



APPLICATION ACCESS MANAGER

AAM INTEGRATION - TECHNICAL DOCUMENTATION

Device42, Inc.

<https://device42.com>

Device42

18.05.00

December 29, 2022

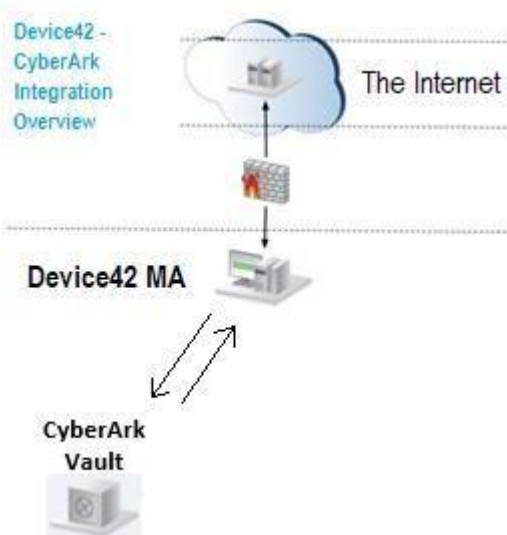
DEVICE42 SOLUTION OVERVIEW

V18.05.00 of Device42, a CMDB product featuring powerful infrastructure auto-discovery, a full DCIM suite, and more, is shipped on a standalone Linux (CentOS, not customer accessible) VM.

KEY BENEFITS

Device42 Inc., a leader in the Configuration Management Database (CMDB), Application Dependency Mapping (ADM) and DCIM Software Marketplace, delivers comprehensive, low cost solutions that helps companies automatically maintain an up-to-date inventory of their IP-based Devices and non-IP Assets, whether physical, logical, or virtual. Device42 provides customers with understanding and advanced visualization of their infrastructure and its inter-dependencies, and centralizes data center knowledge into a single source of truth making IT ecosystems clearly visible, understandable, and controllable.

DIAGRAM & DESCRIPTION OF THE INTEGRATION



- *Cyberark is integrated as a Device42 endpoint, queried via the CyberArk protocol. The integration supplies passwords in response to D42 queries that provide CyberArk a username or 'label' field, results of which are then used by Device42's auto-discovery to authenticate to client machines [never exposing the PW to the D42 user].*
- Number of mid-tier servers and number of endpoints in a typical installation:
 - 1 mid, 1 EP

AAM INSTALLATION

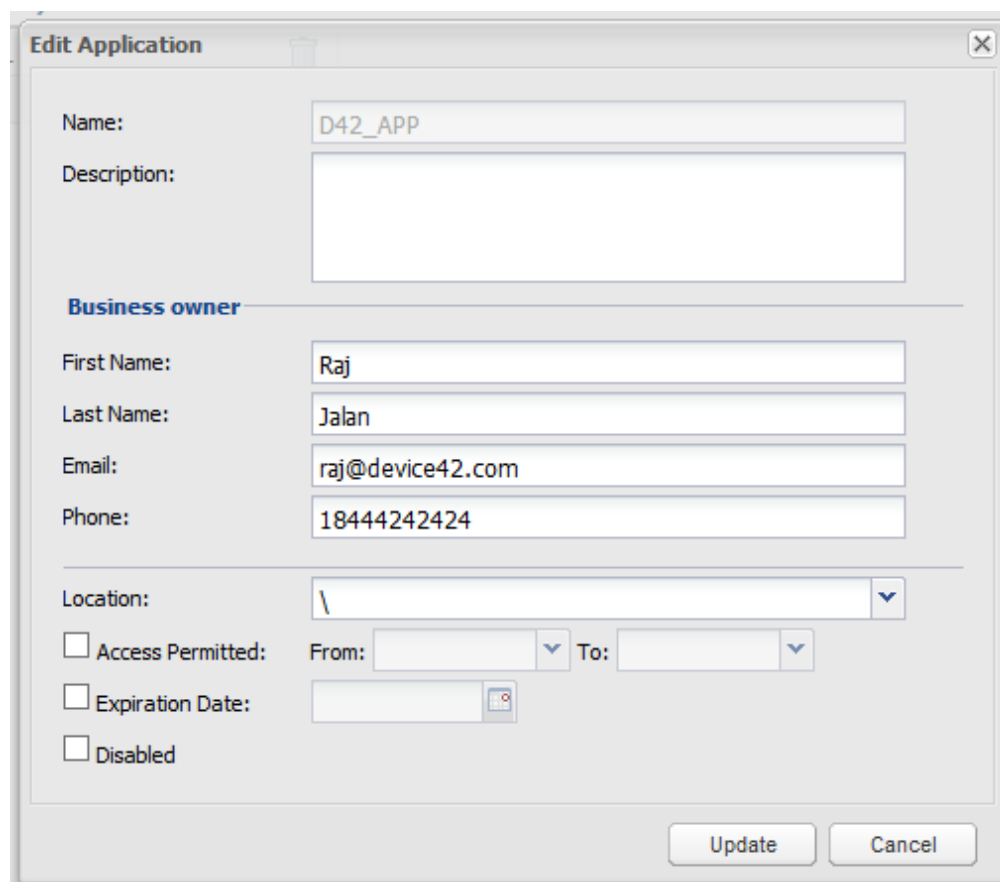
Refer to “Central Credential Provider Implementation Guide” for CyberArk Credential Provider installation.

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.



The screenshot shows the 'Edit Application' dialog box. It contains the following fields and options:

- Name:** D42_APP
- Description:** (Empty text area)
- Business owner:**
 - First Name:** Raj
 - Last Name:** Jalan
 - Email:** raj@device42.com
 - Phone:** 18444242424
- Location:** \ (Dropdown menu)
- Access Permitted:** ☐ From: (Dropdown) To: (Dropdown)
- Expiration Date:** ☐ (Calendar icon)
- Disabled:** ☐

At the bottom right, there are two buttons: **Update** and **Cancel**.

2. Specify the following information:
 - In the Name edit box, specify D42_APP
 - 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: D42_APP

Application Id: D42_APP

Description:

Business Owner: Raj Jalan

Business Owner's Phone: 18444242424

Business Owner's Email: raj@device42.com

Location: \

Access Permitted: None

Expiration Date: None

Disabled: No

Authentication	
Value	Extended Info
No authentications to display	

Page 1 of 1

☐ 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.

Added Device42 MA IP Address – Integration users should do the same.

Allowed Machines

Add

Address

151.181.77.66

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 Account 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

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

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

Add Safe Member

Search: Search In:

Selected Search: Vault Display 1 result(s)

Name	Business Email	Full Name
D42_APP	raj@device42.com	Raj Jalan

☐ Access

☐ Use accounts

☒ Retrieve accounts

☐ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☐ View Audit log

☐ View Safe Members

D42_APP has been added.

Retrieve accounts

- 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**.

DEVICE42 INSTALLATION & INTEGRATION CONFIGURATION

Refer to <https://docs.device42.com/getstarted/> for Device42 Product installation.

Configure Integration via TOOLS menu Integrations CyberArk:

DEVICE42  DataCenter  Devices  Network  Apps  Secrets  Discovery  Reports  Tools       | admin 

Setup CyberArk integration used to lookup Passwords

☒ Enable CyberArk

Cyberark URL:

http://services-uscentral.skytap.com:10526

Enter the address of your Cyberark HTTP Component Uri and Port

App Id:

D42adam

Enter the Application Id to access the Cyberark API.

Skip HTTPS Certificate Verification

☒

Will skip the HTTPS certificate verification

Note:

By default passwords are looked up by name in CyberArk by matching the Password label in Device42. If no label is provided then the username will be matched directly. You may also customize the Folder or Safe the password is retrieved from by utilizing Password Custom fields named Folder and Safe.

TestSave

Provide the URL of your CyberArk instance and create an App ID for Device42: **D42_APP**

When testing you CyberArk connection, if you receive **unable to validate configuration** notifications related to certificate validation errors you will want to go back to your CyberArk configuration page and select the **Skip HTTPS Certificate Verification** checkbox. This can be an issue if your CyberArk instance is using a self-signed SSL Certificate.

PARTNER CONTACT INFO

Business Contact	Name	Drew Conly
	Email	drew.conly@device42.com
Technical Contact	Name	Chris Scaglione
	Email	chris.scaglione@device42.com
Support Contact	Name	Jason Lomax
	Email	jason.lomax@device42.com