APPLICATION ACCESS MANAGER

(Agentless Central Credential Provider CCP)

AAM INTEGRATION - TECHNICAL DOCUMENTATION TEMPLATE

DOCUMENT PURPOSE: THIS TEMPLATE IS TO BE COMPLETED BY PARTNER AND IS REQUIRED FOR CYBERARK SECURED CERTIFICATION. THE AAM INTEGRATION TECHNICAL DOCUMENTATION WILL BE MADE AVAILABLE TO PARTNERS, CUSTOMERS AND PROSPECTS. **AS YOU COMPLETE EACH SECTION, PLEASE REMOVE THE DIRECTIONS PROVIDED.**

Name of Company: JDisc GmbH

Website: https://www.jdisc.com

Name of Product: JDisc Discovery

Version: 5.0 (and later)

Date: 08/10/2021

PARTNER SOLUTION OVERVIEW

JDisc Discovery is an automated network inventory and discover solution. It collects asset and configuration information from a variety of different devices on the network. The goal is to have an up-to-date database with asset and configuration information of all the devices on a client's network.

Asset and configuration information include installed operating system, installed software, services, patches, processors, memory modules, network interfaces and many more.

In order to obtain this information access (in some cases root/admin access) is required. Up to now, customers configure the username and password required to authenticate within our configuration dialogs. However, more and more customers are concerned about having one account accessing all information and thus used password managers such as Cyberark. In this case, passwords are managed by Cyberark and not in our product. JDisc Discovery will then query Cyberark via API whenever it needs a username and password to obtain access to a device.

KEY BENEFITS

Benefits of JDisc Discovery

- Obtains a current and up-to-date database with IT asset and configuration information.
- Obtains relationships between IT assets
- JDisc Discovery obtains all information automatically via APIs from the devices on the network. No manual data gathering needed.

Benefits of integrating JDisc Discovery with CyberArk AAM:

- Customers using CyberArk do not want to enter credentials into our tool for security reasons
- CyberArk can also change the passwords on a high frequency which makes it impossible to store that frequently changing credentials in our database.

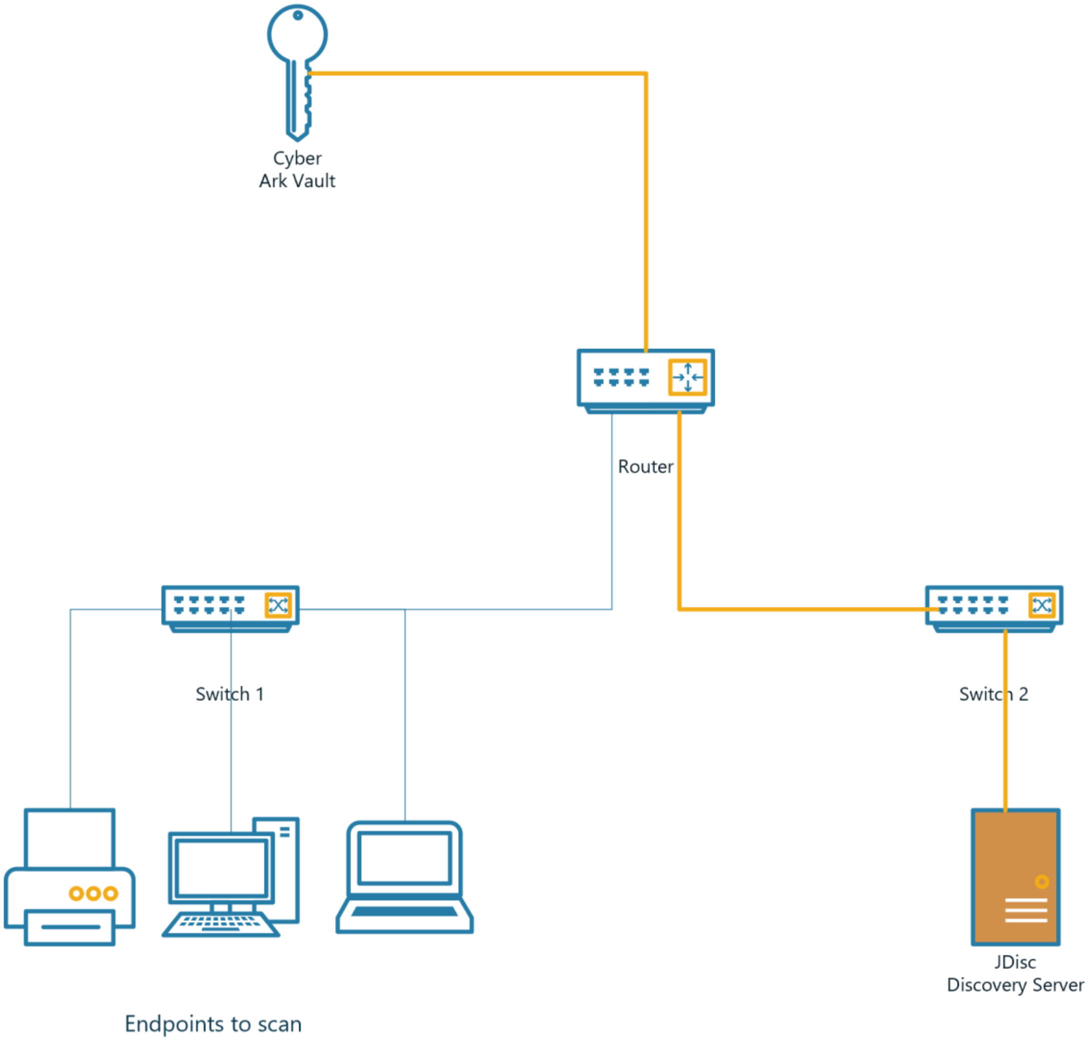
PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

The JDisc Discovery server is a central server installed on premises at a customer site. From that central location, it pings and performs LDAP queries in order to find the endpoints and their IP addresses. Once the endpoints get scanned and JDisc Discovery needs the access credentials to access an endpoint, it queries the CyberArk server for the current username and password. Then it uses this username and password to connect to the actual endpoint. When it succeeds, then JDisc Discovery is able to pull asset and configuration information.

Since we are using HTTPS REST requests, it doesn't matter whether the CyberArk server resides in the cloud or on premises. The only prerequisite is that it is accessible via HTTPS and that the REST calls from the JDisc Discovery Server to the CyberArk server are not blocked by a firewall.

The diagram below displays a simple network consisting of a router, two switches and the CyberArk server. "Switch 1" connects to the endpoints to be scanned and the JDisc Discovery server is typically located in another network connected via a router.

During the discovery, the JDisc Server connects to both – the CyberArk server in order to obtain current access credentials for a device and to the endpoints in order to query asset and configuration information.



AAM INTEGRATION

The integration is part of our central JDisc Discovery server. Configuration dialogs let users add as many CyberArk servers as required. During the device scan, JDisc Discovery queries the current access credentials from the CyberArk server and then uses those credentials to query the actual endpoint. The number of endpoints might vary from customer to customer depending on its size (starting from just a few hundred to thousands of devices).

The number of JDisc Discovery servers might vary from one (when the whole network is accessible from the JDisc server) to a few (usually 3-5) when there are firewalls blocking the traffic in between.

CREDENTIAL RETRIEVAL

JDisc Discovery has several phases when scanning a network. The first phase is to find the active devices on the network. This is accomplished by pinging networks or querying LDAP information. Once, we have identified the active IP addresses, then those IP addresses will be added to a discovery device queue which is then processed by a configurable number of concurrent jobs.

For each of those jobs where each of them processes one particular IP address, we perform the following steps:

- Check the available protocols
- Collect asset and configuration information using the available protocols.

For most devices, JDisc Discovery requires access credentials to obtain information from endpoints using protocols such as WMI (Window Management Instrumentation), SMB, or SSH/telnet. On Windows devices, WMI and SMB are the most important protocols and both require authentication. Most customers use a dedicated scan account (where the access credentials are stored within CyberArk). JDisc Discovery can associate the CyberArk account with a Windows domain or AD organizational unit. So when our protocol check determines that a Windows device is part of a particular domain or OU, then it can use the associated CyberArk credential definition (consisting of CyberArk server address, safe name, and object name). So before checking the protocol, JDisc Discovery uses the CyberArk API to obtain the current associated access credentials (username/password) in order to connect to the endpoint.

For Unix and VMware servers, JDisc Discovery can be configured with a set of default accounts to test the SSH connection with. In addition to provide the username/password directly in JDisc Discovery, we can associate the account with a CyberArk account and then we will also query the current username/password at runtime from via the API.

The retrieval is always triggered by a device scan. Whenever we need access to an endpoint, then we query the CyberArk server for the current access credentials. There are typically 2-5 CyberArk queries while scanning a device. A device scan usually takes about 3-10 minutes depending on the speed or load on the target endpoint.

When there is no scan, then there will be no requests via the API.

REQUIREMENTS

There are no special requirements except that the JDisc Discovery server needs HTTPS access to the CyberArk server.

AAM INSTALLATION

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

AAM CONFIGURATION

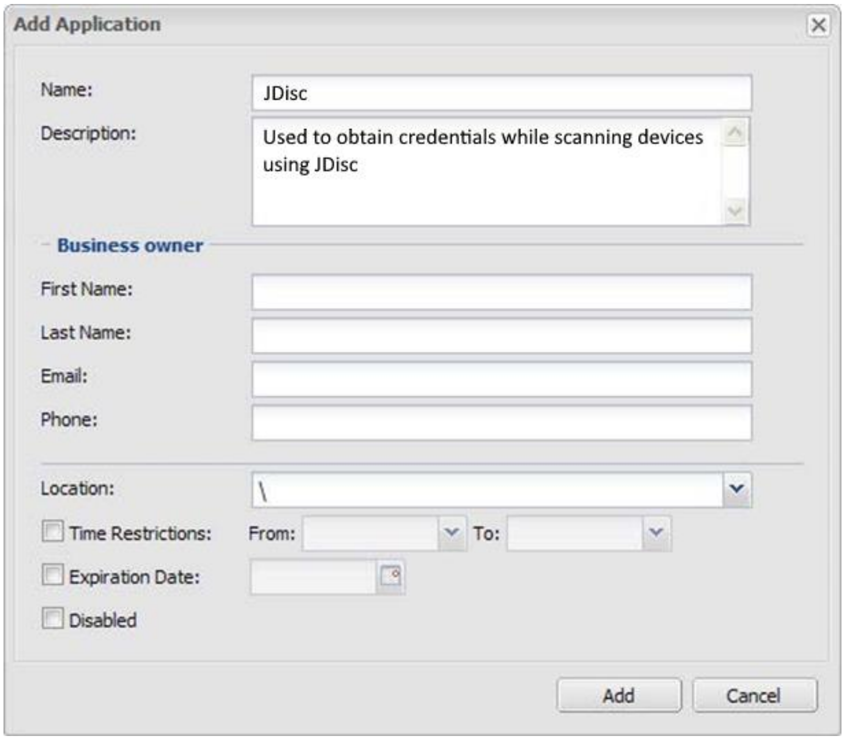
The following sections provide details on JDisc Discovery configuration with CyberArk AAM.

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.

We do not have an specific requirements for the APPID. So any name can be used.



Add Application

Name: JDisc

Description: Used to obtain credentials while scanning devices using JDisc

Business owner

First Name:

Last Name:

Email:

Phone:

Location: \

□ Time Restrictions: From: To:

□ Expiration Date:

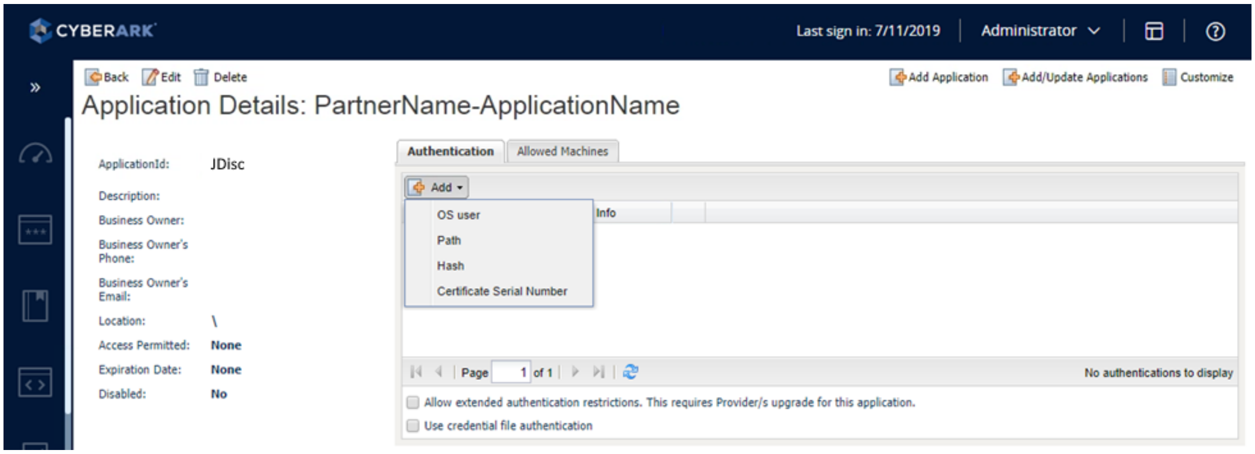
□ Disabled

□ Specify the following information:

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

ApplicationId: JDisc
Description:
Business Owner:
Business Owner's Phone:
Business Owner's Email:
Location: \
Access Permitted: None
Expiration Date: None
Disabled: No

No authentications to display

□ Allow extended authentication restrictions. This requires Provider/s upgrade for this application.
□ Use credential file authentication

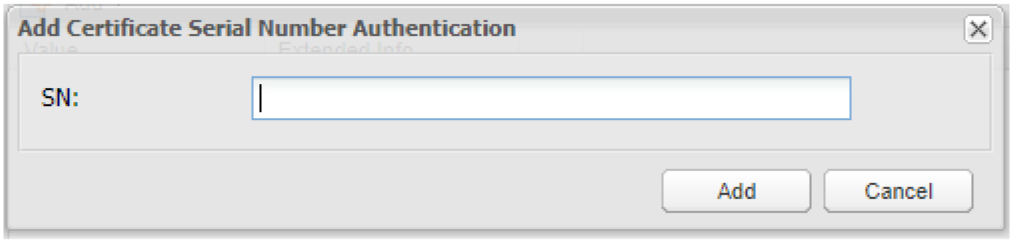
□ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.

□ 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 Certificate Serial Number.

□ Specify the Certificate Serial Number.

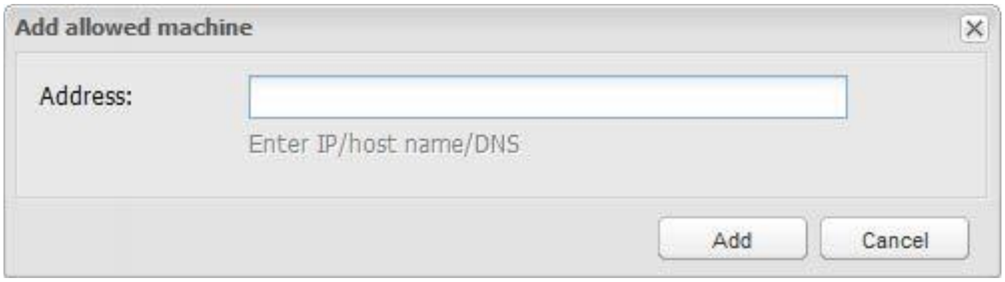


Add Certificate Serial Number Authentication

SN:

□ Specify the application's Allowed Machines. This information enables AAM 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.**

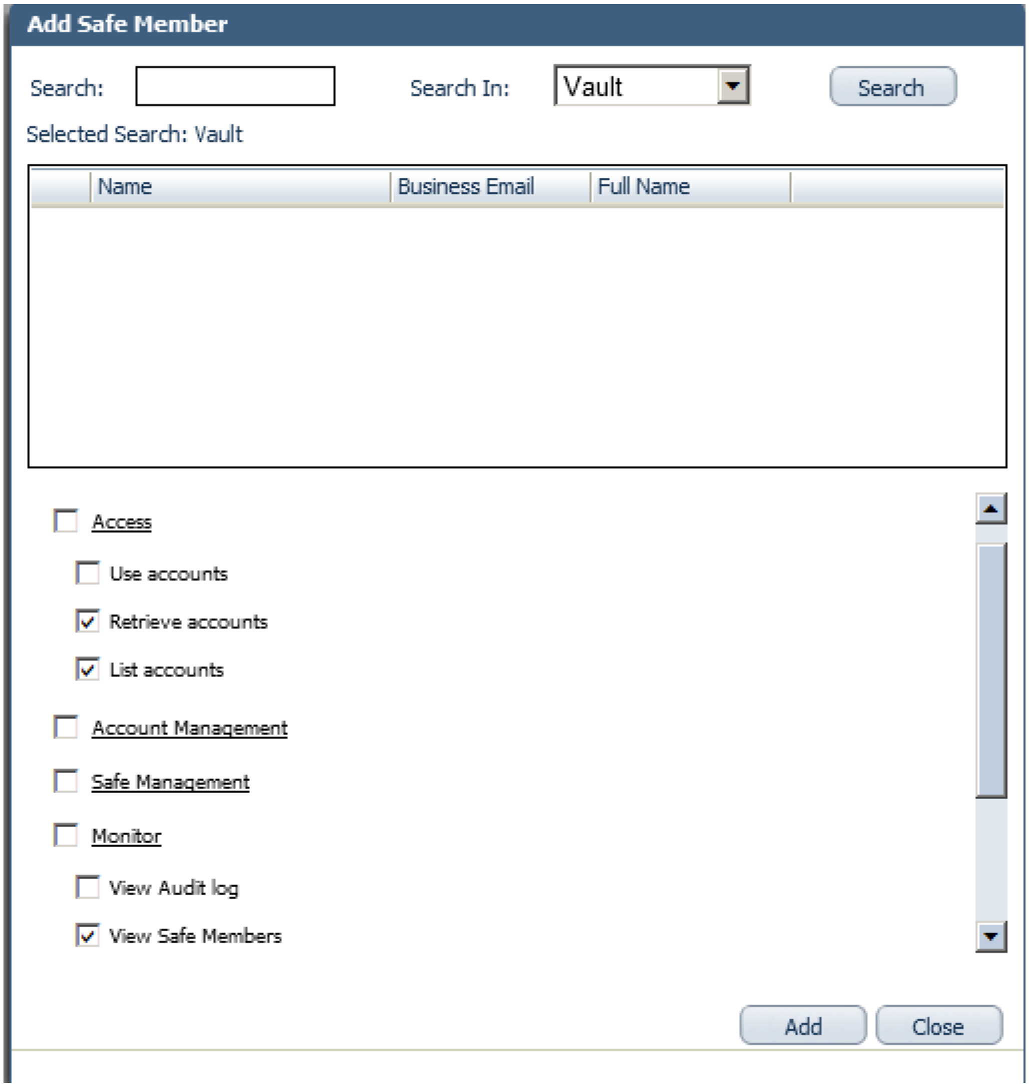
Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

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 Safe Member

Search: Search In: Vault Search

Selected Search: Vault

Name	Business Email	Full Name

□ Access

- □ Use accounts
- ☑ Retrieve accounts
- ☑ List accounts

□ Account Management

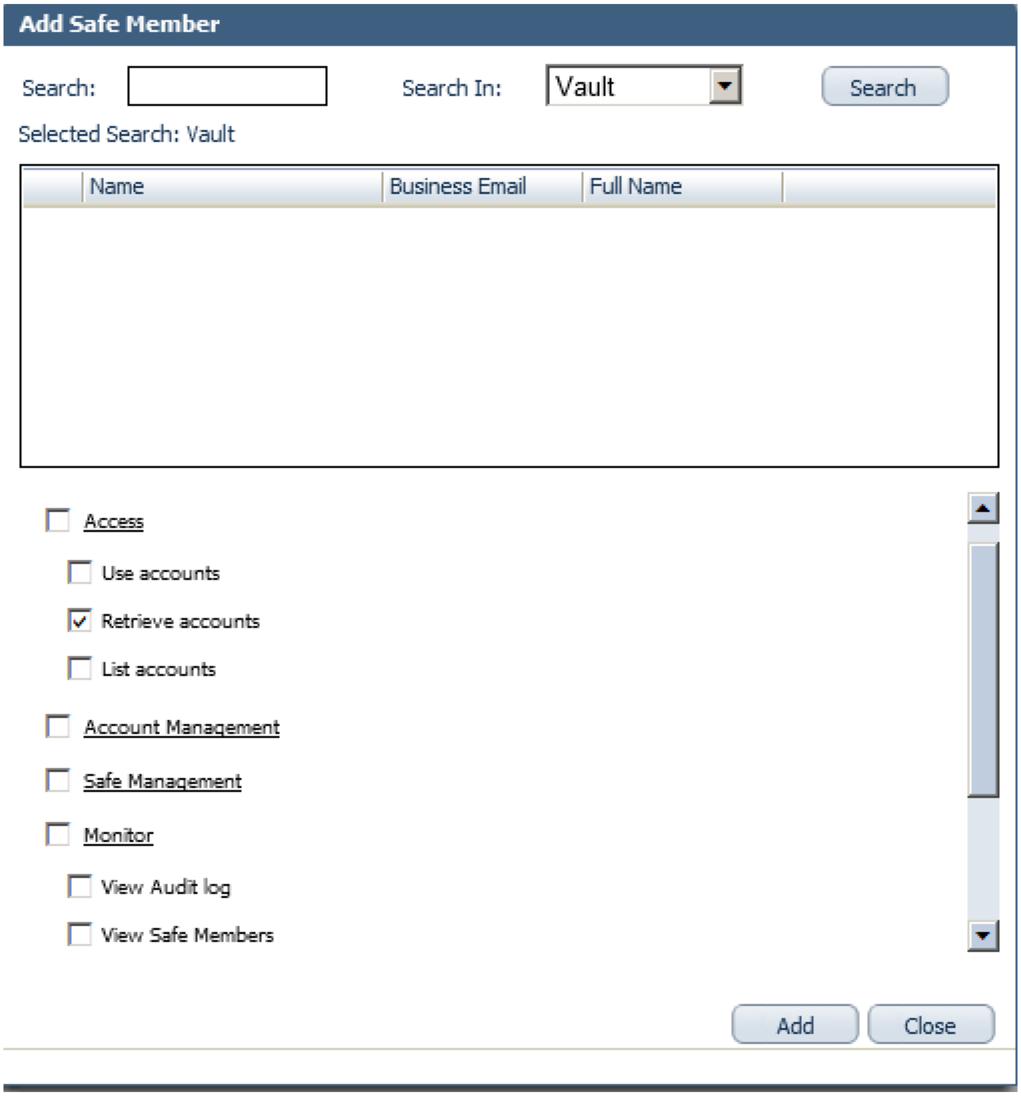
□ Safe Management

□ Monitor

- □ View Audit log
- ☑ View Safe Members

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

- Retrieve accounts



Search In: Vault

Selected Search: Vault

☐ Access

☐ Use accounts

☑ Retrieve accounts

☐ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☐ View Audit log

☐ View Safe Members

☐ 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.**

PARTNER PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

Refer to JDisc Discovery Installation Guide (included in the JDisc Discovery Download) for JDisc Discovery installation.

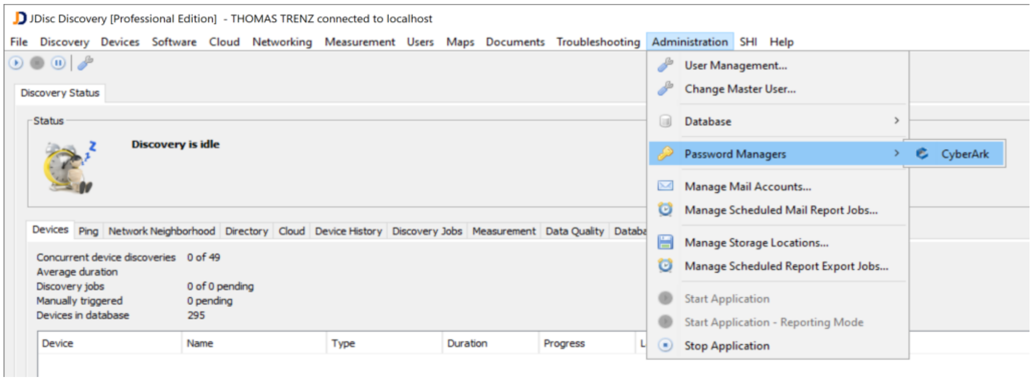
Prerequisites:

- The root certificate for the client certificate must be imported to the global certificate store on the JDisc Discovery server unless it is already there.

Configuration Steps

Once your CyberArk Instance is configured, you have to configure the CyberArk access within the Product Inventory application. Product Inventory can use as many CyberArk servers as needed. Each server instance has its own access credentials and configured application. Follow the steps below in order to add a new CyberArk server instance to Product Inventory's configuration:

Open the CyberArk server configuration dialog via *Administration > Password Managers > CyberArk*.


JDisc Discovery [Professional Edition] - THOMAS TRENZ connected to localhost
File Discovery Devices Software Cloud Networking Measurement Users Maps Documents Troubleshooting Administration SHI Help
Discovery Status
Status
User Management...
Change Master User...
Database
Password Managers
CyberArk
Manage Mail Accounts...
Manage Scheduled Mail Report Jobs...
Manage Storage Locations...
Manage Scheduled Report Export Jobs...
Start Application
Start Application - Reporting Mode
Stop Application
Devices Ping Network Neighborhood Directory Cloud Device History Discovery Jobs Measurement Data Quality Databa
Device Name Type Duration Progress L

Discovery is idle

Concurrent device discoveries 0 of 49
Average duration
Discovery jobs 0 of 0 pending
Manually triggered 0 pending
Devices in database 295

Figure: Open the CyberArk Server Configuration Dialog

This is going to open the CyberArk Server Configuration dialog. The dialog lists all currently configured CyberArk servers.

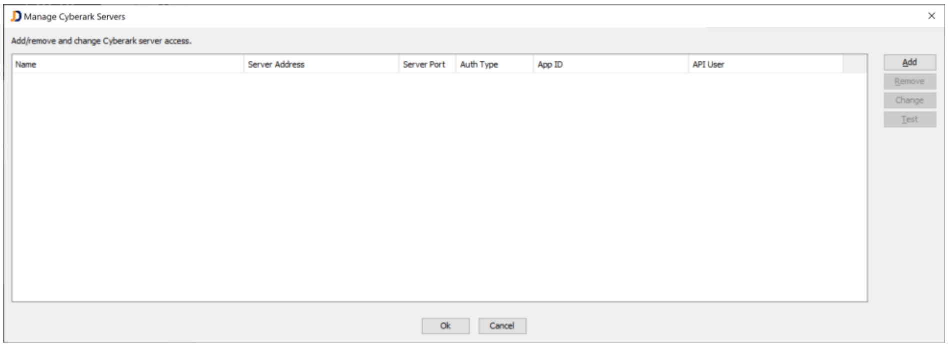
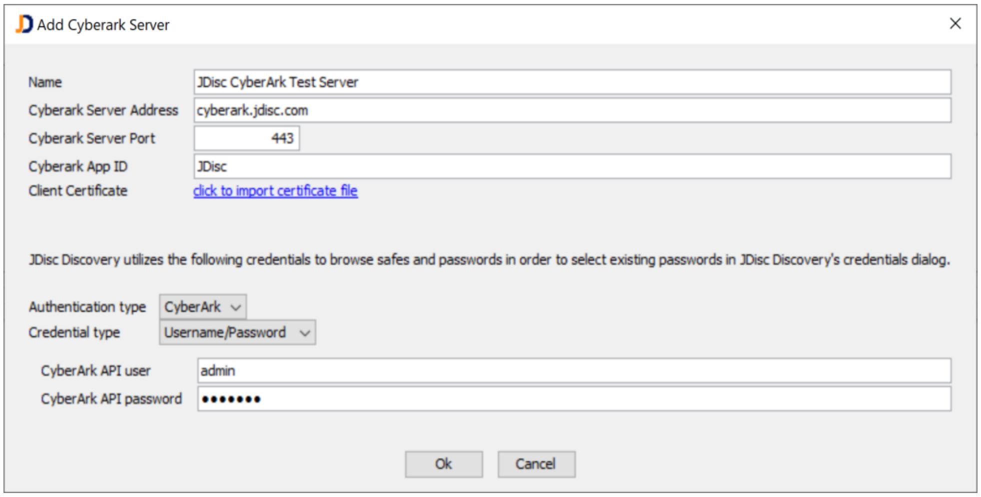


Figure: CyberArk Servers Dialog

Click on the *Add* button in order to add an additional CyberArk server. Then enter a name for the server, the server address (hostname or IP address), the port (default it HTTPS port 443). Finally configure the *application id* configured in the CyberArk preparation.

Furthermore import the client certificate by clicking on the *click to import certificate file*. The file must be in the .p12 format and include the client certificate and the certificate's private key.

❗	The root certificate for the client certificate must be imported into certificate store on the server where Product Inventory is installed.



Name: JDisc CyberArk Test Server
Cyberark Server Address: cyberark.jdisc.com
Cyberark Server Port: 443
Cyberark App ID: JDisc
Client Certificate: click to import certificate file

JDisc Discovery utilizes the following credentials to browse safes and passwords in order to select existing passwords in JDisc Discovery's credentials dialog.

Authentication type: CyberArk
Credential type: Username/Password
CyberArk API user: admin
CyberArk API password: •••••••

Figure: Add a new CyberArk Server Connection

The App-ID and the client certificate is used to retrieve the current credentials. In order to list the CyberArk accounts and the safes, you need to specify an additional user.

Depending on the user configuration within CyberArk, you can choose an authentiction type:

- CyberArk
- Windows
- LDAP
- Radius

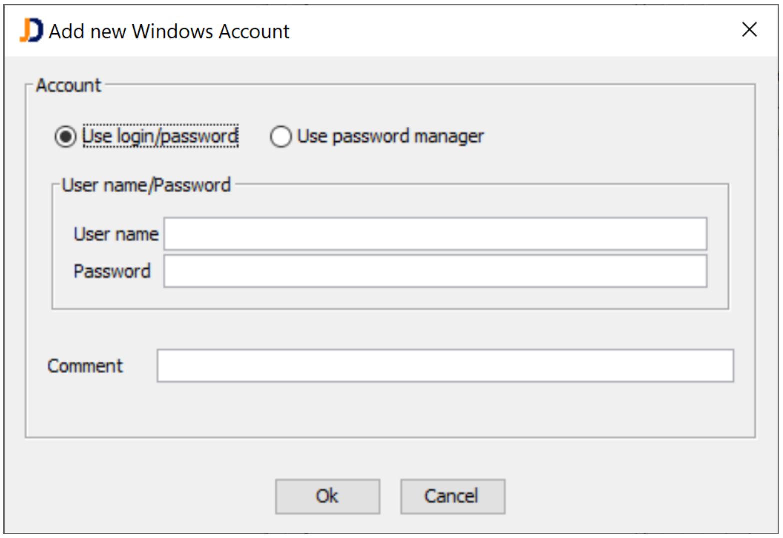
In order to get the username and password for this user, you can specific the username and password directly or you can specify a CyberArk safe and object name to define the credentials.

Finally, you can use the *Test* button to check the connectivity. In order to check the connectivity, you need to provide a safe and object name to test the access with.

4.12.3 Using CyberArk Accounts

Once the connection has been established successfully, you can use CyberArk accounts from virtually anywhere where you configure access credentials (just a few exceptions).

All credential dialogs supporting password managers have now a radio button to choose whether you would like to enter a username/password combination or whether you would like to choose credentials managed by a password manager.



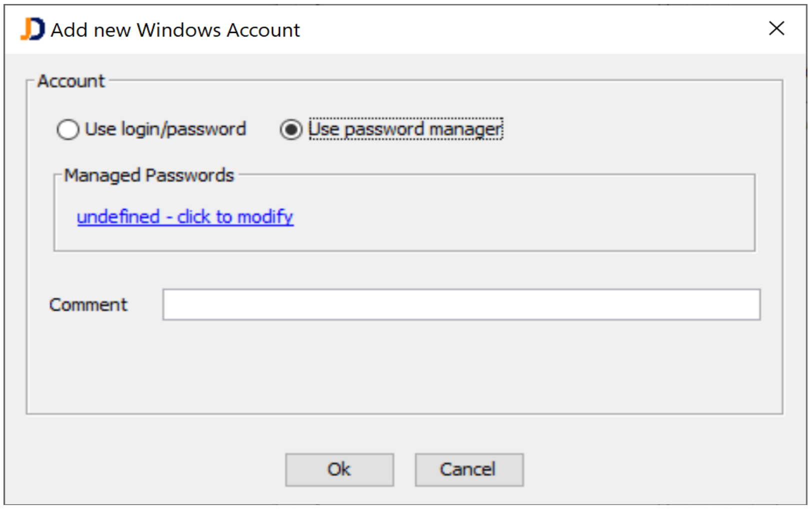
Add new Windows Account

Account

● Use login/password ○ Use password manager

Figure: Credential Dialog supporting Password Managers

Either enter a username and password or select the *User password manager* radio button in order to select credentials managed by a password manager.



Add new Windows Account

Account

○ Use login/password ● Use password manager

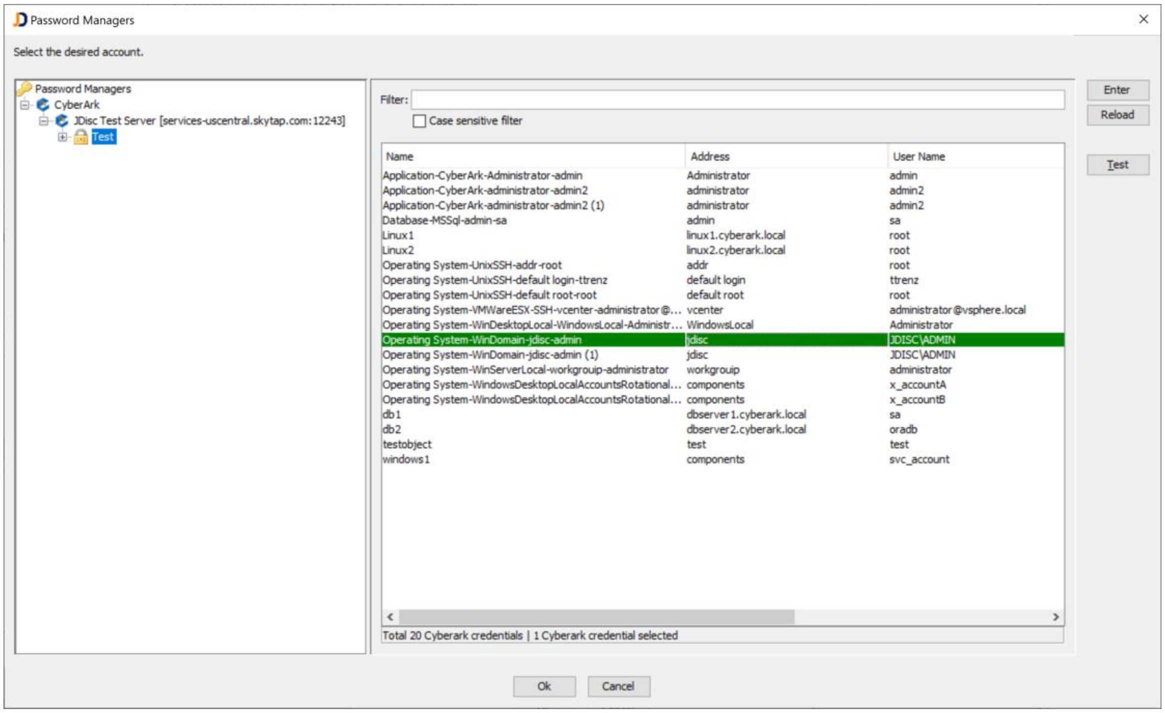
Managed Passwords

undefined - click to modify

Figure: Select Password Manager Credentials

The *Managed Passwords* area contains the selected password from a password manager. Click on the *undefined – click to modify* link in order to select the desired credentials.

This will open a selection dialog where you can see the configured password managers on the left and once you select a safe the list of the actual passwords on the right side.



Select the desired account.

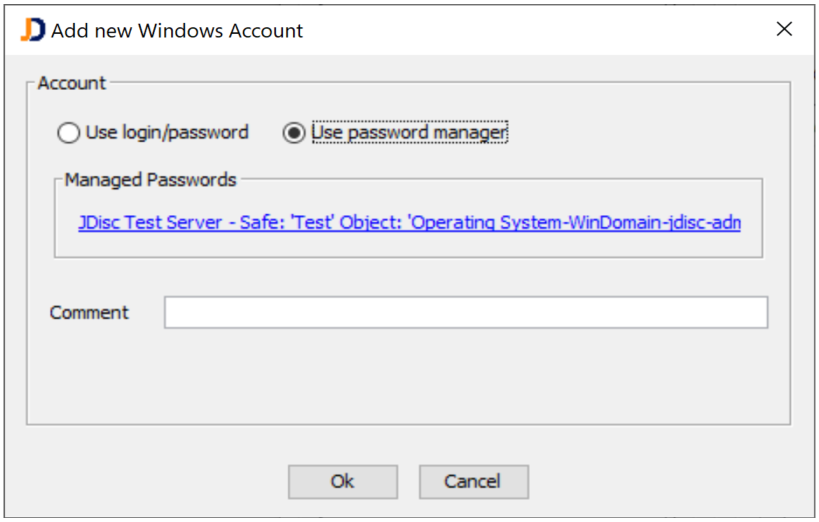
□ Case sensitive filter

Name	Address	User Name
Application-CyberArk-Administrator-admin	Administrator	admin
Application-CyberArk-administrator-admin2	administrator	admin2
Application-CyberArk-administrator-admin2 (1)	administrator	admin2
Database-MSSql-admin-sa	admin	sa
Linux1	linux1.cyberark.local	root
Linux2	linux2.cyberark.local	root
Operating System-UnixSSH-addr-root	addr	root
Operating System-UnixSSH-default login-ttrenz	default login	ttrenz
Operating System-UnixSSH-default root-root	default root	root
Operating System-VMWareESX-SSH-vcenter-administrator@…	vcenter	administrator@vsphere.local
Operating System-WinDesktopLocal-WindowsLocal-Administr…	WindowsLocal	Administrator
Operating System-WinDomain-jdisc-admin	jdisc	JDISC\ADMIN
Operating System-WinDomain-jdisc-admin (1)	jdisc	JDISC\ADMIN
Operating System-WinServerLocal-workgrouip-administrator	workgrouip	administrator
Operating System-WindowsDesktopLocalAccountsRotational…	components	x_accountA
Operating System-WindowsDesktopLocalAccountsRotational…	components	x_accountB
db1	dbserver1.cyberark.local	sa
db2	dbserver2.cyberark.local	oradb
testobject	test	test
windows1	components	svc_account

Total 20 Cyberark credentials | 1 Cyberark credential selected

Figure: Select the desired Credentials

Finally, the credentials dialog displays the password name.



○ Use login/password ● Use password manager

JDisc Test Server - Safe: 'Test' Object: 'Operating System-WinDomain-jdisc-adn

Figure: The selected Credentials

From now on, the discovery will use this account and query the current username and password from the CyberArk server when the account is needed.

PARTNER CONTACT INFO

Business Contact	Name	Thomas Trenz
	Email	thomas.trenz@jdisc.com
	Tel	+49 7034 99921041
Technical Contact	Name	Thomas Trenz
	Email	thomas.trenz@jdisc.com
	Tel	+49 7034 99921041
Support Contact	Name	JDisc Support
	Email	support@jdisc.com
	Tel	+49 7034 99921041