart decision-making. The key features and functionalities of ignio™ are noted below.

Describe partner product, providing context of usage and integration.

Version: 2.x (Cheetah)

LEARN

Understanding business context is critical for IT to deliver business value. ignio™ combines pre-built knowledge of IT technology and infrastructure with self-learning of your unique business context.

ignio™ also captures tacit knowledge that has always been difficult to document. This helps preserve critical knowledge and details that are essential to business operation.

Blueprint: ignio™ begins by identifying the various applications and infrastructure components within your enterprise environment. The resulting 360-degree view, which is updated automatically when changes are made, allows IT to operate with the most up-to-date intelligence.

Normal Behavior Characterization: Once ignio™ has built an initial blueprint of the enterprise environment, it creates a baseline temporal-spatial view of the various infrastructure resources and components in their normal state of behavior. This makes it possible to monitor the IT environment more effectively through a multi-dimensional view of health of the underlying systems.

Explicit Training: The ignio™ platform also allows users to create specific knowledge that helps to enhance its learning capability to an even greater degree.

Observational Self-Learning: The ignio™ self-learning engine starts operating at deployment, observing the systems in the environment and learning how they work together

Enterprise Systems Integration: ignio™ integrates with existing enterprise infrastructure and applications. This ensures that existing IT investments can run normally and do not need to be replaced or modified.

RESOLVE

Once ignio™ gains working knowledge of your business and IT environment, it derives insights from multiple data sources to facilitate better decision-making.

Unlike traditional deterministic automation that requires explicit preprogramming and scripting, ignio™ constructs an end-to-end automation workflow by assembling a series of actions from its inventory of skills.

Intelligent Root Cause Analysis: When an IT incident occurs, ignio™ automatically conducts a root cause analysis to identify problem areas. ignio™ troubleshoots problems from the top by comparing the behaviors of all components against historical norms to check whether they are behaving normally. ignio™ repeats this process until it identifies the offending nodes.

Aggregation, Correlation, and Prioritization of Events and Alerts: IT teams are constantly inundated with alerts due to static thresholds set in various monitoring systems. ignio™ suppresses unnecessary and redundant alerts based on an understanding of how alerts from different monitoring systems are associated with the same root cause. At the same time, ignio™ prioritizes alerts with an immediate negative impact on the business, allowing IT teams to effectively focus their attention where it is most needed.

Autonomous Action for Execution and Validation: Automation scripts often fail when faced with an unknown state, requiring IT to spend countless hours troubleshooting the automation mechanism itself. ignio™ can function autonomously to fix incidents without the need for explicit instructions, avoiding these time-consuming failures.

Resource Provisioning and Patch Management: ignio™ automates installation, provisioning, patching, configuration management, and data migration across the IT infrastructure. The solution provisions resources to ensure that the environment has the needed capacity as well as making appropriate configuration changes to optimize system performance.

Real-Time Health Diagnostics: ignio™ performs real-time health checks against applications and infrastructure components. This includes verifying whether applications and underlying infrastructure are operating normally, as well as testing applications to ensure that their basic capabilities are accessible.

PREVENT

Early identification of outages enables IT to take appropriate remediation actions before an outage occurs. ignio™ simulates complex scenarios so that businesses can analyze and model potential impacts.

Future State and What-If Simulations: Based on data that ignio™ captures over time, IT can run simulations of their environment for a selected future date. They can also introduce complex variables to simulate — and assess the impact of — various business and technology scenarios.

KEY BENEFITS

Key benefits of ignio™:

- Intelligently automates complete IT workflow and autonomously handles the majority of IT tasks, such as release and environment management, ready-for-business functional checks, application and infrastructure health diagnostics, compliance audit for CIS, root cause analysis, and self-healing
- Mitigates risks and predicts outages by achieving very high levels of accuracy in predicting future impacts

- Comes bundled with prebuilt knowledge of various IT technologies and understands organization's business context to resolve incidents, automate tasks, and provide insights
- Supports many different ways of learning, such as connected intelligence, observational learning, crowd sourcing, and machine learning techniques
- Provides a 360-degree view of enterprises' technology, which helps to understand dependencies across business functions and technology elements
- Enables digital experience by creating a context-aware and personalized command center

Integrating ignio™, the world's leading cognitive automation platform, with CyberArk Secrets Manager, a class-leading Secrets Manager provides users with:

- Unified credential management, leading to enhanced security and integrity
- Enhanced auditing capability for credential management
- Reduction in manual steps required for credential management
- Scalable and automated credential management for large infrastructure
- Enhanced security, due to seamless integration of credential management rotation policies

Off-the-shelf integration of CyberArk Secrets Manager with ignio™ leads to reduced cycle time for deployment.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

In a typical infrastructure, support operations, requests, and incidents are reported to the service desk (or) logged in IT service management tools like Remedy or ServiceNow. Based on the availability of ignio™ capabilities and knowledge, these requests are assigned to ignio™ for resolution or fulfillment by the IT service management tool. ignio™ performs required action on the target systems to resolve incidents. To perform operations on the target systems, ignio™ uses the credentials of said target systems. The required credentials are fetched from CyberArk to perform necessary operations.

The overview diagram of ignio™ and CyberArk integration is depicted in Figure 1 and detailed step-by-step operations of ignio™ are outlined below.



Figure 1: Overview diagram of ignio™ and CyberArk integration

SECRETS MANAGER INTEGRATION

1. ignio™ receives a service request from IT Service management tool such as ServiceNow, Remedy, to perform the operations. Based on the capability of ignio™, IT service management tool assigns the ticket to ignio™.
2. ignio™ identifies the hostname based on the service request details. ignio™ requests CyberArk the credential details (user name and password) of the target using **Password SDK API**. ignio™ sends registered appID, Safe ID and Object ID of hostname to CyberArk.
3. ignio™ receives credentials for the requested host.
Note: ignio™ securely manages the credentials received from CyberArk. It does not store/cache the credentials received from CyberArk
4. ignio™ connects to the host (windows, Linux, network devices) based on the credentials received from CyberArk and performs the operations as per service request. ignio™ connects to windows, Linux, network devices using PowerShell, SSH, SNMP respectively.

Typical installation of ignio™ requires up to 8VMs. Secrets Manager will be installed on one of the VMs where the ignio Proxy-Agent component of ignio™ is deployed. In the case of high availability deployment, Secrets Manager agent will be installed on each instance of ignio Proxy-Agent.

Typical customer installations have 15k to 20k resource units being managed by ignio™. However, ignio™ has been shown to seamlessly scale to any number of resource units through horizontal and vertical scaling mechanisms.

ignio™ and CyberArk interaction

CyberArk provides the following two solutions to manage credentials.

- Credential provider (agent based)
- Central credential provider (agentless)

ignio™ uses credential provider (agent based) for its integration with CyberArk. The credential provider agent is copied in the ignio Proxy-Agent component of ignio™ as shown in Figure 2.

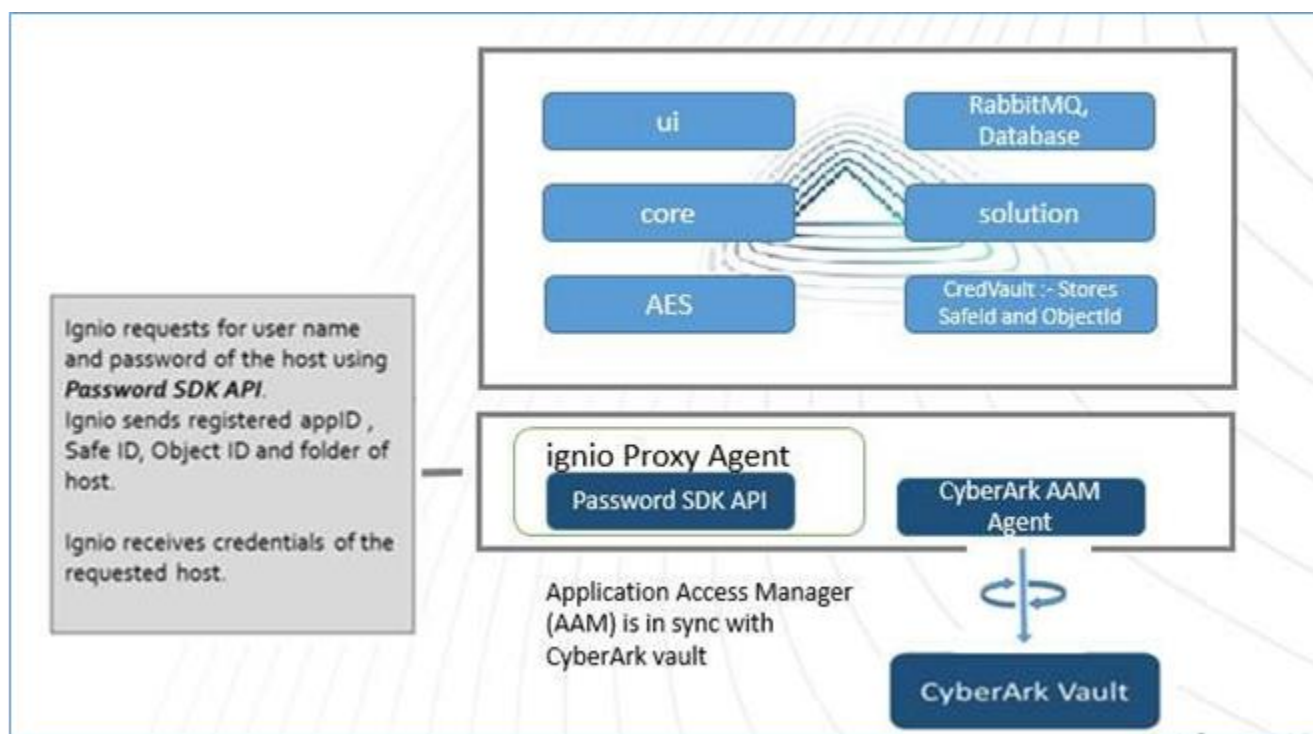


Figure 2: ignio™ and CyberArk interaction details

ignio™ performs operations on the host based on the service request from (IT Service Management) ITSM tool (or) during selfheal. ignio™ refers to its blueprint and obtain the required details of the host. Subsequently, it requests for user name and password of the host using Password SDK API. ignio™ sends the registered appID, Safe ID, Object ID and folder of the host to Password SDK API. Password SDK API interacts with CyberArk Secrets Manager agent and sends the credentials of the requested host (PSDKPassword) to ignio™. ignio™ uses these credentials to connect to the host and perform necessary automation activities based on the pre-built knowledge.

CREDENTIAL RETRIEVAL

Credentials are retrieved from CyberArk and used when a received action request requires access to the target systems. The frequency of credential retrieval varies based on the ignio™ workload.

Note: ignio™ does not store credentials received from CyberArk in database or in memory.

REQUIREMENTS

Typical installation of ignio™ requires up to 8VMs.

SECRETS MANAGER INSTALLATION

Refer to the [“Credential Provider and ASCP Implementation Guide”](#) for CyberArk Agent based installation and configuration.

Steps to configure CyberArk Secrets Manager with ignio™.

- Create application ID for ignio™ in CyberArk
- Install CyberArk Credential Provider on the ignio™ core engine
- Create a Safe for ignio™ user accounts in CyberArk
- Add the ignio™ service accounts in the Safe created
- Update the ignio™ configuration to enable CyberArk as credential provider
To use the credentials for a particular target system, map the Application ID, Safe Name, and Account Name (Object ID) in the lookup file of ignio™ configuration

SECRETS MANAGER CONFIGURATION

The following sections provide details on ignio™ 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.

The screenshot shows the 'Add Application' dialog box. The 'Name' field is populated with 'Ignio'. The 'Description' field is empty. Under the 'Business owner' section, the 'First Name', 'Last Name', 'Email', and 'Phone' fields are empty. The 'Location' field is a dropdown menu showing a backslash character. The 'Access Permitted' checkbox is unchecked, and the 'From' and 'To' dropdowns are empty. The 'Expiration Date' checkbox is unchecked, and the 'Disabled' checkbox is unchecked. The 'Add' and 'Cancel' buttons are at the bottom right.

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

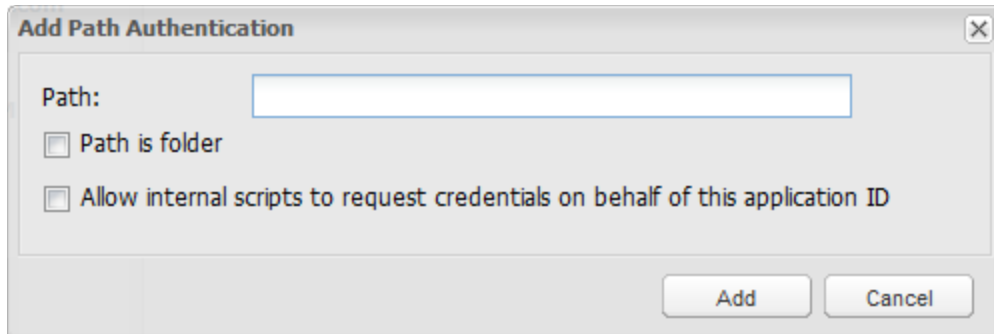
- ☐ Click **Add**. The application is added and is displayed in the Application Details page.

The screenshot shows the 'Application Details: Ignio' page in the Administration console. The left sidebar contains fields for Application ID, Description, Business Owner, Business Owner's Phone, Business Owner's Email, Location, Access Permitted, Expiration Date, and Disabled. The main content area has tabs for 'Authentication' and 'Allowed Machines'. The 'Authentication' tab is active, showing an 'Add' button and a table with columns 'Value' and 'Extended Info'. Below the table, there are checkboxes for 'Allow extended authentication restrictions' and 'Use credential file authentication'.

- ☐ 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.

The screenshot shows the 'Add Operating System User Authentication' dialog box. It has a title bar with a close button. Inside, there is a label 'OS User:' followed by a text input field. At the bottom right, there are 'Add' and 'Cancel' buttons.

- ☐ 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.



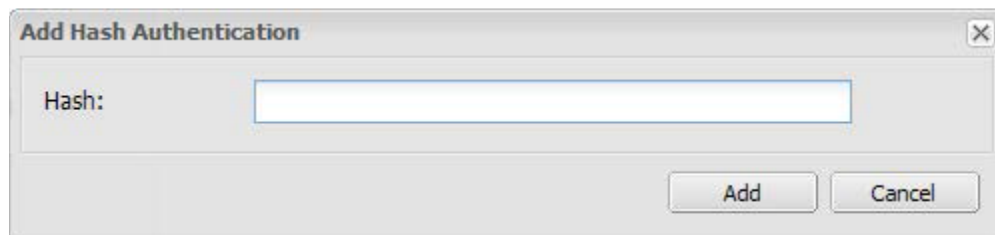
The 'Add Path Authentication' dialog box features a title bar with a close button. It contains a 'Path:' label followed by a text input field. Below the input field are two checkboxes: 'Path is folder' and 'Allow internal scripts to request credentials on behalf of this application ID'. At the bottom right, there are 'Add' and 'Cancel' buttons.

- ☐ 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.



The 'Add Hash Authentication' dialog box has a title bar with a close button. It contains a 'Hash:' label followed by a text input field. At the bottom right, there are 'Add' and 'Cancel' buttons.

- 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.

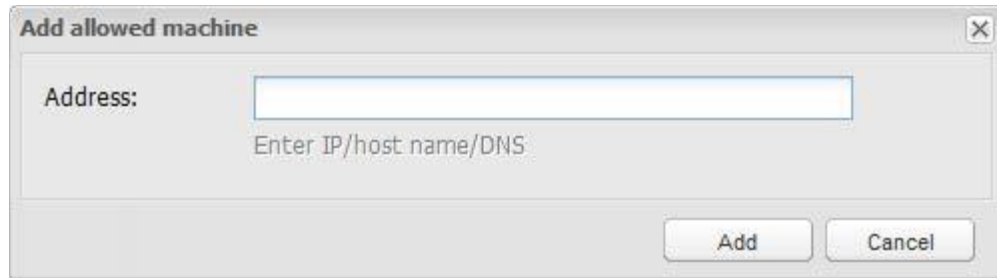
For example, OE883B7OD5B6E3EE37D37198049C9507C8383DB6 #app2

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.

A screenshot of a Windows-style dialog box titled "Add allowed machine" with a close button (X) in the top right corner. The dialog contains a label "Address:" followed by a text input field. Below the input field is a placeholder text "Enter IP/host name/DNS". At the bottom right of the dialog are two buttons: "Add" and "Cancel".

- 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 Safe Member

Search:

Search In:

Vault

Search

Selected Search: Vault

Name	Business Email	Full Name
------	----------------	-----------

☐ Access

☐ Use accounts

☒ Retrieve accounts

☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

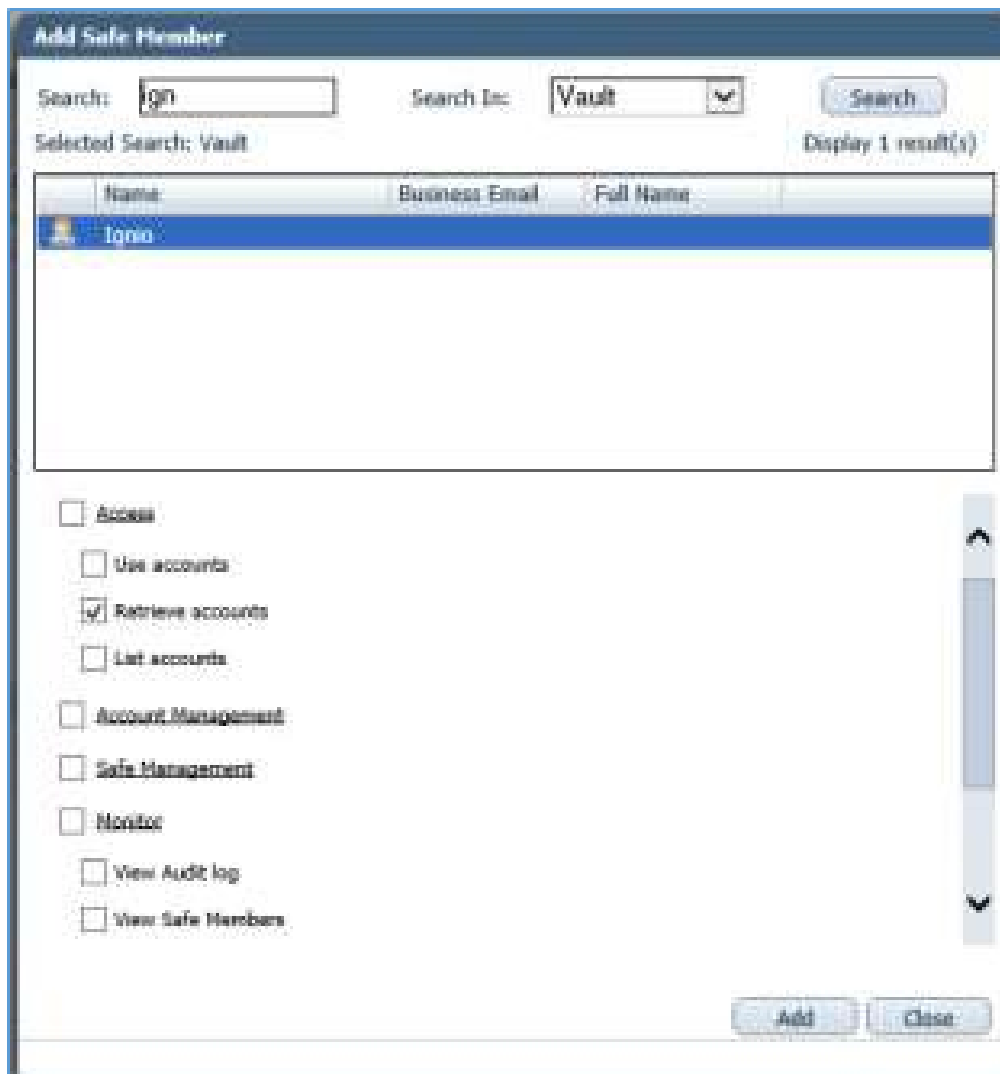
☐ View Audit log

☒ View Safe Members

Add

Close

- ☐ 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**.

IGNIO™ INSTALLATION & INTEGRATION CONFIGURATION

Refer to 'ignio™ Installation guide' for ignio™ installation.

ignio™ integration details with CyberArk are as follows:

1. Copy JavaPasswordSDK.jar to \\ignioProxyAgentInstallationFolder\externaljars folder on the proxy agent machine.
2. Restart proxy-agent

3. In ignio™ runtime, go to **Maps > Graph View > Manage View**
4. Select the node and then click (Add Node) icon.
5. Provide a credential provider entity for CyberArk. Fill values for Application ID and Safe ID. Refer the following figure.

6. In ignio™ runtime, go to **Settings > Platform Configuration > Credential Vault**. Create a new entry
7. Select Credential Provider as CyberArk and Fill data for Object ID, Folder ID and Fail request On Password Change. Refer the following figure.

8. In ignio™ runtime, go to **Settings > Platform configuration > Policy Configuration > Action Execution Engine > Credential**. Apply the policy for the respected node.

Common use cases:

1. Windows domain credentials or other standard credentials
 - a. The user will specify: username, address, platform
 - b. Safe name – optional but recommended for increasing performance
2. Local accounts (windows/Unix)
 - a. The user will specify: username & platform

- b. Safe name – optional but recommended for increasing performance
 - c. When scanning, need to request in the API these username and platform, and add the address of the current machine being scanned
- 3. Non-standard credentials (can't be unique with username+address+Platform)
 - a. The user will specify: Safe and object name (folder is usually root by default)

PARTNER CONTACT INFO

Business Contact	Name	Atul Gupta
	Email	Atul4.g@digitate.com
	Tel	+1 (408) 200-2988
Technical Contact	Name	Harish Iyers
	Email	Harish.iyers@digitate.com
	Tel	+91 (922) 331-8201
Support Contact	Name	Pradyumna Madiwale
	Email	Pradyumna.madiwale@digitate.com
	Tel	+91 (982) 253-0050