



SECRETS MANAGER INTEGRATION

(Agentless Central Credential Provider CCP)

AAM INTEGRATION - TECHNICAL DOCUMENTATION TEMPLATE

Name of Company: Metric Insights

Website: <https://www.metricinsights.com/>

Name of Product: Metric Insights

Version: 6.3.0

Date: 08.20.2021

PARTNER SOLUTION OVERVIEW

Metric Insights is the leading BI Portal solution. Connect to all your BI tools, databases, and operational systems to give users a single point of access to their BI. Automated anomaly detection and enterprise distribution ensure users know about the right data at the right time and never miss critical events again.

Version: 6.3.0

Platform components:

- Single-server Docker deployment:
 - 6 services: *web* (UI), *data analyzer*, *dataprocessor*, *seed*, *monitoring*, *MySQL*
- Deployment in orchestrated environments:
 - 5 services: *web* (UI), *data analyzer*, *dataprocessor*, *seed*, *monitoring*
 - MySQL deployed on a separate server

KEY BENEFITS

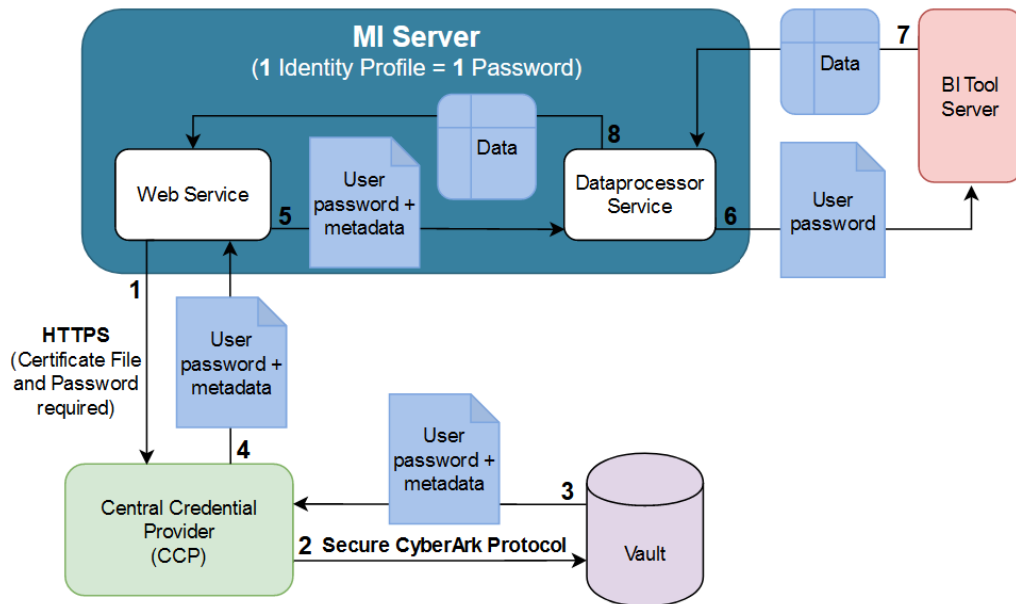
Benefits of Metric Insights:

- Metric Insights' Enterprise BI Portal enables BI governance, providing analysts a way of documenting, categorizing, and certifying their key BI reports and dashboards and publishing them into a centralized portal for users

Benefits of integrating Metric Insights with CyberArk AAM:

- The credentials are stored outside of our system

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



Example of HTTPS Request to CCP:

`https://<CCP host and port>/AIMWebService/api/Accounts?appid=MetricInsights&safe=Test&folder=Root&object=testobject`

Parameters	Central Credential Provider URL	Application ID	Safe	Folder	Object
------------	---------------------------------	----------------	------	--------	--------

AAM INTEGRATION

The integration lies in the application tier. A new Identity Profile is created and selected as an authorization method for a Data Source. When user tries to fetch data from the Data Source:

1. Metric Insights' *web* service sends an HTTPS GET request to the Central Credential Provider (CCP) using Certificate File and Password.
 - See the example request and parameters at the bottom of the diagram.
2. CCP communicates with the Vault via Secure CyberArk Protocol.
3. The Vault responds to CCP with user password and metadata.
4. CCP sends the user password and metadata obtained from the Vault to the *web* service.
5. *Web* service sends the user password and metadata to the *dataprocessor* service (DP).
6. DP sends a request to a BI tool server using the user password.
7. BI tool server sends data to DP in response.
8. DP sends the obtained data to the *web* service. *Web* service displays the data in the UI.

CREDENTIAL RETRIEVAL

The credential retrieval is triggered when:

- User Accesses a Data Source and clicks **Refresh Object List**
- User Creates a new element from a Data Source
- Data collection is triggered by a Data Collection Trigger
- Content is distributed on a Notification Schedule via bursting

REQUIREMENTS

List software, network, and hardware requirements. Provide context of requirements and team expertise for user planning needs.

Software requirements:

For servers without outbound access, the host machine must have the following packages installed manually to support the application:

- docker-ce v18+
- docker-compose v1.19.0+
- python v2/v3

Hardware requirements:

- Metric Insights application server:
 - 8 Core
 - 32 GB RAM
 - 1 TB+ disk total

Additionally for Orchestrated environments:

The MySQL database must be running on a separate server, preferably on a database cluster managed by a DBA team or a native cloud solution like Amazon RDS.

- 8 Core
- 32 GB RAM
- 1 TB+ HD total

Network requirements:

If the Metric Insights application uses a firewall on Linux machine, the following ports must be accessible:

- **80, 443** - HTTP and HTTPS ports for the Web Application (by default redirection to 443)
- **2550** - TCP port for the Data Processor service
- **2551** - TCP port for the Seed service
- **3306** - MySQL port for external access to the database
- **8080, 8443** - HTTP and HTTPS ports for the REST API Data Processor Service (only one port is enabled at one time)
- **8081** - TCP port for the Monitoring service (separate GUI service that admins can use to monitor the health of the application containers in a browser)

AAM INSTALLATION

Refer to [CyberArk Agentless installation and configuration](#).

AAM CONFIGURATION

The following sections provide details on Metric Insights configuration with CyberArk AAM.

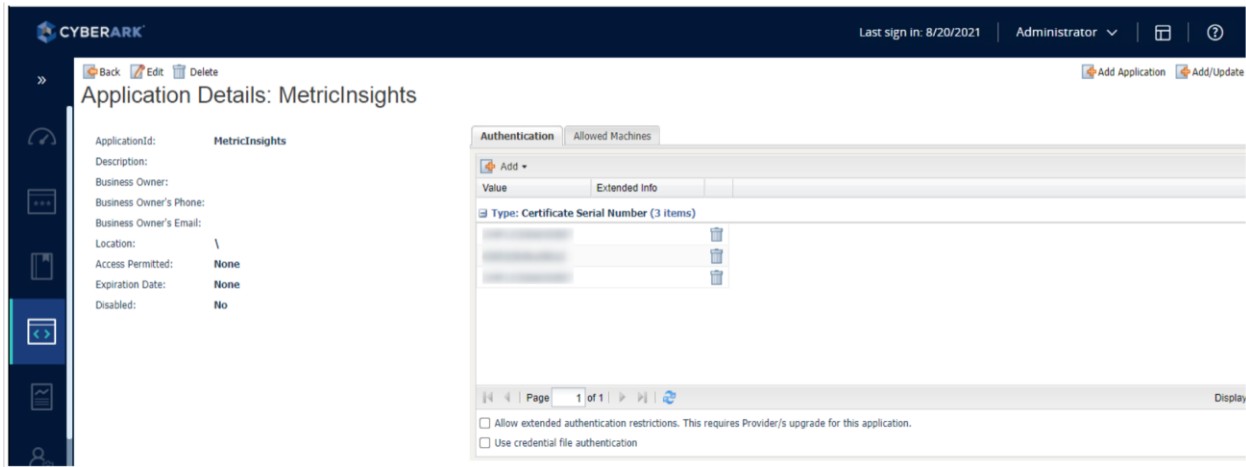
DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

To define the application, define it manually through the CyberArk Password Vault Web Access (PVWA) interface:

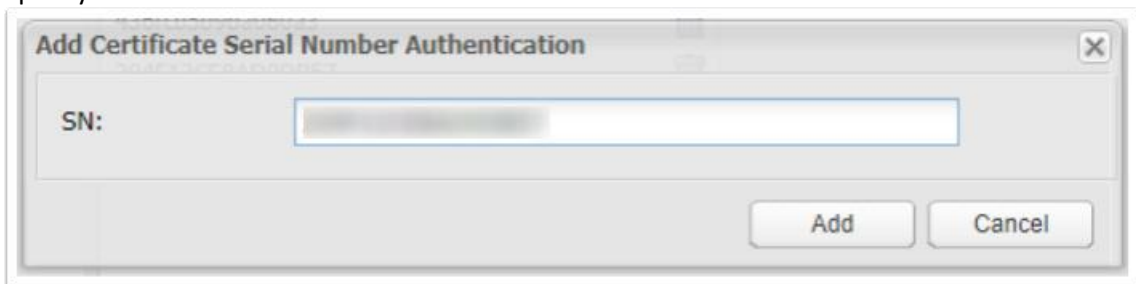
1. Log in as user allowed to manage applications (it requires Manage Users authorization)
2. In the Applications tab, click **Add Application**. The Add Application page appears.

The screenshot shows the 'Edit Application' dialog box. The 'Name' field is populated with 'MetricInsights'. The 'Description' field is empty. The 'Business owner' section includes fields for 'First Name', 'Last Name', 'Email', and 'Phone', all of which are empty. The 'Location' field is a dropdown menu showing a backslash character. Below this are three checkboxes: 'Access Permitted', 'Expiration Date', and 'Disabled', all of which are unchecked. The 'Access Permitted' checkbox is followed by 'From' and 'To' date pickers. The 'Expiration Date' checkbox is followed by a date picker. At the bottom right are 'Update' and 'Cancel' buttons.

3. 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 = MetricInsights
4. Click **Add**. The application is added and is displayed in the Application Details page.



5. Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password.
 - 5.1. In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.
 - 5.2. Select **Certificate Serial Number**.
 - 5.3. Specify the Certificate Serial Number.



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.

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

Add Safe Member

Search: Search In:

Selected Search: Vault Display 1 result(s)

Name	Business Email	Full Name
MetricInsights		

☐ Access

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

☐ Account Management

☐ Safe Management

☐ Monitor

- ☐ View Audit log
- ☐ View Safe Members

☐ Workflow

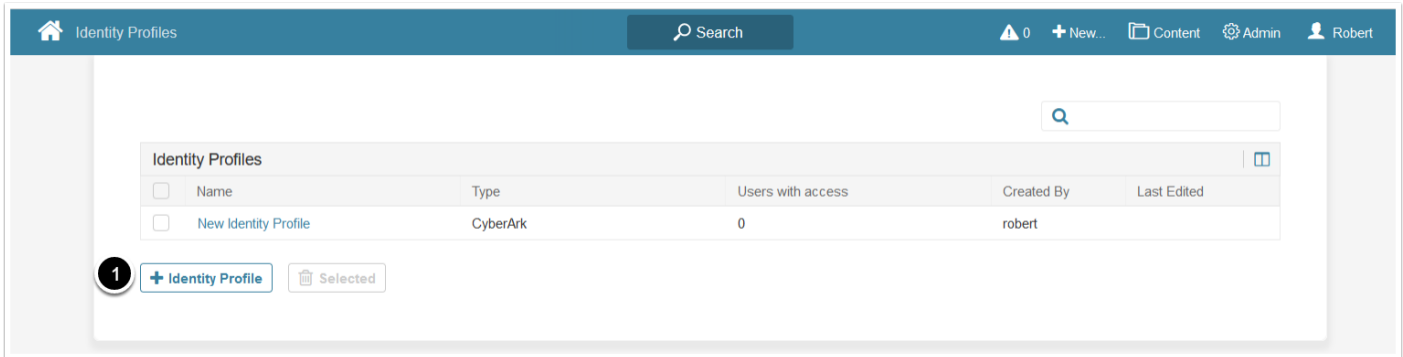
For more information about configuring Safe Members, refer to [Add a Safe Member](#).

PARTNER PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

Refer to [Install or Update MI via Installation Packages \(for MI v6.x\)](#) for Partner Product installation.

Partner Application UI:

1. Create a New Identity Profile
 - Access **Admin > System > Identity Profiles**



- 1.1. Click **+ New Identity Profile**
2. Configure Identity Profile

1. Give a **Name** to the Identity Profile
2. Enter **Central Credential Provider URL** in the following format: `https://<CCP host and port>/AIMWebService`
3. Enter **Application ID**
4. Enter **Username**
5. **Type:** CyberArk
6. Enter **Safe** name
7. Enter **Folder** name
8. **Object:** Enter the Account Name
 - Access your CyberArk account > **Accounts** > **Accounts View (Classic UI)** > **Advanced** > **Name**
9. **Certificate File:** click **Upload Certificate**

10. Enter the **Certificate Password**
11. Click **Test Connection**, this will also save your entries

3. Add the Identity Profile to a Data Source

Plugin: **Microsoft Power BI Cloud**

Data Source Name:

Tags:

Start typing to find or create Tags, then press the Enter key to save.

1 Auth Type:

2 Identity Profile:

☐ Enable On-Demand Element Creation

☐ Enable Content Auto Synchronization

3 [Test Connection](#)

- 3.1. Auth Type: Identity Profile
- 3.2. Select the created Identity Profile
- 3.3. Click **Test Connection**, this will also save your entries

PARTNER CONTACT INFO

Business Contact	Name	Grayson Stebbins
	Email	grayson@metricinsights.com
	Tel	415-846-7997
Technical Contact	Name	Aaron Cho
	Email	aaron@metricinsights.com
	Tel	408-667-4319
Support Contact	Name	Aaron Cho
	Email	aaron@metricinsights.com
	Tel	408-667-4319