



CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Axios Systems

Website: www.axiossystems.com

Name of Product: assyst ITOM

Version: 5.0

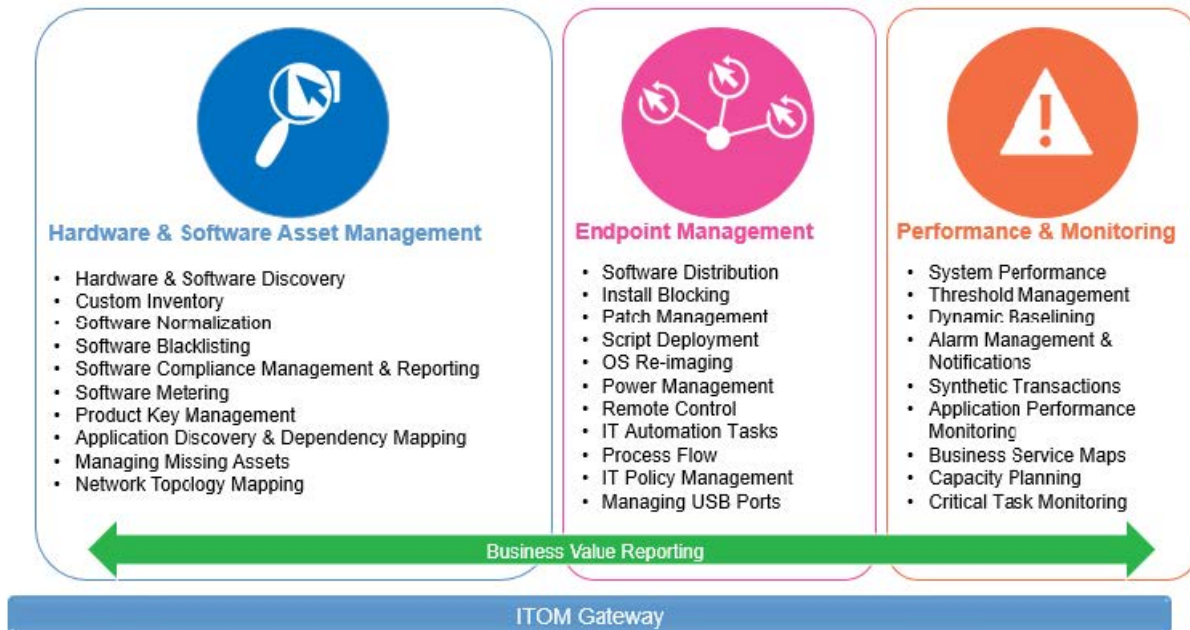
Date: 12 April 2020 (Revised 3 November 2020)

ASSYST ITOM OVERVIEW

assyst ITOM is an enterprise solution for Network Discovery and Inventory Management, Endpoint Management, Software Asset Management and Performing Monitoring Capabilities.

Version: 5

assyst ITOM the application is installed on Windows Platform.



KEY BENEFITS

assyst ITOM is an enterprise solution which enables organizations to:

- Reduce IT costs by aligning the purchasing of hardware and software with business demand.
- Improve ROI of IT by maximizing the utilization of assets.
- Avoid license fines.
- Mitigate Software Security Risks & Avoid Breaches.
- Minimize the risk and costs of unplanned IT service outages and downtime.
- Ensure efficient service delivery by integrating with ITSM.

One of the key benefits of integrating assyst ITOM with Secrets Manager is that it provides a secure solution in which any privileged IT account(s) required by assyst ITOM are managed by CyberArk, which is specifically designed to protect data residing in business systems by eliminating hard-coded credentials from application scripts, configuration files and software code.

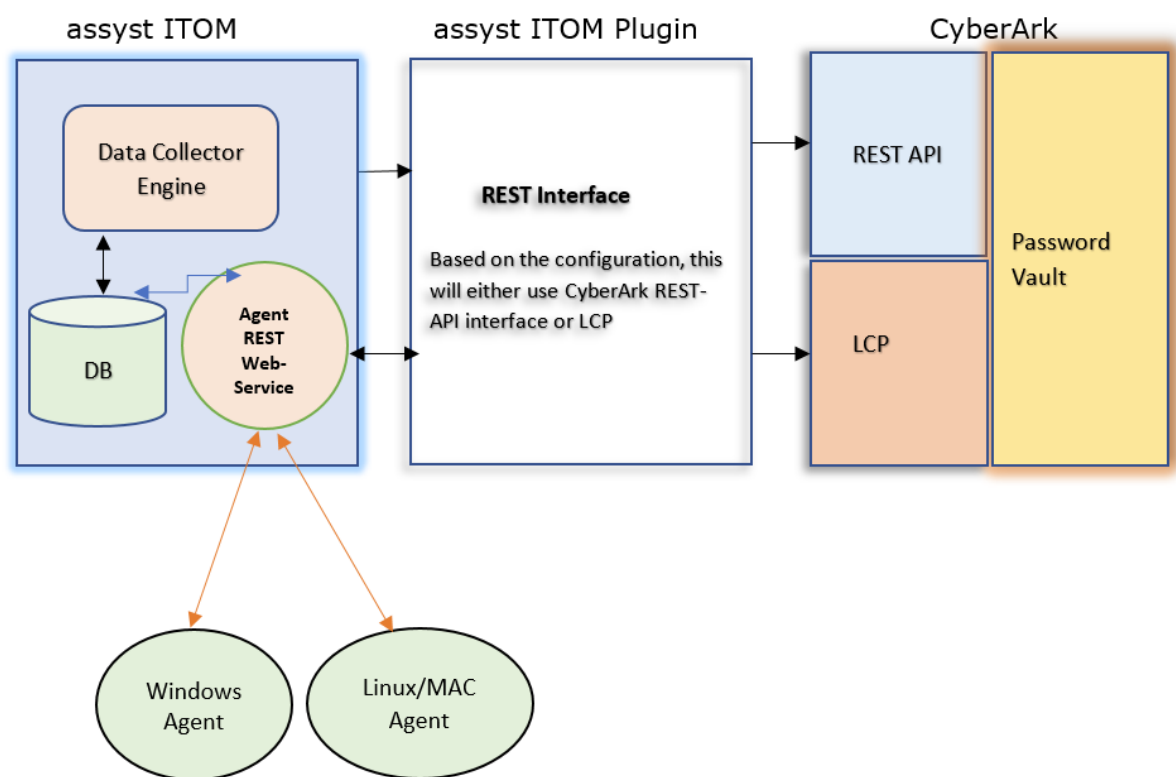
Several of our customers and prospects are already using CyberArk to help them adhere to their IT security policies for privileged IT accounts. Any application running within their IT environment which utilizes and/or stores privileged access accounts must be integrated with or managed by CyberArk.

As an IT Operations solution, assyst ITOM requires credentials which are classified as privileged accounts. Therefore, to be considered as a viable option for our customers and prospects Axios must integrate with CyberArk.

The integration will address the needs of the following roles within an organization:

- **IT Security Mangers** who must ensure that applications running within their organization which utilize or store privileged accounts are run and maintained in accordance with their IT security policies.
- **assyst ITOM Administrators** and users who routinely need to access assyst ITOM to maintain the system or perform their day-to-day operations.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER INTEGRATION

assyst ITOM is typically made up of a central application server, one or more probe servers for remote sites, and a separate database server. assyst ITOM can be installed on premise or in SaaS. Where the SaaS model is concerned, the central application server and Database server are in the cloud and the local collector (probe servers) are installed on the customers' environment.

Axios has developed a plugin for CyberArk. The plugin's REST interface is a common interface for all the password vaults including CyberArk. The plugin queries CyberArk using CyberArk's REST API or LCP based on the configuration and retrieves username and password from vault. Various assyst ITOM features which require credential information leverage the plugin's REST interface. The plugin runs as a

standalone application which can be installed on any server as long as it has network connectivity to the assyst ITOM Server. The plugins' web-services need to be allowed access from firewalls.

CREDENTIAL RETRIEVAL

There are various features in assyst ITOM which require credential information. For example, when an activity such as discovery or software deployment is triggered, it will leverage assyst ITOM plugin's LCP configuration or REST interface. These types of IT Automation activities can be run on demand by the end user or on a scheduled basis.

The required credential information is queried runtime from vault and the memory buffers are cleared after using this. None of the passwords will be stored in a local database.

assyst ITOM's agents (Windows, Linux and MAC) communicate to the ITOM server using a REST API. If any credential information is required by an agent, the communicating web service will leverage the CyberArk's plugin's web services.

Agents don't communicate to a plugin API rather; it will continue to communicate its conventional REST APIs. These conventional APIs will be responsible for obtaining the required information from the CyberArk Vault by talking to the CyberArk plugin's APIs.

SECRETS MANAGER INSTALLATION

This integration supports both the local & central provider Secrets Manager providers. Refer to the "Credential Provider and ASCP Implementation Guide" or "[Central Credential Provider Implementation Guide](#)" for CyberArk Agent based installation and configuration.

The following steps are required:

1. Enable the Password Vault from the assyst ITOM application.
 2. Install the 'assyst ITOM Password Vault Manager' plugin on a server which has network. connectivity to the CyberArk Secrets Manager Server.
 3. Configure Password Vault Configuration in assyst ITOM.
 4. Configure corresponding profiles in assyst ITOM.
-
1. Enable the Password Vault from the ITOM application UI:
 - In assyst ITOM, navigate to **Settings > Advanced System Settings > Global Settings**.
 - Search for '**Password Vault Integration**'.

axios assyst® April 12, 2019 13:09:49 IST Evaluation period expires on 26/4/2019

Home Fault Performance IT Automation Inventory Reports Settings

Global Settings Category All

password Search Clear

Setting Key	Setting Value
Change the text string in the login page for forgot password	Forgot Password
Enable Display of Password Strength	1
Enable/Disable change password option for users	0
Enable/Disable Default Password	0
Enable/Disable password reset Feature	0
Forcing the users to change the passwords during the first login	0
One Time Password Audit Log Details Purging	30
Password change and unlock account audit log details purging	90
Password to access Sapphire VMS	ZzV2VhVUEJWUmrOE5tSnRQdTFBTj6UGc9PV9TQVBQXzM=
Password Vault integration	1
Port for password resetting	636
Preferences Password Policy	Please contact your admin for the password policy
SMTP password	dW1JdDNVYVVLZnVSmNnSip1c0pzNS91eNIQVF1SVh0OGIEbzZRPV9TQVBQXzEz
VNC Password	ZzV2VhVUEJWUmrOE5tSnRQdTFBTj6UGc9PV9TQVBQXzM=

☐ Enable the setting key to **1**.

axios assyst® April 12, 2019 13:10:43 IST Evaluation period

Home Fault Performance IT Automation Inventory Reports Settings

Global Settings

Setting Key Name Password Vault integration

Setting Value **1** Number

Description Password Vault integration for password retrieval, 0 - Disable 1 - Enable

Update Cancel

☐ Select **Update**.

axios assyst® April 12, 2019 13:10:43 IST Evaluation period

Home Fault Performance IT Automation Inventory Reports Settings

Global Settings

Setting Key Name Password Vault integration

Setting Value **1** Number

Description Password Vault integration for password retrieval, 0 - Disable 1 - Enable

Update Cancel

☐ A new icon **Password Vault Integration** will be visible on the settings page:

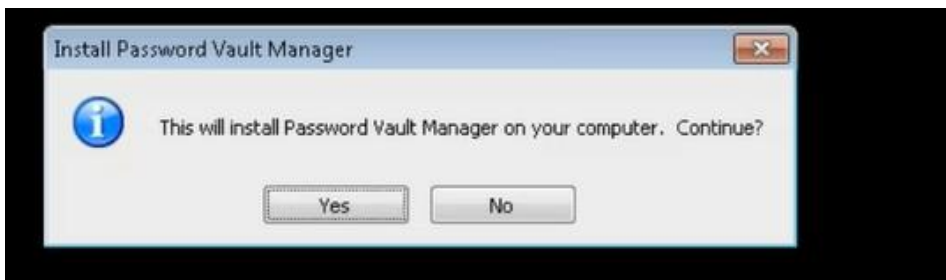
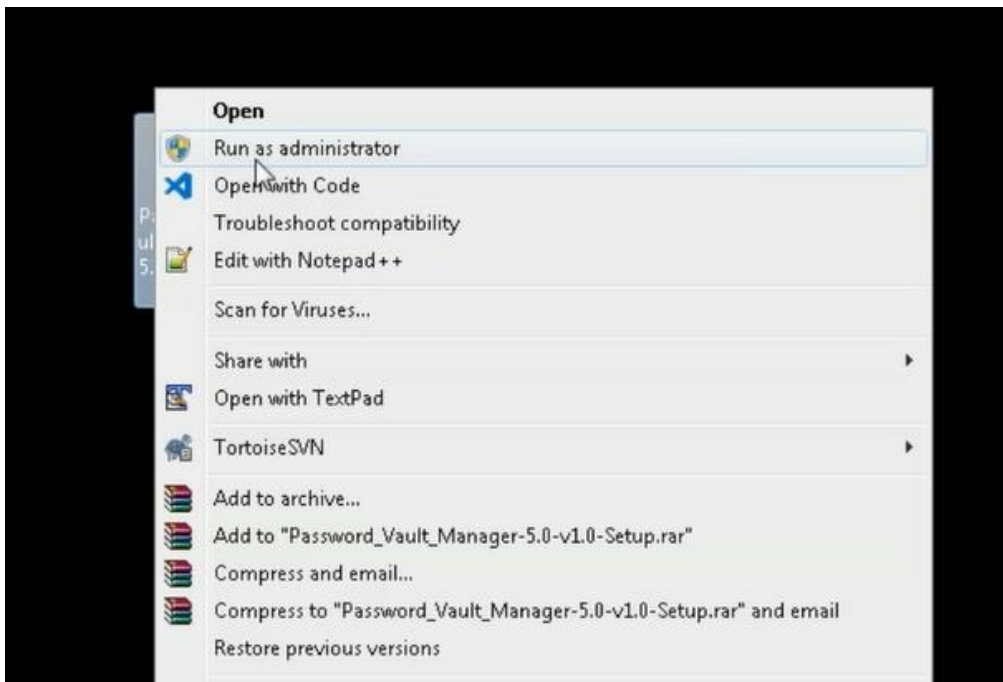
Advanced System Settings

Global Settings Customize Appearance Product License Usage SMTP Settings Proxy Settings About

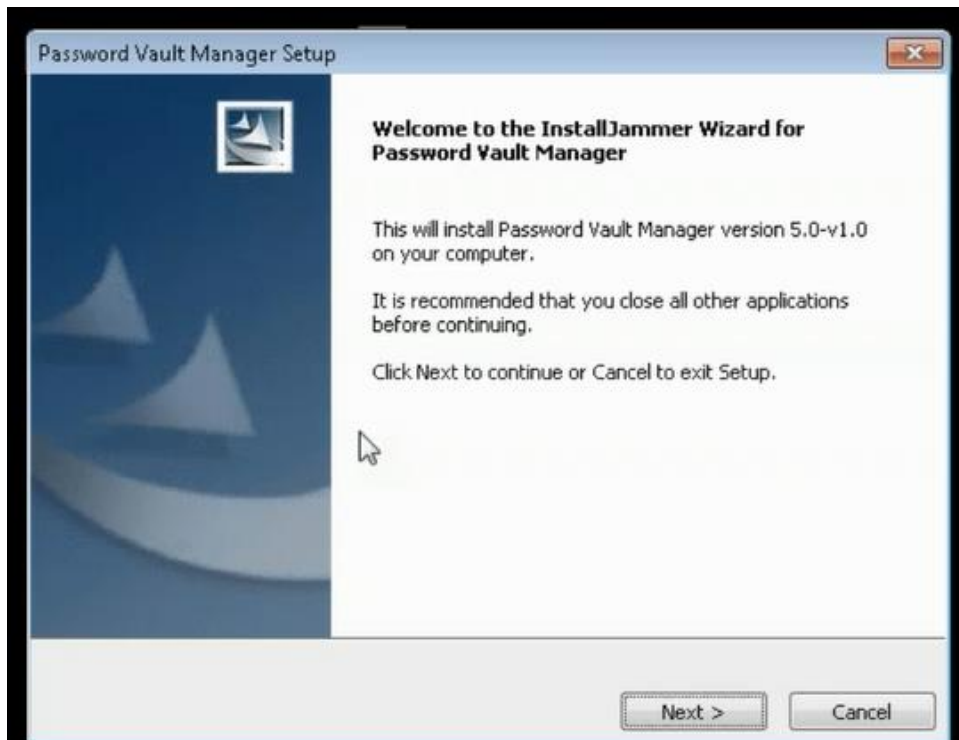
Database Maintenance Mobile Widgets Jump Hosts Encryption Keys **Password Vault Integration**

☐ This concludes enabling the Password Vault from the ITOM application UI.

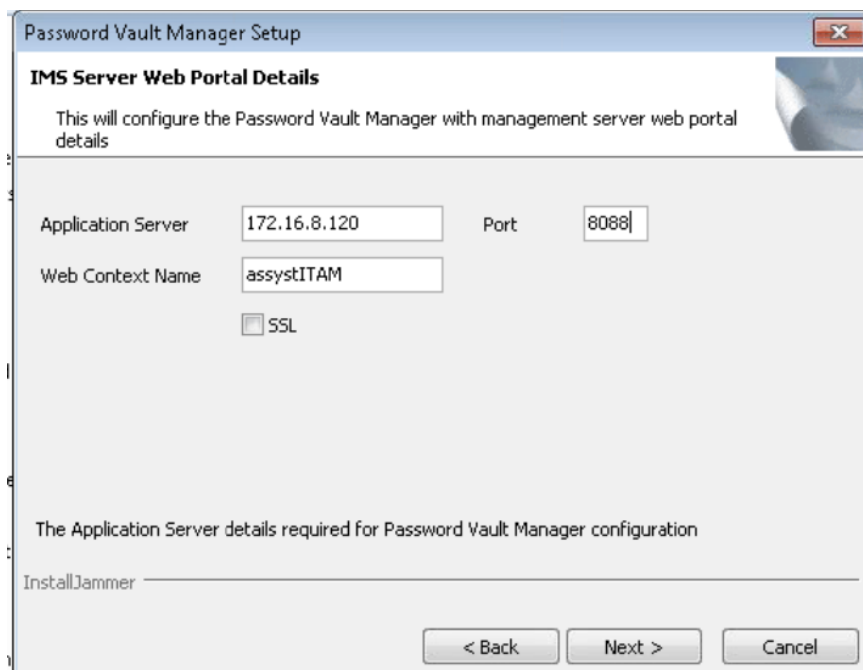
2. Install the **assyst ITOM Password Vault Manager** plugin:
 - Right Select on **Password_Vault_Manager_5.0** plugin.
 - Select **Run as Administrator**.



- Select **Yes**.



- Select **Next**.



- Select **Next**.
- Configure Server Web Portal details as required and Select **Next**.

The screenshot shows the 'Password Vault Manager Setup' window with the 'IMS Server Web Portal Details' tab selected. The window title is 'Password Vault Manager Setup'. Below the title bar, the text reads 'IMS Server Web Portal Details' and 'This will configure the Password Vault Manager with management server web portal details'. The main area contains two text input fields: 'Application Server' with the value '172.16.8.120' and 'Port' with the value '8088'. Below these is a 'Web Context Name' field with the value 'assystITAM' and an unchecked 'SSL' checkbox. At the bottom, there is a progress bar labeled 'InstallJammer' and three buttons: '< Back', 'Next >', and 'Cancel'.

Password Vault Manager Setup

IMS Server Web Portal Details

This will configure the Password Vault Manager with management server web portal details

Application Server: 172.16.8.120 Port: 8088

Web Context Name: assystITAM

☐ SSL

The Application Server details required for Password Vault Manager configuration

InstallJammer

< Back Next > Cancel

- Configure Web Portal Port Configuration details as required.
- Select **Next**.

The screenshot shows the 'Password Vault Manager Setup' window with the 'Password Vault Manager Web Portal Port Configuration' screen. The window title is 'Password Vault Manager Setup'. On the left is a blue sidebar with a white icon. The main area has the title 'Password Vault Manager Web Portal Port Configuration' and the text 'Specify the port for running Password Vault Manager Web Portal'. Below this is a 'Port' input field with the value '8087'. A note at the bottom states: 'NOTE: The port should be in the range 1025-65535 or 8080.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

Password Vault Manager Setup

Password Vault Manager Web Portal Port Configuration

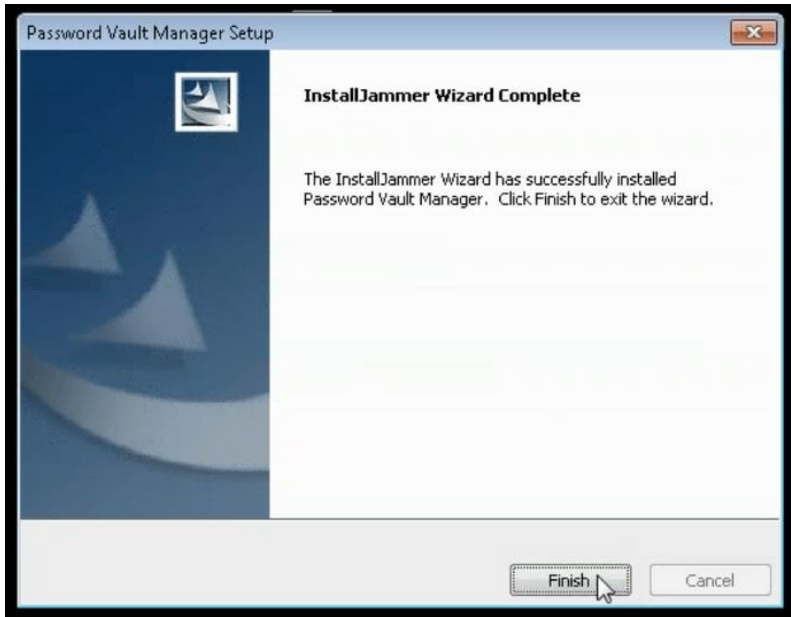
Specify the port for running Password Vault Manager Web Portal

Port: 8087

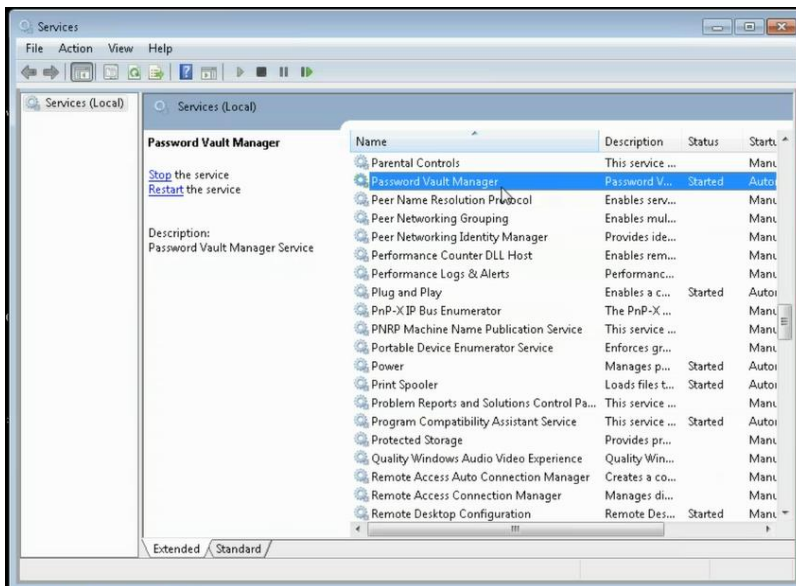
NOTE: The port should be in the range 1025-65535 or 8080.

< Back Next > Cancel

- Select **Finish**.



- Once it is installed it will create a Service called 'Password Vault Manager'.



- This concludes Installing the 'assyst ITOM Password Vault Manager' plugin.

The next step is only required if the customer is using the local credential provider assyst ITOM Password Vault Manager console. If the customer is using the local credential provider, the JAR File will need to be uploaded.

The JAR File comes from Secrets Manager local credential provider installation.

The JAR File connects to CyberArk vault to retrieve information (this is for security).

- Open an internet browser.

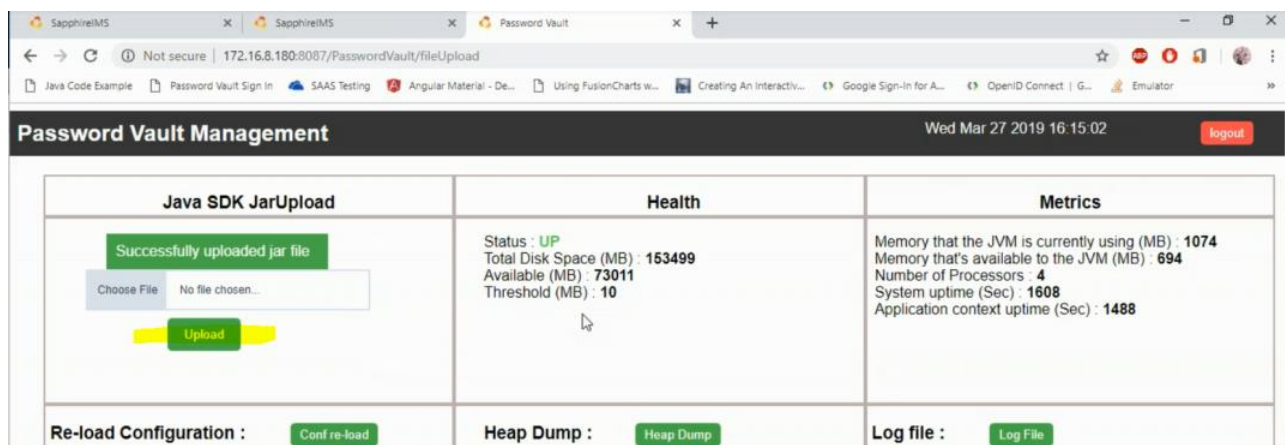
- Enter the IP address or hostname of the server where the Password Vault Manager plugin has been installed following by **"/PasswordVault/"**.
For example: 172.16.8.180.8087/PasswordVault/
- ☐ Enter the username and password:
 - Default credentials are **"admin"/"admin"**.
 - We strongly recommend that these are changed after plugin install.



- ☐ Once authenticated this will bring you to the console where was can upload the JAR file:



- ☐ From the **Java SDK JarUpload** section select **Choose File**.
- ☐ Located the **JavaPasswordsSDK.JAR** file from the Secrets Manager local provider folder.
- ☐ Select **Open**.
- ☐ Then select **Upload**.



- ☐ You will see a message to confirm the upload was successful.

3. Configure Password Vault Configuration:

- In ITOM, navigate to **Settings > Advanced System Settings > Password Vault Integration**.
- Select **Password Vault Configuration**.
- Configure as required:
 - Enter the hostname of IP address of the Server where the plugin is installed.
 - Enter the port number.
 - If https was enabled during install of plugin, check **https**.
 - The Authentication Key or Authentication Token can be entered manually, or you can select the **Generate** button.

axios assyst® April 12, 2019 13:27:01 IST Evaluation period expires

Home Fault Performance IT Automation Inventory Reports **Settings**

Password Vault Password Vault Configuration

IP Address/Host Name: 172.16.8.180

Port: 8080

https: ☐

Authentication Key: 167ca53c-6400-44c1-9bab-8c9692b34c63 **Generate**

Authentication Token: 2bf8da8a-b231-4e56-afc1-230b2b5215e4 **Generate**

API Type: ☒ Local Credential Provider ☐ REST

Save Cancel

- Select **Save**.
 - Back in the PasswordVault, perform a **Cong re-load** so that the Authentication Key and Authentication Token can be re-synced.
- For example: 172.16.8.180.8087/PasswordVault/

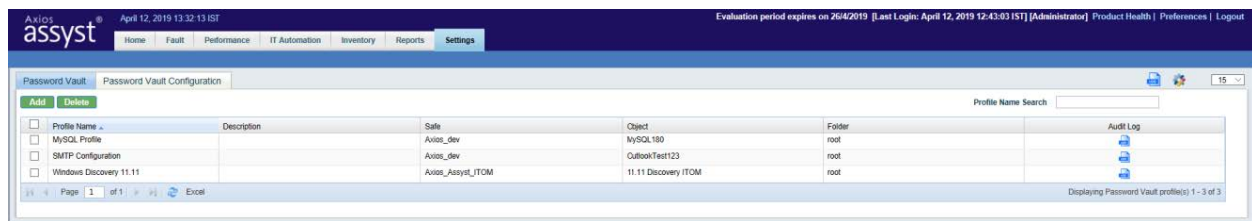
Wed Mar 27 2019 16:15:02 **logout**

Java SDK JarUpload	Health	Metrics
Successfully uploaded jar file Choose File No file chosen... Upload	Status : UP Total Disk Space (MB) : 153499 Available (MB) : 73011 Threshold (MB) : 10	Memory that the JVM is currently using (MB) : 1074 Memory that's available to the JVM (MB) : 694 Number of Processors : 4 System uptime (Sec) : 1608 Application context uptime (Sec) : 1488
Re-load Configuration : Conf re-load	Heap Dump : Heap Dump	Log file : Log File

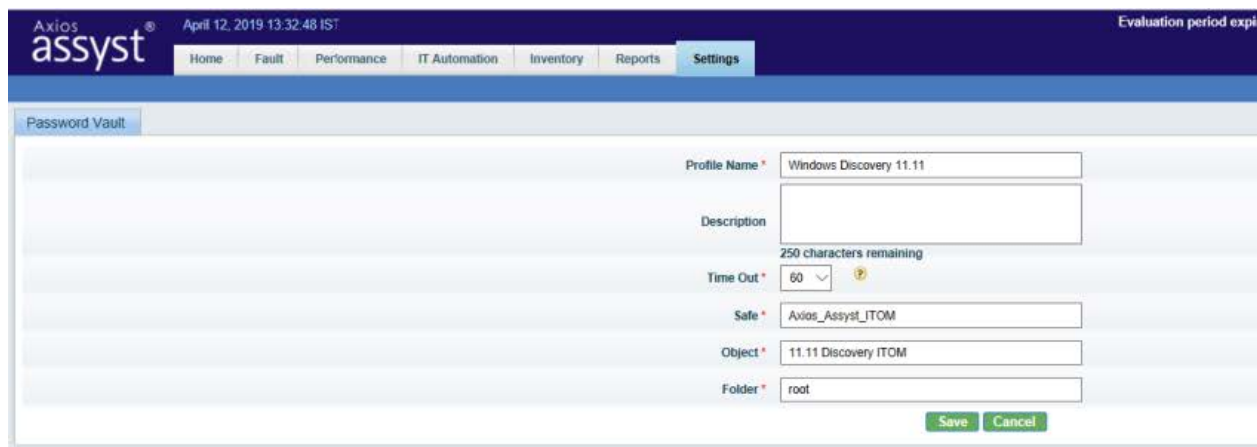
4. Configure corresponding profiles in the assyst ITOM.

Note: Profiles in the CyberArk vault will need to be referenced as part of this activity.

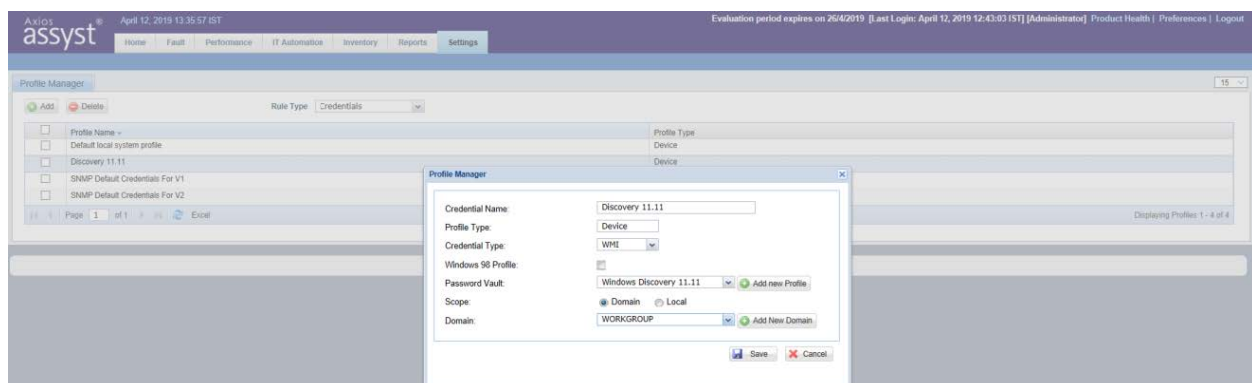
- Navigate to **Settings > Advanced System Settings > Password Vault Integration > Password Vault**.



- Select **Add**.
- Populate the required details accordingly:
 - Safe, Object and Folder details should reflect those configured in the CyberArk Vault.
 - Folder will be root by default unless the Profile in CyberArk vault has been saved elsewhere.



- Select **Save**.
- Now create a standard discovery profile in ITOM. This is the first step required when discovery any devices or applications in ITOM i.e. setting up the credentials which will be used during the network scan process.
- Navigate to **Settings > Asset and Inventory Management > Profile Manager**.
- Select **Add**.
- Configure as required, selecting the corresponding profile in CyberArk from the Password Vault drop down.



- Populate as required.
- Select **Save**.

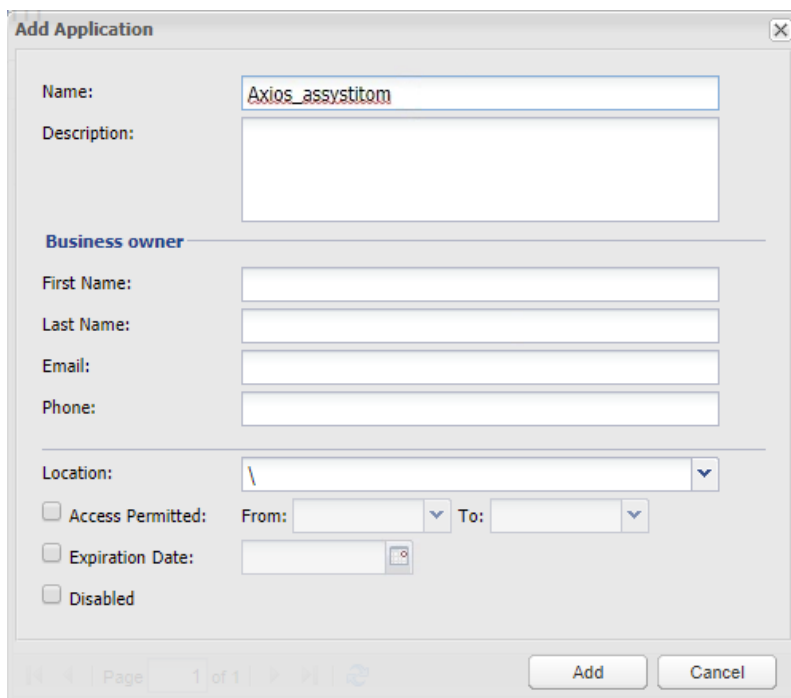
SECRETS MANAGER CONFIGURATION

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

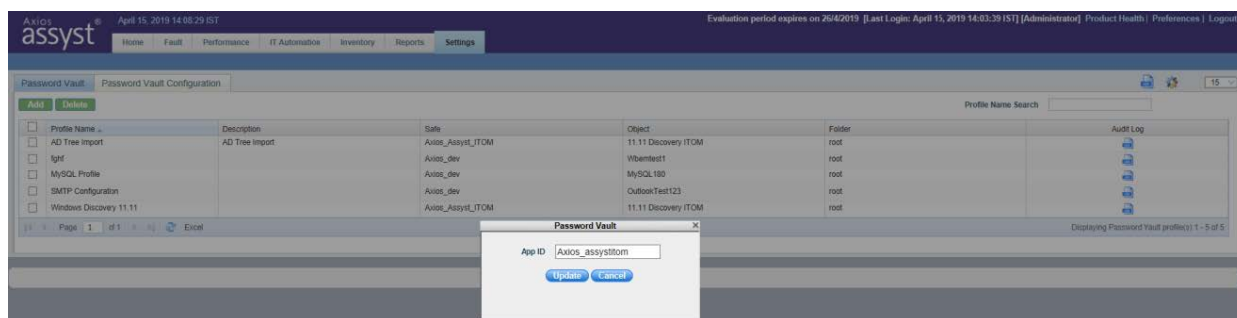
DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

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.



- ☐ In ITOM, navigate to **Settings > Advance System Settings > Password Vault Integration**.
 - On the right-hand side, select settings and populate the App ID to reflect that which was configured in CyberArk.



- Select **Update**.
- ☐ Specify the following information:

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

Application Details: Axios_assystitom

Application Id: Axios_assystitom

Description:

Business Owner:

Business Owner's Phone:

Business Owner's Email:

Location: \

Access Permitted: None

Expiration Date: None

Disabled: No

Authentication tab selected. Add button clicked. OS user selected.

- ☐ 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.

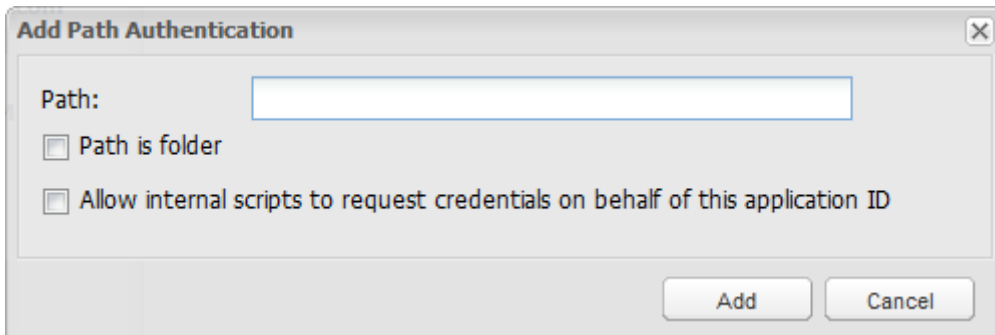
Add Operating System User Authentication

OS User: [Text Box]

Add Cancel

- ☐ 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 image shows a dialog box titled "Add Path Authentication". It has a close button (X) in the top right corner. Inside the dialog, there is a label "Path:" followed by a text input field. Below the input field, there are two checkboxes: "Path is folder" and "Allow internal scripts to request credentials on behalf of this application ID". At the bottom right of the dialog, there are two buttons: "Add" and "Cancel".

- ☐ 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.

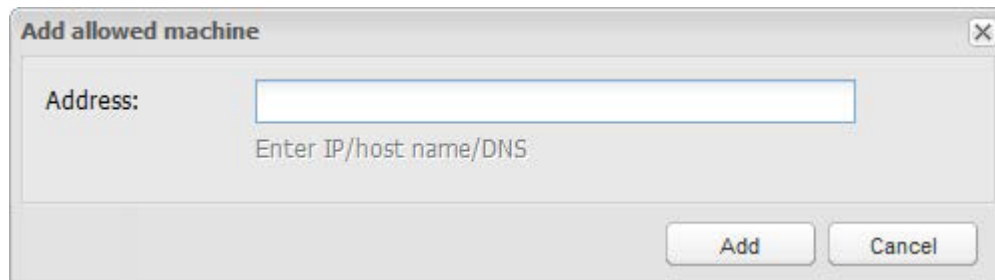
- ☐ Specify a hash:

- 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 image shows a dialog box titled "Add Hash Authentication". It has a close button (X) in the top right corner. Inside the dialog, there is a label "Hash:" followed by a text input field. At the bottom right of the dialog, there are two buttons: "Add" and "Cancel".

- 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". It features a close button (X) in the top right corner. The main area 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, there 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

Add Safe Member

Search: Search In:

Selected Search: Display 1 result(s)

Name	Business Email	Full Name
 Axios_assysitom		

☐ Access

- ☐ Use accounts
- ☒ Retrieve accounts
- ☐ List accounts

☐ Account Management
☐ Safe Management
☐ Monitor

- ☐ View Audit log
- ☐ View Safe Members

Axios_assysitom has been added.

- ☐ 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**.

ASSYST ITOM INSTALLATION & INTEGRATION CONFIGURATION

Refer to [assyst ITOM installation document](#) for assyst ITOM installation.

Axios assyst® April 12, 2019 16:24:59 IST
 Home Fault Performance IT Automation Inventory Reports **Settings**

Password Vault

Profile Name * Windows Discovery 11.11
 Description
 250 characters remaining
 Time Out * 60
 Safe * Axios_Assyst_ITOM
 Object * 11.11 Discovery ITOM
 Folder * root
 Save Cancel

Use Case 1 - Creating Windows Domain Account

Note: Profiles in the CyberArk vault will need to be referenced as part of this activity.

- Navigate to **Settings > Advanced System Settings > Password Vault Integration > Password Vault**.

Profile Name	Description	Safe	Object	Folder	Audit Log
☐ MySQL Profile		Axios_dev	MySQL180	root	
☐ SMTP Configuration		Axios_dev	OutlookTest123	root	
☐ Windows Discovery 11.11		Axios_Assyst_ITOM	11.11 Discovery ITOM	root	

Add Delete Profile Name Search
 Page 1 of 1
 Displaying Password Vault profiles 1 - 3 of 3

- Select **Add**.
- Populate the required details accordingly.
 - Safe, Object and Folder details should reflect those configured in the CyberArk Vault.
 - Folder will be root by default unless the Profile in CyberArk vault has been saved elsewhere.

Axios assyst® April 12, 2019 13:32:13 IST
 Home Fault Performance IT Automation Inventory Reports **Settings**

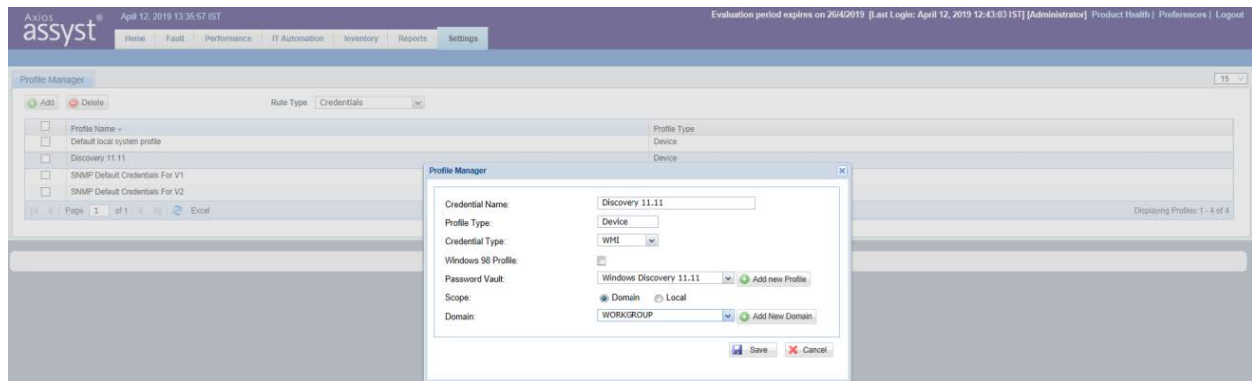
Password Vault

Profile Name * Windows Discovery 11.11
 Description
 250 characters remaining
 Time Out * 60
 Safe * Axios_Assyst_ITOM
 Object * 11.11 Discovery ITOM
 Folder * root
 Save Cancel

- Select **Save**.

Now create a standard discovery profile in ITOM. This is the first step required when discovery any devices or applications in ITOM i.e. setting up the credentials which will be used during the network scan process.

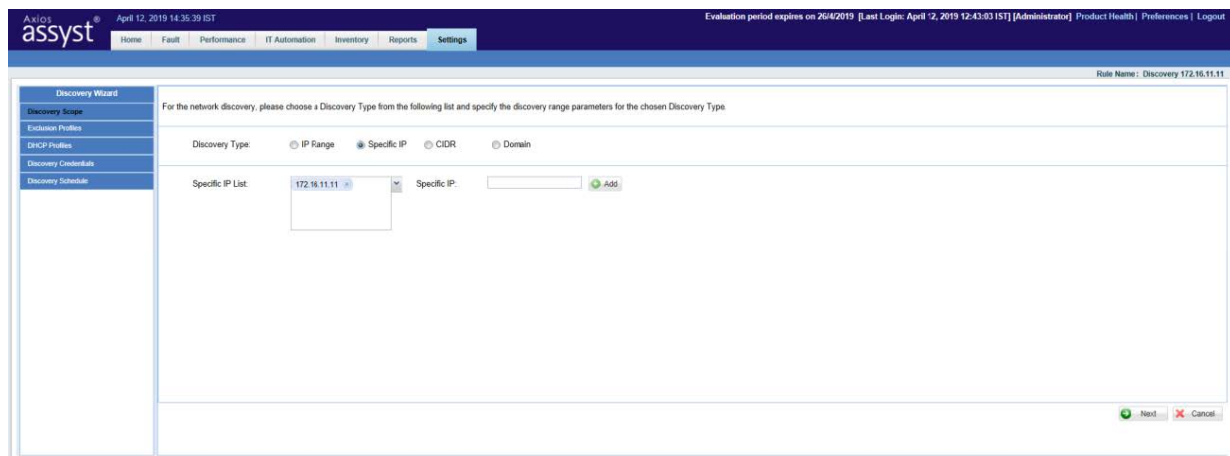
- Navigate to **Settings > Asset and Inventory Management > Profile Manager**.
- Select **Add**.
- Configure as required, selecting the corresponding profile in CyberArk from the Password Vault drop down.



- Populate as required.
- Select **Save**.

Now that the credential profile is created, we will setup a discovery scan in ITOM:

- Navigate to **Settings > Asset and Inventory Management > Discovery Profiles and Wizard > Add**.



- Configure Exclusion and DHCP Profiles if required.
- Select correct credential profile.

- Select **Next**.
- Select **Once** for the schedule.

- Save Configuration using a unique name.
- Select **Save**.
- New devices will appear under **Discovered Nodes**.

Host Name	Status	Inventory Time	Discovery Time	Last Response Time	Device Category	Error Description	Scheduler Info
WIN2003-DEMO0		2019-04-11 19:51	2019-04-11 19:46	2019-04-12 17:46	Domain Controller	--	
BEIJING		2019-04-12 13:47	2019-03-06 16:11	2019-04-12 17:47	Desktop	--	

Use Case 2 - Active Directory User Import

- In ITOM Navigate to **Settings > User Management > User Management > AD and LDAP Authentication > LDAP Rule Configuration > Add**.
- Configure the rule as required:
 - Produce LDAP Rule Name.
 - Credential Profile which corresponds with correct CyberArk Vault profile.

- Hostname/IP Address of LDAP server.

LDAP Rule Configuration

LDAP Rule

LDAP Rule Name*

Job Processor

Credential Profile Mapping

Credential Profile*

Host Name/IP Address*

Protocol and OS Configuration

Protocol Type ☐ AD/L ☒ LDAP

Operating System ☐ UNIX ☒ Windows

AD-SapphireIMS Attribute Mapping

Set Default ☒

AD ATTRIBUTE	SAPPHEREIMS FIELD
Display Name	Full Name
Mobile	Choose
Office	Wing
Email	Email Address
City	Choose
Employee ID	Choose
Telephone Number	Choose

- Select **Save**.
- Then Select **LDAP Configuration**.
- Select on **Add**.
- Configure as required.

LDAP Configuration

Configuration

Configuration Name

Default User Role

LDAP Rule*

Organizational Unit

Organizational Unit

- phyll_test
- new2122
- new1
- kalaschev
- harish_ad
- Users
- UrusChandran
- Testok
- Test_Data11
- Test4

Notification

Notify On User Status Change/Task Finished ☐

Incremental Sync Scheduler ☒ Enable ☐ Disable

☐ Hourly ☐ Daily ☐ Weekly ☐ Monthly ☒ Once

Date

Retry Count

Retry Interval (Mins)

Default User Role:
The default behaviour will map all LDAP users to Users role. Selecting a role will always map the users to the selected role. LDAP sync and local role changes will not be preserved.

User status alert notification:
Enable global settings to get notification on change of user status. Setting key - LDAP user status alert notification Category-ServiceDesk.

Incremental Sync Configuration:
All users will be fetched when configuration is created for the first time. Incremental sync will add the new users which are created in AD as well as it will update the existing user role if anything got changed in AD.

- Select **Next**.
- Populate scheduler details.

Incremental Sync Scheduler ☒ Enable ☐ Disable

☐ Hourly ☐ Daily ☐ Weekly ☐ Monthly ☒ Once

Date: 2019-04-12 17:04 Priority: High

Retry Count: 0

Retry Interval: 15 (Mins)

Full Sync Scheduler ☒ Enable ☐ Disable

☐ Hourly ☐ Daily ☐ Weekly ☐ Monthly ☒ Once

Date: 2019-04-12 17:04 Priority: High

Retry Count: 0

Retry Interval: 15 (Mins)

Incremental Sync Configuration:
All users will be fetched when configuration is created for the first time. Incremental sync will add the new users which are created in AD as well as it will update the existing user info if anything got changed in AD.

Full Sync Configuration:
Full sync will import the users from the selected OU's and update all the user details.

[Next](#) [Update](#) [Cancel](#)

- Select **Save**.
- Status of IT Automation Task can be tracked under **IT Automation > Automation Tasks > Automation Tasks Status**.

Name	Job Title	% of Completion	% of Success
CMDB Configuration Backup	Allows to take Database backup	100	100
CMDB Data Backup	Allows to take Database backup	100	100
Product Configuration Backup	Allows to take Database backup	100	100
Product Data Backup	Allows to take Database backup	100	100
ServiceDesk Configuration Backup	Allows to take Database backup	100	100
ServiceDesk Data Backup	Allows to take Database backup	100	100
LDAP RULE IMPORT_import	Allows to import Users from ldap server	100	100
LDAP RULE IMPORT_RE_SYNC_2...	Allows to import Users from ldap server	0	0
LDAP RULE IMPORT_resync	Allows to import Users from ldap server	100	100
Compliance Calculation Job	Allows to perform IT and Software Compliance Calculation	100	100

Page 1 of 1

Once complete you can verify that users that have been imported

- Navigate to **Settings > User Management > Users**.

User ID	Full Name	Email Address	Cell No	Access Type	Employee ID	Wing	Telephone No
admin	Administrator	--	--	Master Admin	--	--	--
AMCUSER	AMCUSER	--	--	User	--	--	--
dhama	dhama dhama	--	--	User	--	--	--
mspadmin	MSP Administrator	--	--	Master Admin	--	--	--
mspenginer	MSP Engineer	--	--	Master Admin	--	--	--
mspmanager	MSP Manager	--	--	Master Admin	--	--	--
ScheduleJobAlerts	ScheduleJobAlerts	--	--	User	--	--	--
System	System	--	--	Master Admin	--	--	--

Page 1 of 1

Use Case 3 – Application Performance Monitoring for MySQL

- In ITOM navigate to **Settings > Advanced System Settings > Password Vault Integration > Password Vault**.
- Select **Add**.
- Configure accordingly.

Axios assyst® April 12, 2019 17:51:01 IST

Home Fault Performance IT Automation Inventory Reports **Settings**

Password Vault

Profile Name * MySQL Profile

Description
 250 characters remaining

Time Out * 60 ?

Safe * Axios_dev

Object * MySQL180

Folder * root

Save Cancel

- Select **Save**.
- Now configure the MySQL instance for performance monitoring.
- Navigate to **Settings > Performance Monitoring > Application Performance**.
- Select **Add**.
- Configure as required.

Axios assyst® April 12, 2019 17:51:33 IST

Home Fault Performance IT Automation Inventory Reports **Settings**

Applications

Resource Name MySQL 9.100

Poller Category Database Servers

Poller Type MySQL

Poll Interval (Minutes) 3

Poll Status Enabled

Organization Unit ROOT > PreShipped OU

Description

Password Vault MySQL Profile AddVaultProfile

Server Hostname/IP Address 172.16.9.100

Port 3306

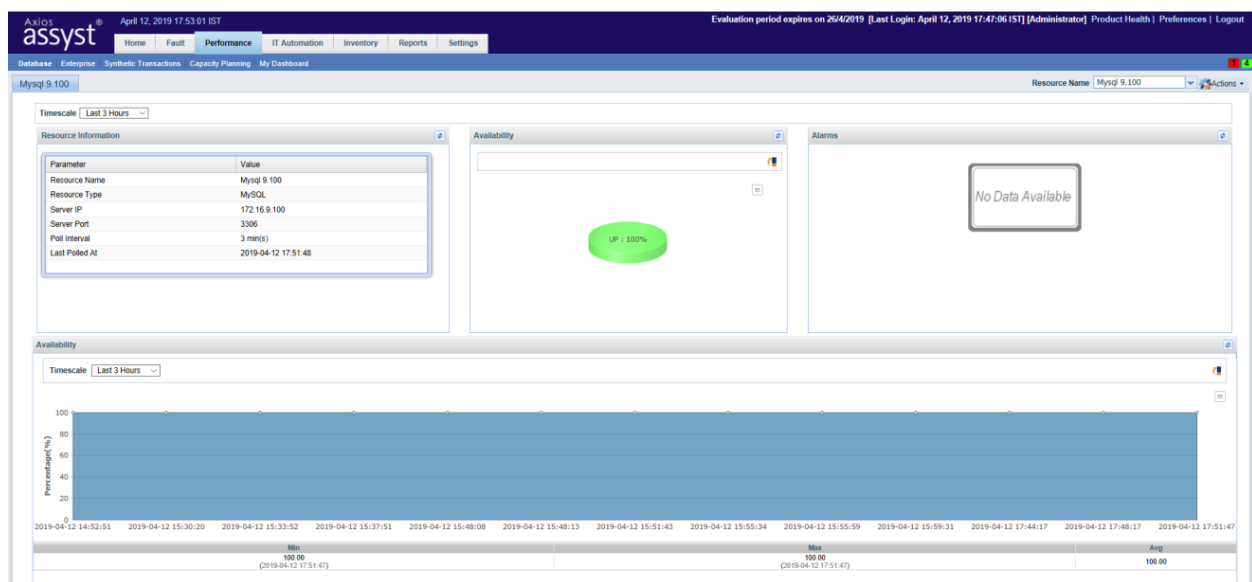
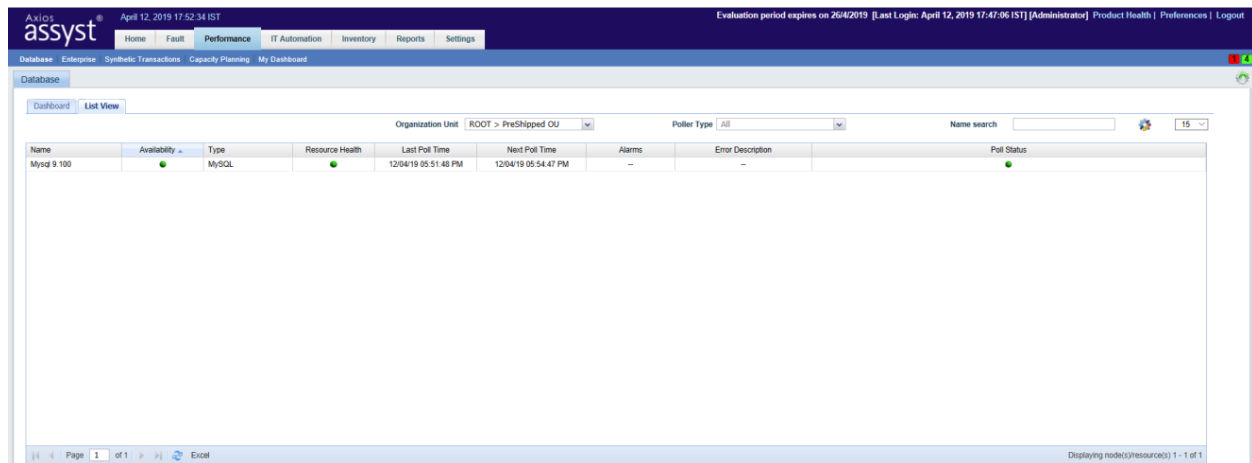
Schema ims

Enable Custom Queries ☐

Test Update Cancel

- Select **Test** to verify successful authentication.
- Select **Save**.

Results can be configured under **Performance > Database**.



Use Case 4 – SMTP Settings

- In ITOM, navigate to **Settings > Advanced System Settings > Password Vault Integration > Password Vault**.
- Configure accordingly.

axios
assyst® April 12, 2019 16:58:17 IST

Home Fault Performance IT Automation Inventory Reports **Settings**

Password Vault

Profile Name * SMTP Configuration

Description

250 characters remaining

Time Out * 60 ?

Safe * Axios_dev

Object * OutlookTest123

Folder * root

Save Cancel

- Select **Save**.
- Navigate to **Settings > Advance System Settings > SMTP Settings**.
- Configure accordingly.

axios
assyst® April 12, 2019 17:02:42 IST Evaluation period expires on 26/4/2019 [Last Login: April 12, 2019 16:55:44 IST] [Administrator] Product Health | Preferences | Logout

Home Fault Performance IT Automation Inventory Reports **Settings**

SMTP Settings

Select mail service ☒ SMTP ☐ Exchange

SMTP Server smtp-mail.outlook.com

From Address aruna.chandrapa021@outlook.com

From Address Display Tag aruna.chandrapa021@outlook.com

SMTP Port 587

Authentication ☒ SMTP server needs authentication

Password Vault SMTP Configuration Add Vault Profile

isTLS ☒

isSSL ☐

Test Update Cancel

- Select **Test** to verify successful authentication.
- Select **Save**.

Business Contact	Name	Laura Herr
	Email	Laura.herr@axiossystems.com
	Tel	+44 (0131) 220-4748
Technical Contact	Name	Paul McCulloch
	Email	Paul.McCulloch@axiossystems.com
	Tel	+44 (0131) 220-4748
Support Contact	Name	Axios Service Centre
	Email	support@axiossystems.com
	Tel	+44 (0131) 220-3600