



CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Active Navigation

Website: www.activenavigation.com

Name of Product: Discovery Center

Version: 4.6.0

Date: 20 November 2018 (Revised 19 October 2020)

DISCOVERY CENTER OVERVIEW

Discovery Center is a proven market-leading file analysis software for content discovery, compliance, tagging, and ongoing governance. It provides consistent and repeatable analysis across file shares, SharePoint, Exchange, Office 365, Cloud Storage Gateways, OpenText Content Server, and other connected repository types.

Discovery Center indexes and manages unstructured content in place across any connected repository, including defensible deletion, reorganization, or quarantining. It manages customizable metadata schemas, visualizes and explores content at scale, and records activity history and auditing. It also applies business classifications, taxonomies, and policies.

Discovery Center is capable of scalable textual content analysis to tag and classify documents using any combination of keywords, patterns, proximity and thematics.

Despite its low footprint, it is capable of analyzing hundreds of Terabytes of content with low network impact.

Version: 4.6.0

Discovery Center can be installed on the Microsoft stack (Windows Server, IIS, SQL Server, .NET Framework) in either a physical or virtual environment. Discovery Center is certified for Azure Marketplace.

KEY BENEFITS

Discovery Center supports content compliance, governance, and migration by:

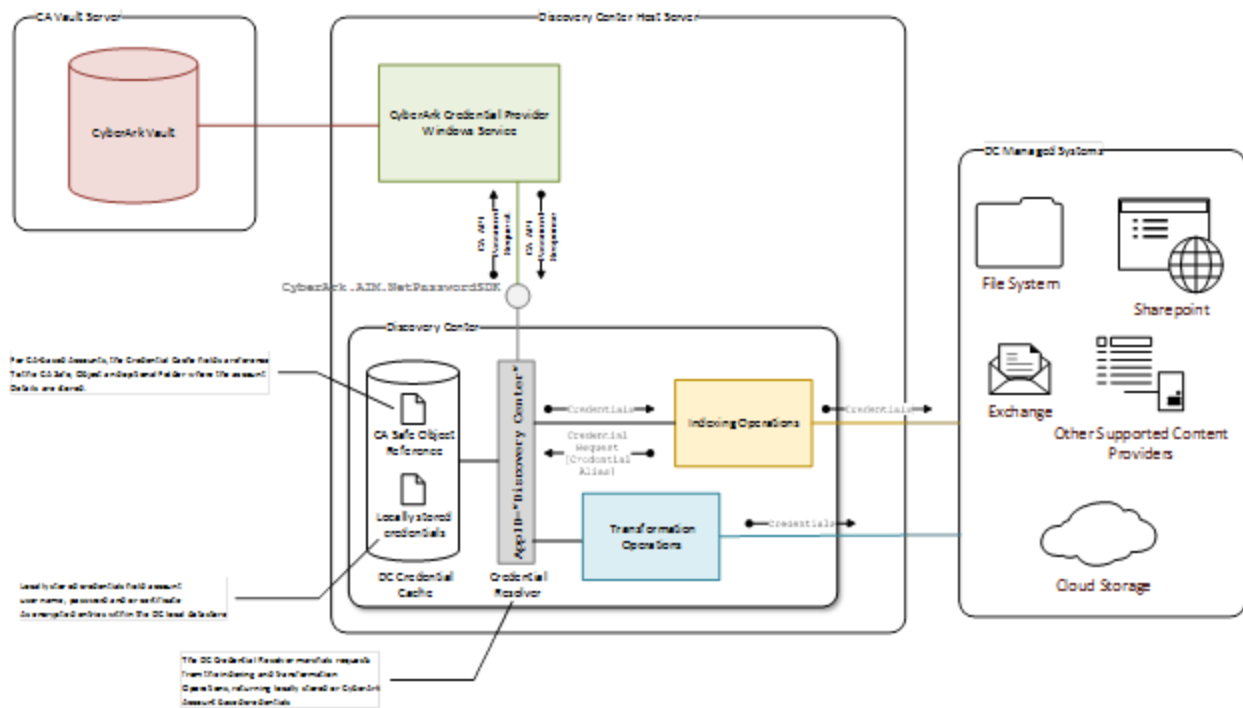
- Reducing the risk and cost of storing unstructured content and managing digital landfill
- Keeping content compliant by providing in-place monitoring with user impact
- Adding value to migrated content by efficiently analyzing, classifying, and tagging content

By adding support for CyberArk Secrets Manager, Discovery Center will be able to delegate its credential management to a dedicated, enterprise-level password vault and seamlessly align with the host organization's access security policies.

CyberArk Secrets Manager will reduce the overhead required to define, update, and retire credential information directly in Discovery Center, reducing the risk of unauthorized access or failure to access permitted content. CyberArk's encryption, account management and auditing capabilities will also provide a greater level of account security than can be achieved within the Discovery Center environment alone.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

Discovery Center is a server-based application that interrogates, indexes, and optionally transforms unstructured content across supported data stores accessible to the host server.



SECRETS MANAGER INTEGRATION

The Discovery Center application runs as a set of Windows processes orchestrated by a Scheduler Windows service. These processes encapsulate a number of operations that index, analyze and optionally transform data on the target data stores.

Discovery Center is designed to operate within a customer's existing system architecture, including their existing CyberArk configuration.

Discovery Center offers an optional integration with the CyberArk Secrets Manager solution to delegate the storage of the account details used by Discovery Center to access protected data stores.

CREDENTIAL RETRIEVAL

In many cases, access to a target data store is restricted by user account or certificate authentication and authorization mechanisms. In order to process the content held in restricted data stores, Discovery Center can hold preconfigured matching account details (Credentials), in its local Credential Cache. Discovery Center Credentials encapsulate the account details required to access a restricted data store. Each Credential is identified by a unique Alias.

When configuring a target data store for Discovery Center, a user will first define a set of Credentials and then assign these to the data stores that require some form of authentication and authorization to grant access. If an operation requires some form of credential to access a data store, it retrieves the required account details or certificate through the Discovery Center Credential Resolver component.

The Discovery Center Credential Cache supports basic (username and password) and certificate-based credentials. In both cases, the credentials are stored as encrypted fields in Discovery Center's local SQL Server Database.

When Discovery Center's CyberArk Secrets Manager interface is enabled, the Credential Cache may alternatively store a reference to the CyberArk location where the actual credential details are stored. Instead of retrieving the credentials directly from the Cache, Discovery Center uses the CyberArk location information to request the account details from CyberArk through the locally installed CyberArk Credential Provider service. The credentials to be used by Discovery Center to access the target data store are then constructed from the account details, including the password, and returned from CyberArk.

REQUIREMENTS

The minimum server configuration to host only Discovery Center is 64bit quad core with 4Gb RAM and 100GB disk storage, plus additional space for application data. Discovery Center's SQL Server and SSAS instances should also be hosted on a machine with similar capabilities. If Discovery Center, SQL Server, and SSAS are installed on the same server, the specifications for the host server will need to increase proportionally. See the Discovery Center Installation Guide for more details.

SECRETS MANAGER INSTALLATION

Secrets Manager Installation - https://docs.cyberark.com/Product-Doc/OnlineHelp/AAM-CP/Latest/en/Content/CP%20and%20ASCP/installing-the-Credential-Provider.htm?tocpath=Installation%7CCredential%20Provider%7CInstall%20the%20Credential%20Provider%7C_0

SECRETS MANAGER CONFIGURATION

The following sections provide details on Discovery Center 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.

Add Application

Name: Discover Center

Description: Active Navigation Discovery Center Application

Business owner

First Name: Jane

Last Name: Doe

Email: j.doe@company.com

Phone:

Location: \

☐ Access Permitted: From: To:

☐ Expiration Date:

☐ Disabled

Add Cancel

- ☐ Specify the following information:
- In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: Discover Center
 - In the **Description** box, specify a short description of the application that will help you identify it.
 - In the **Business owner** section, specify contact information about the application's business owner.
 - In the **Location** box, specify the location of the application in the Vault hierarchy. If a location is not selected, the application will be added in the same location as the user who is creating this application.
- ☐ Click **Add**. The application is added and is displayed in the Application Details page.

- ☐ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.
- ☐ Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password. These details are optional and will depend on how Discovery Center is installed and configured on the host machine.
- ☐ In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.
- ☐ Select the authentication characteristic to specify.
- ☐ Select **OS user**. The Add Operating System User Authentication window appears.

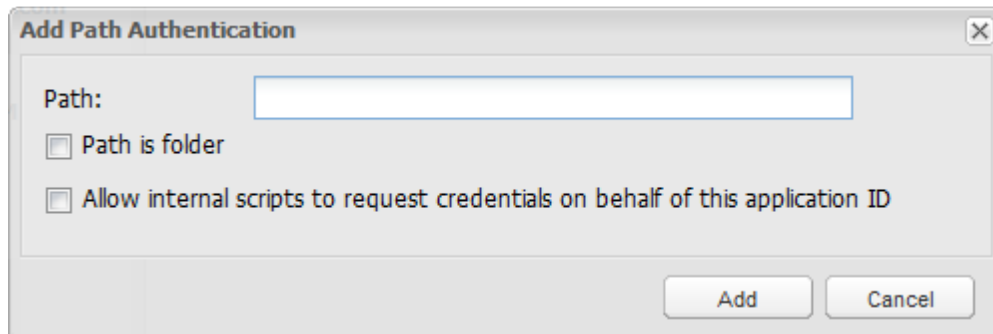
- ☐ Specify the name of the OS user who will run the application, then click **Add**. The OS user is listed in the Authentication tab.
- ☐ Specify the application path. Discovery Center processes run from a number of locations. For a default installation, you will need to include the following folders:

```
\Program Files (x86)\Active Navigation\Discovery Center\Scheduler
\Program Files (x86)\Active Navigation\Discovery Center\Skimmer
\Program Files (x86)\Active Navigation\Discovery Center\Analysis
```

The paths must also include the Discovery Center Web Application path. By default, this will be

\\inetpub\\wwwroot\\AN40web

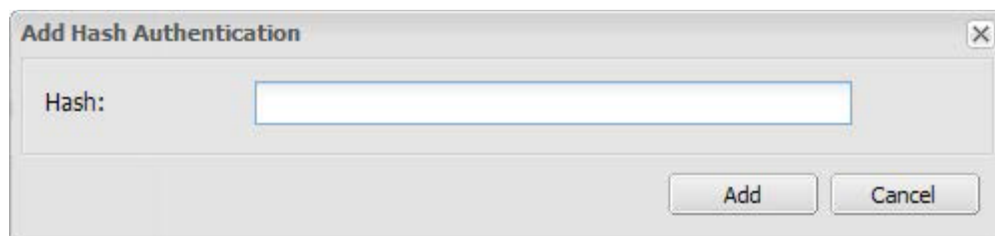
- ☐ Select **Path**. The Add Path Authentication window appears.

The 'Add Path Authentication' dialog box has 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 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 are 'Add' and 'Cancel' buttons.

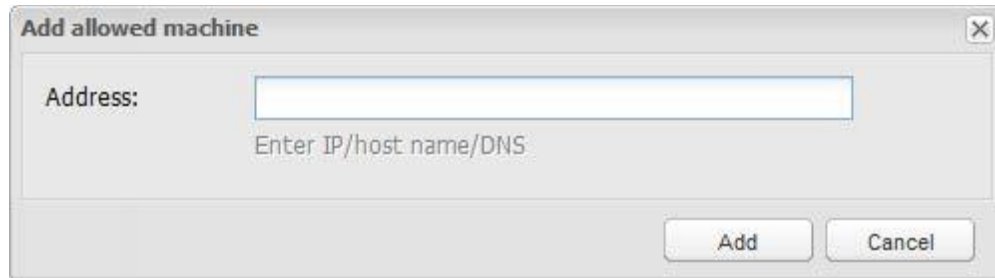
- In the Hash edit box, paste the application's unique hash value, or specify multiple hash values with a semi-colon. You can add additional information in a comment after each hash value specified for an application by specifying '#' after the hash value, followed by the comment.

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". 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

10

Add Safe Member

Search: Search In:

Selected Search: Vault Display 1 result(s)

Name	Business Email	Full Name
 Discovery Center	j.doe@company....	Jane Doe

☐ Access

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

☐ Account Management
☐ Safe Management
☐ Monitor

- ☐ View Audit log
- ☐ View Safe Members

Discovery Center 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**.

DISCOVERY CENTER INSTALLATION & INTEGRATION CONFIGURATION

Refer to the Discovery Center Installation Guide for Discovery Center installation.

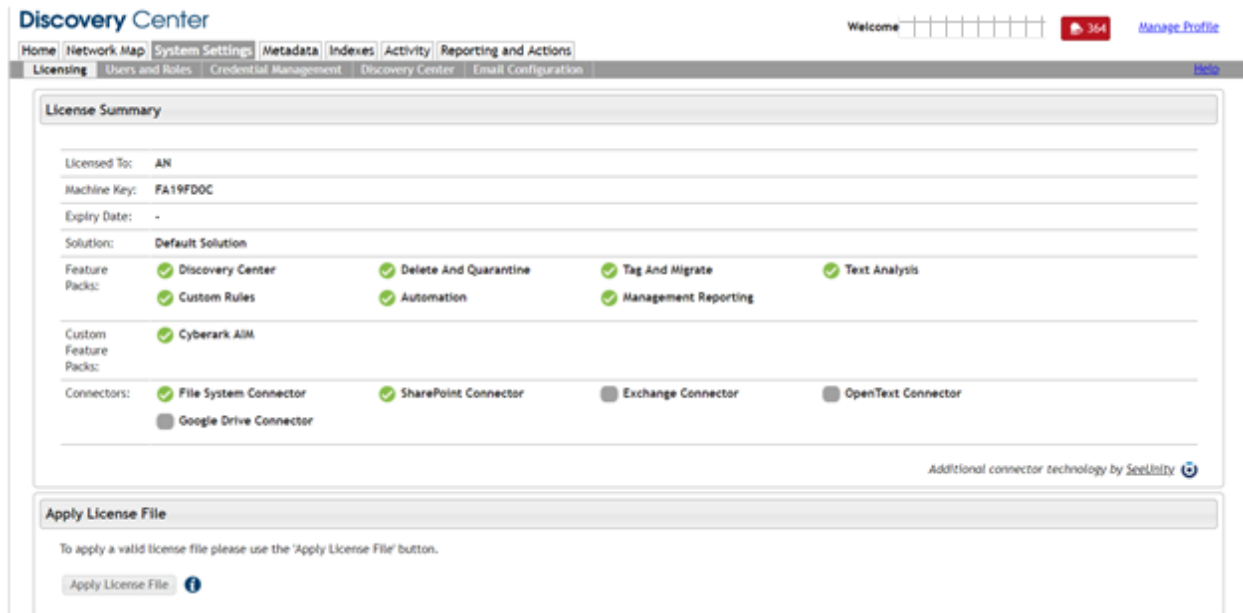
Discovery Center does not require any specific installation or integration steps to install the CyberArk Secrets Manager interface. The CyberArk interface is a licensed feature and will only be available to users with the 'CyberArkAAM' feature enabled.

To enable the CyberArk Secrets Manager feature, first contact Active Navigation to obtain a new license file. To install or update the license:

- Open Discovery Center in a browser.
- Using the navigation tags at the top of the page, go to System Settings -> Licensing
- Click on the 'Apply License' button

In the dialog, navigate to the folder containing the xml license file, select it and then click 'Open'. The license will update.

If successful, the License Summary pane will list 'CyberArk AIM' in the 'Custom Feature Packs' section. The 'CyberArk AIM' option will now be available when defining Discovery Center Credentials.



Once licensed, CyberArk credentials can be defined in the same way as the other credential types supported by Discovery Center:

- Navigate to the **System Settings > Credential Management** tab
- Click **Add** to add a new Credential definition
- In the **Credential Dialog**, select 'CyberArk AIM' in the **Credentials Type** dropdown.
- Enter the **Credential Alias** (the common term used to identify the credential definition within Discovery Center) and a description if needed.
- Enter the Safe, folder, and ObjectName where the credentials reside on the CyberArk vault.
- Click **Save** to store the CyberArk Credential definition.

Add Credential

Credentials Type:

CyberArk AIM

Alias:

Access to Data Folder on Server ABC

Description:

These are demo credentials

Safe:

FileSystemPwsSafe

Folder:

Object:

Server_ABC

Save

Cancel

See the Discovery Center User Guide for a detailed description of Discovery Center’s Credential Management function and how this integrates with CyberArk AIM.

PARTNER CONTACT INFO

Business Contact	Name	Analisa Scott (Partner Manager)
	Email	analisa.scott@activenavigation.com
	Tel	(717) 982-5226
Technical Contact	Name	Abel Palustre
	Email	abel.palustre@activenavigation.com
	Tel	(571) 346-7607
Support Contact	Name	Abel Palustre
	Email	abel.palustre@activenavigation.com
	Tel	(571) 346-7607