

IBM **Automation**



APPLICATION ACCESS MANAGER

AAM INTEGRATION - TECHNICAL DOCUMENTATION TEMPLATE

IBM Content Manager

8.6.3

06/24/2020

PARTNER SOLUTION OVERVIEW

The main components of the IBM Content Manager 8.6.3 (Windows, AIX, and Linux) system include a library server, one or more resource managers, and a set of object-oriented application programming interfaces (APIs). To administer your IBM Content Manager system, you are also provided with a Java-based system administration client.

IBM Content Manager 8.6.3 (Windows, AIX, and Linux) provides Java application programming interfaces (APIs), which are the building blocks for creating applications that access Content Manager Data.

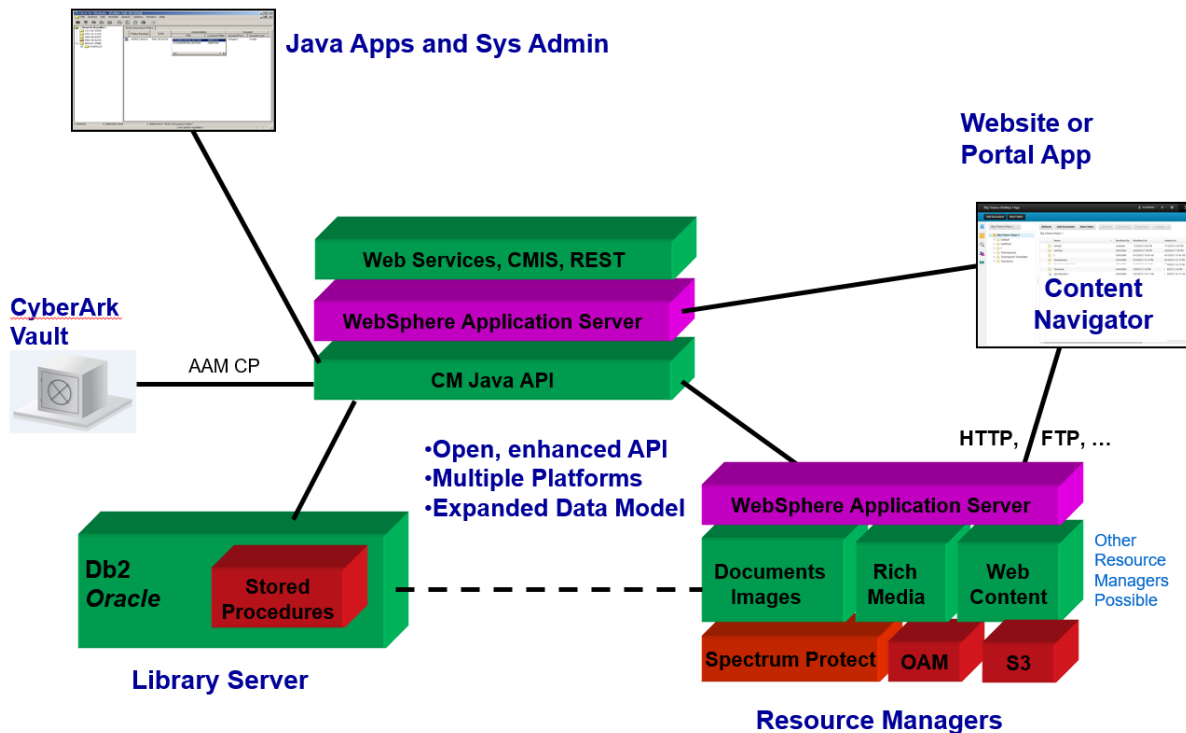
KEY BENEFITS

IBM Content Manager Enterprise Edition is a complete solution for storing and retrieving documents. IBM Content Manager Enterprise Edition features multi-operating system support, client options, and administration tools including document routing to manage the flow of work through the system.

IBM Content Manager Enterprise Edition provides a flexible system that you can use to manage unstructured content according to the needs of your business. Content Manager Enterprise Edition also provides a complete solution to the problem of storing and retrieving documents in almost any format.

The Content Manager API, starting in version 8.6 fix pack 3, includes the infrastructure to provide a credential vault user exit. An exit can be implemented to map CyberArk login information to the actual database user id and password that are used by Content Manager. With this integration, CyberArk is the credential vault for IBM Content Manager database user ids and passwords for the IBM Content Manager system. With the CM API integration, any application that uses the CM API can be configured to use CyberArk.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



A Content Manager credential vault user exit is the location of the integration between Content Manager and CyberArk. This exit is implemented in the CM Java API. Any application that uses the CM Java API may take advantage of this integration. This includes the Content Manager system administration client and IBM Content Navigator.

Note that Content Manager does not support using CyberArk for database user ids that are used for installation and configuration of the product. When running the product install and configuration, a real database user id and password must be used. Content Manager does not support using CyberArk with database user ids that are used in WebSphere Application Server data sources. To use CyberArk for these data sources, contact the WebSphere Application Server product to discuss integration.

The Credential retrieval is triggered whenever a connection is made to Content Manager using the Content Manager API to get database logon information. When an application connects to the Content Manager system using the Java API, the API will check if the exit is configured. If it is, the exit is loaded and called with the user id of the caller and the CyberArk configuration information. The exit then calls CyberArk Java password SDK to get the real database user id and password. This is then returned to the CM API, which uses the database userid and password to connect to the database.

Note that if the CM API is configured to use WebSphere Application Server JDBC connection pooling, the exit is not applied. In this case, CyberArk integration must be applied to the WebSphere Application Server data source.

AAM INSTALLATION

Refer to the “Credential Provider and ASCP Implementation Guide” for CyberArk Agent based

List specific steps to configuring AAM Provider with Partner Product.

To use the CyberArk integration with the Content Manager Java API, do the following:

1. Download the sample CyberArk exit from <https://www.ibm.com/support/pages/node/6116272> .
2. Customize the Java code for the sample exit as needed
3. Compile the exit code into a jar file and include in the classpath of the application that will use the CM API integration
4. Update the cmbicmsrvs.ini file to enable the use of the exit
5. Run your application to test the integration

For more details on configuring and using the CyberArk exit in different scenarios, see <https://www.ibm.com/support/pages/node/6116272>. Here we provide the exact configuration needed in different scenarios.

AAM CONFIGURATION

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

To define the Application, here are the instructions to define it manually via CyberArk’s PVWA (Password Vault Web Access) Interface:

1. Logged in as user allowed to managed applications (it requires Manage Users authorization), in the Applications tab, click **Add Application**; the Add Application page appears.

Add Application

Name: IBM_CM8-Appl

Description:

Business owner

First Name:

Last Name:

Email:

Phone:

Location:

☒ Access Permitted: From: To:

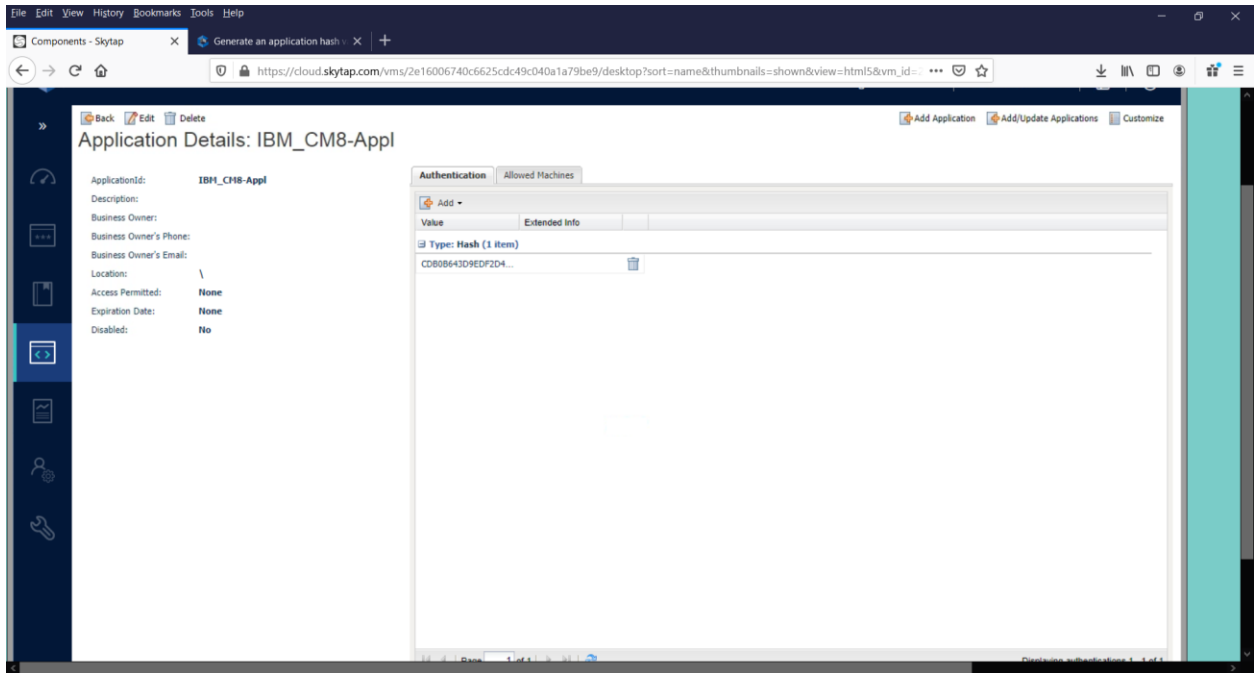
☐ Expiration Date:

☐ Disabled

Add Cancel

2. Specify the following information: ^{SEP}
 - In the Name edit box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: ^{SEP} APP ID = IBM_CM8-Appl
 - In the Description, 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 lowest section, 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.
3. Click **Add**; the application is added and is displayed in the Application Details page. The administrator manually adds the unique hash generated by the JavaAIMGetAppInfo utility to

the Authentication tab.



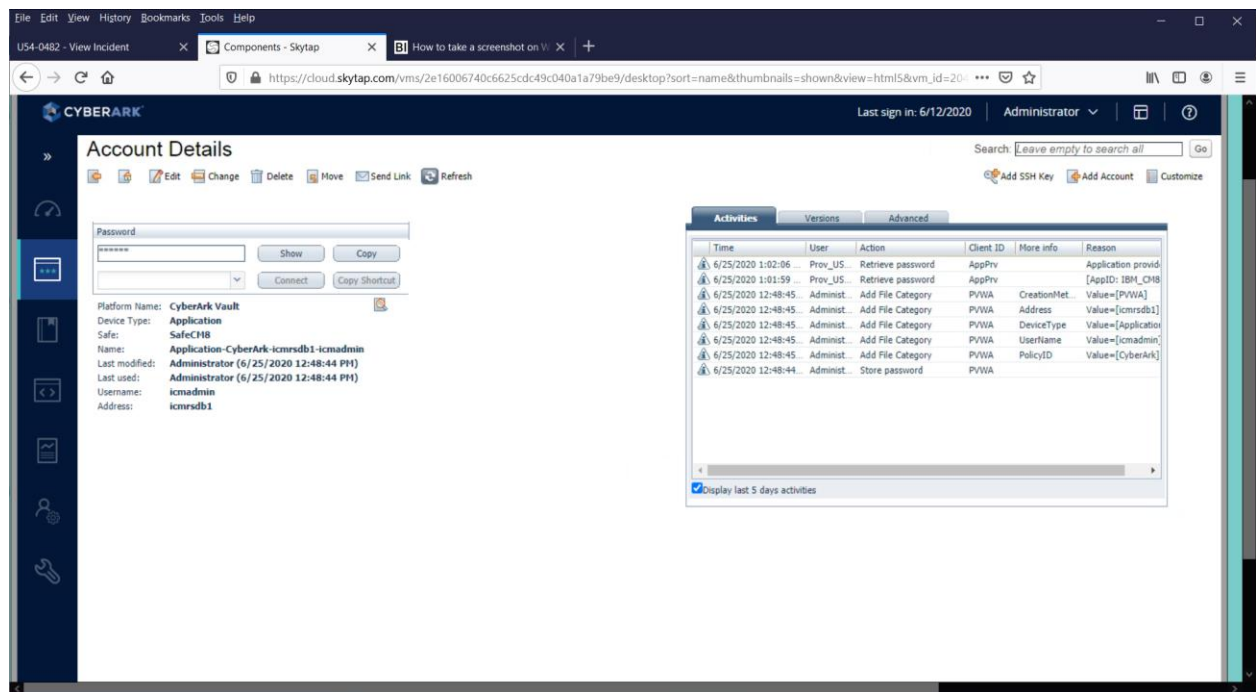
PROVISIONING ACCOUNTS AND SETTING PERMISSIONS FOR APPLICATION ACCESS

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 (Step 1). 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 (Step 2).

1. 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**.



2. 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 accounts for Content Manager database usersids/passwords (icmadmin, icmconct).

File Edit View History Bookmarks Tools Help

US4-0482 - View Incident Components - Skytap BI How to take a screenshot on V...

https://cloud.skytap.com/vms/2e16006740c625cdc49c040a1a79be9/desktop?sort=name&thumbnails=shown&view=html5&vm_id=20...

CYBERARK Last sign in: 6/12/2020 Administrator

Add Account

Store in Safe: SafeCH8

Device Type: Application

Platform Name: CyberArk Vault

Required Properties:

Username: icmadmin

Address: icmsdb1

Optional Properties:

☐ Port:

☐ Timeout:

☐ Reconnect Period:

☐ Proxy Type: [Select]

☐ Proxy Address:

☐ Proxy Port:

☐ Proxy Authentication:

☐ Domain:

☐ Proxy User:

☐ Proxy Password:

☐ Behind Firewall: [Select]

☐ Use Only HTTP: [Select]

Password Context

Password: [Masked]

Confirm Password: [Masked]

Name: ☒ Auto-generated (Name pattern: DeviceType-PolicyID-Address-Username-vty-DSW-ServiceName-TaskName-SystemNumber-Client) ☐ Custom

☐ Disable automatic management for this account

Reason: [Text Field]

Save Cancel

File Edit View History Bookmarks Tools Help

US4-0482 - View Incident Components - Skytap BI How to take a screenshot on V...

https://cloud.skytap.com/vms/2e16006740c625cdc49c040a1a79be9/desktop?sort=name&thumbnails=shown&view=html5&vm_id=20...

CYBERARK Last sign in: 6/12/2020 Administrator

Add Account

Store in Safe: SafeCH8

Device Type: Application

Platform Name: CyberArk Vault

Required Properties:

Username: icmconnect

Address: icmsdb1

Optional Properties:

☐ Port:

☐ Timeout:

☐ Reconnect Period:

☐ Proxy Type: [Select]

☐ Proxy Address:

☐ Proxy Port:

☐ Proxy Authentication:

☐ Domain:

☐ Proxy User:

☐ Proxy Password:

☐ Behind Firewall: [Select]

☐ Use Only HTTP: [Select]

Password Context

Password: [Masked]

Confirm Password: [Masked]

Name: ☒ Auto-generated (Name pattern: DeviceType-PolicyID-Address-Username-vty-DSW-ServiceName-TaskName-SystemNumber-Client) ☐ Custom

☐ Disable automatic management for this account

Reason: [Text Field]

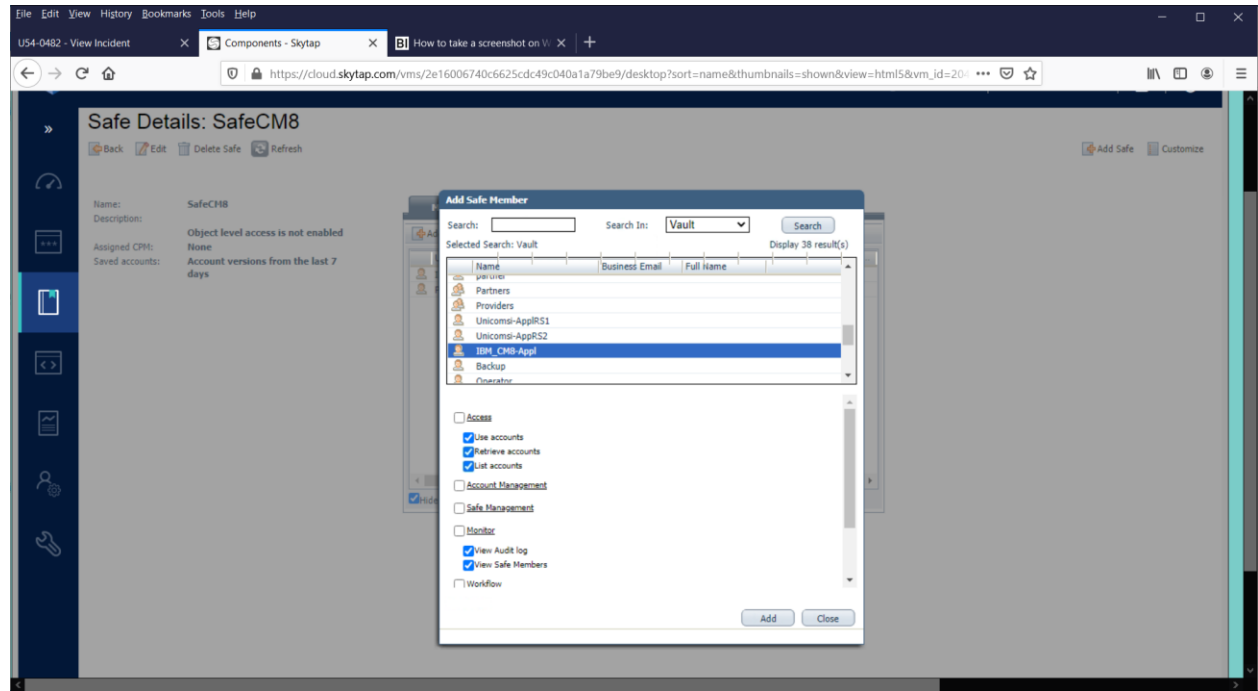
Save Cancel

i. 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.

- ii. Add the application(the APPID) as a Safe Member with the following authorizations:
 - Add Safe Member



- iii. If your environment is configured for dual control:
 - In Privileged Account Security solutions (v8.0 and higher), when working with dual control, the Provider user can always access without confirmation, thus, it is not necessary to set this permission.
- iv. 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 Sample CyberArk credential vault user exit integration with Content Manager Java Connector API for Partner Product installation.

<https://www.ibm.com/support/pages/node/6116272>

PARTNER CONTACT INFO

Business Contact	Name	Neil Parrott
	Email	nparrott@us.ibm.com
	Tel	
Technical Contact	Name	Randy Richardt
	Email	Randy.Riachardt@unicomsi.com
	Tel	
Support Contact	Name	Randy Richardt
	Email	Randy.Riachardt@unicomsi.com
	Tel	