



APPLICATION ACCESS MANAGER

AAM INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company Apica Inc

Website www.apica.io

Name of Product Apica Synthetic Monitoring / ZebraTester

Version ASM version 11.8.0.16360, ZebraTester version 5.5A+

Date July 15, 2024

APICA SOLUTION OVERVIEW

Apica Synthetic Monitoring (current version as of 05/14/2019, 11.8.0.16360) Apica Synthetic proactively monitor your websites, applications and APIs around the clock and identify availability and performance issues before they affect your customers. Detect any issues that impact the end-user experience—from page load time and page size to network instability, the impact of third-party providers and much more. Run your monitors like a scientist in a lab. Apica’s synthetic monitoring solution provides a controlled environment where you can minimize variables and reduce false positives.

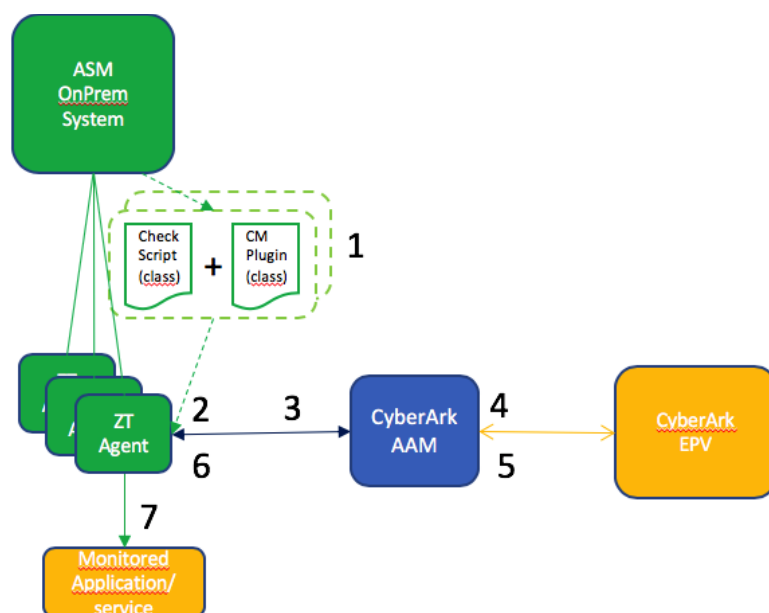
ZebraTester scripting tool (integration will work on versions 5.5A and above). Apica ZebraTester is Apica’s first generation scripting tool. A powerful scripting tool that offers a range of features to create advanced scripting used for load testing and monitoring. With the universally usable HTTP(S) Proxy Recorder, scenarios can be recorded using any web browser, including AJAX calls and requests made from pop-up windows. Data traffic for HTTP(S)-based web service client programs can also be recorded. Simple test scenarios can be created automatically with an Integrated Web Crawler which discovers all the pages comprising a website. Test scenarios can also be created manually by importing pre-defined URL calls from a definition file. Apica ZebraTesters high number of features and complexity makes the tool suitable for the advanced user and test experts.

KEY BENEFITS

Apica Synthetic Monitoring ensures web uptime and tracks performance while using ZebraTester as a scripting tool to simulate a synthetic user that runs as a check on an interval.

The key benefit of Apica and CyberArk partnership is for customers to utilize credential management by CyberArk while Apica takes advantage of CyberArk’s technology in credentials retrieval.

DIAGRAM & INTEGRATION DESCRIPTION



ZebraTester utilizes plugins to extend functionality of the scripts using Java. Apica developed a new ZebraTester plugin to retrieve credentials from CyberArk AAM to use in the ZebraTester scripts to login the synthetic users. This integration will only be utilized during run-time for the front-end of the application. The new ZebraTester plugin that uses the integration is currently built for only one customer but should be able to support other customers who use CyberArk AAM in their environment using the same plugin code.

As previously mentioned, this integration was implemented as a new Apica ZebraTester plugin. This plugin is only used when a ZebraTester script requires credentials to be retrieved from CyberArk's AAM environment. The plugin needs 5 input parameters: AppID, Safe, Folder, Object, and Reason (optional but recommended). An API URL would also be needed when the customer opts to use a URL method of accessing the credentials from AAM. When a login ZebraTester script runs, it will prefetch the credentials by either using the agent based `javapasswordsdk.jar` or the agentless REST API.

Depending on the number of scripts running, a ZebraTester script/check typically runs once every 10 minutes (when scripts are setup to run automatically at preset time intervals, they are called "checks"). If the customer have 100 checks running, then for example the frequency per hour should be around 600 credential retrievals.

Our Apica tool and portal can run on both Windows and Linux environments. Since our tools is Java based, we utilize AAM's java sdk as well as REST API.

AAM INSTALLATION

Refer to “Credential Provider and ASCP Implementation Guide” for agent based or “Central Credential Provider Implementation guide” for agentless installation.

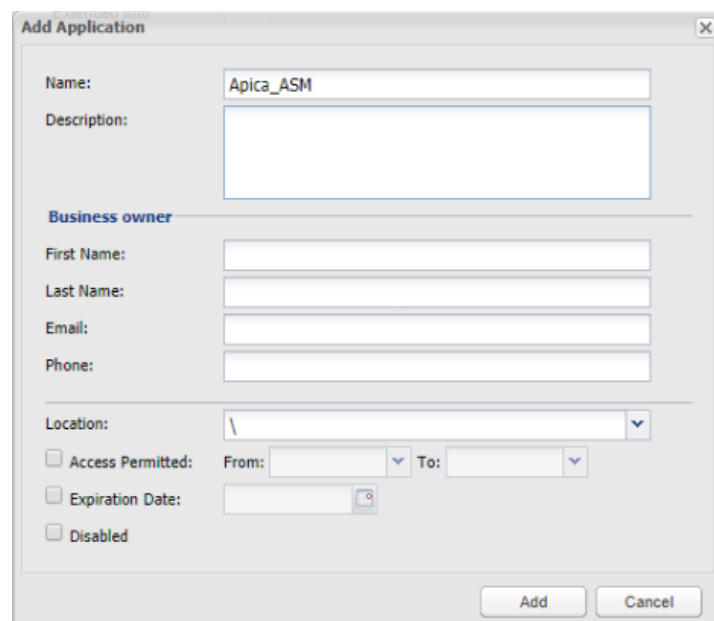
AAM CONFIGURATION

No specific configuration is required.

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.



2. Specify the following information:
 - In the Name edit box, specify Apica_ASM
 - 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.

Application Details: Apica_ASM

Application Id: Apica_ASM

Description:

Business Owner:

Business Owner's Phone:

Business Owner's Email:

Location: \

Access Permitted: None

Expiration Date: None

Disabled: No

Authentication

Allowed Machines

Add

OS user

Path

Hash

Certificate Serial Number

Info

Page 1 of 1

No authentications to display

Allow extended authentication restrictions. This requires Provider/s upgrade for this application.

Use credential file authentication

- **Allowing extended authentication restrictions.** This enables you to specify an unlimited number of machines and Windows domain OS users for a single application. Please check this box.
4. 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.

Add allowed machine

Address:

Enter IP/host name/DNS

Add

Cancel

- 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 AAM 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 (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.

- 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.

Add Safe Member

Search: Search In: **Vault**

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

- ii. 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
Apica_ASM		

☐ Access
☐ Use accounts
☒ Retrieve accounts
☐ List accounts
☐ Account Management
☐ Safe Management
☐ Monitor
☐ View Audit log
☐ View Safe Members

Apica_ASM has been added.

- iii. If your environment is configured for dual control:
 - In PIM-PSM environments (v7.2 and lower), if the Safe is configured to require confirmation from authorized users before passwords can be retrieved, give the Provider user and the application the following permission:
 - Access Safe without Confirmation
 - 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**.

APICA INSTALLATION & INTEGRATION CONFIGURATION

Refer to Apica's ZebraTesterInstallationGuide.pdf for Partner Product installation.

Refer to Apica's ZebraTesterUsersGuideEn.pdf for Partner Product usage.

After installing Apica ZebraTester on your local machine, please copy 2 class files named CredentialsManagerEPV.class and CredentialsManagerEPVAPI.class into the MyTests folder inside the ZebraTester install directory. Since these are new custom ZebraTester plugin files, they are not yet pre-packaged with the ZebraTester installer. After copying the files, you can use these plugins just like you would using other pre-installed plugins. Please refer to chapter 7.4 (Load Test Plug-Ins) of the ZebraTesterUsersGuideEn.pdf on how to use plugins.

Var Handler

Add Load Test Plug-in: (Step 2)

Plug-in #1:	Credentials Manager v24
Class:	CredentialsManagerEPV.class
Constructed:	global
Execution:	before / at start of loop

Run-Time Input Parameter:

App ID: AppID [global]

Safe: Safe [global]

Folder: Folder [global]

Object: Object [global]

Reason: Reason [global]

Run-Time Output Parameter:

Parameter 1: Username

☒ Use Var: username [global]

☐ Create Var

Parameter 2: Password

☒ Use Var: password [global]

☐ Create Var

Add Plug-in

Plug-in Description:

Retrieve encrypted username/password from EPV and plugin will retrieve data to be used in the ZebraTester script.

Var Handler

Add Load Test Plug-in: (Step 2)

Plug-in #1:	Credentials Manager EPV v25
Class:	CredentialsManagerEPVAPI.class
Constructed:	global
Execution:	before / at start of loop

Run-Time Input Parameter:

API URL: ApiURL [global]

App ID: AppID [global]

Safe: Safe [global]

Folder: Folder [global]

Object: Object [global]

Reason: Reason [global]

Run-Time Output Parameter:

Parameter 1: Username

☒ Use Var: username [global]

☐ Create Var

Parameter 2: Password

☒ Use Var: password [global]

☐ Create Var

Add Plug-in

Plug-in Description:

Retrieve encrypted username/password from EPV and plugin will retrieve data to be used in the ZebraTester script.

Common use cases:

There are 4 required input parameters for version 24(v24) and 5 required input parameters for version 25 (v25). The four common parameters that the customer needs to provide the ZebraTester plugin are AppID, Safe, Folder, and Object. For the REST API version of the plugin (v25), the API url is also a required parameter, please refer the [CyberArk REST API documentation](#). An optional but recommended input parameter is Reason. When a customer provides all these values into the plugin and successfully runs with valid values, the username and password output parameters are populated. ZebraTester scripts can now use these populated credentials, usually as Login POST calls within the scripts, to authenticate the users in the customer's synthetic scenario.

PARTNER CONTACT INFO

Business Contact	Name	
	Email	
	Tel	
Technical Contact	Name	
	Email	
	Tel	
Support Contact	Name	Apica Customer Support
	Email	support@apicasystems.com
	Tel	310-776-7569