AIM INTEGRATION - TECHNICAL DOCUMENTATION

Varonis

http://www.varonis.com/

DatAdvantage and DataPrivilege

Versions 6.3.100 and up

Date: 21/06/16

VARONIS SOLUTION OVERVIEW

Varonis DatAdvantage provides organizations the ability to see who is accessing data and what they've accessed, identify excessive permissions, and identify data owners in order to ensure that only the right people have access to the right data at all times, monitor use and alert on abuse.

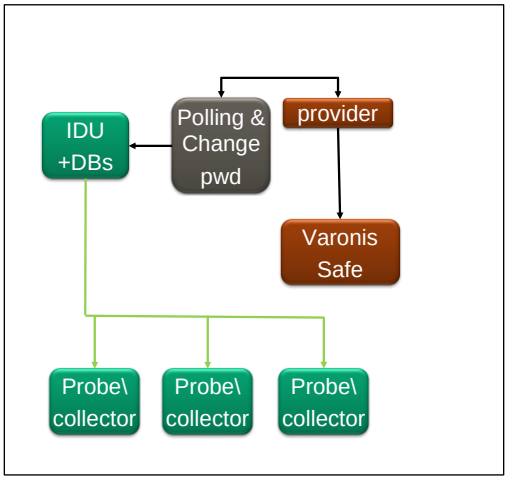
Varonis DataPrivilege automates data governance by providing a framework for users and data owners to be directly involved in access entitlement review and authorization workflows.

KEY BENEFITS

CyberArk's Application Identity Management solution uses the Privileged Account Security solution to eliminate the need to store application passwords embedded in applications, scripts or configuration files, and allows these highly-sensitive passwords to be centrally stored, logged and managed within the Vault. This unique approach enables organizations to comply with internal and regulatory compliance requirements of periodic password replacement, and monitor all activities associated with all types of Privileged Identities whether on-premise or in the cloud, across operating systems, databases, applications, hypervisors, network devices and more.

The integration between CyberArk's Application Identity Management and Varonis DatAdvantage and DataPrivilege provides the ability to manage privileged accounts used by DatAdvantage and DataPrivilege within the CyberArk's Vault, facilitating periodic password replacements for these privileged identities in a manner transparent to the functionality of the Varonis products, eliminating the manual configuration previously required.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION.



A new IDU job will retrieve credentials from the CyberArk Vault. The job will then update the passwords of the Varonis users in different components within the set of supported tasks. The list of users to be polled is configurable in a CSV file read by the job. No change in installation\configuration, passwords still required.

SUPPORTED VARONIS TASKS

Product	Task
DatAdvantage	FileWalk
DatAdvantage	Share detection
DatAdvantage	DCF
DatAdvantage	working share
DatAdvantage	ADWalk
DatAdvantage	Volumes
DatAdvantage	Probe proxy
DatAdvantage	SHS scopes
DatAdvantage	DFS roots
DataPrivilege	Working share
DataPrivilege	ADWalk
DataPrivilege	FileWalk and commit
DataPrivilege	AD commit

AIM INSTALLATION

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

The Credential Provider needs to be installed on the IDU machine.

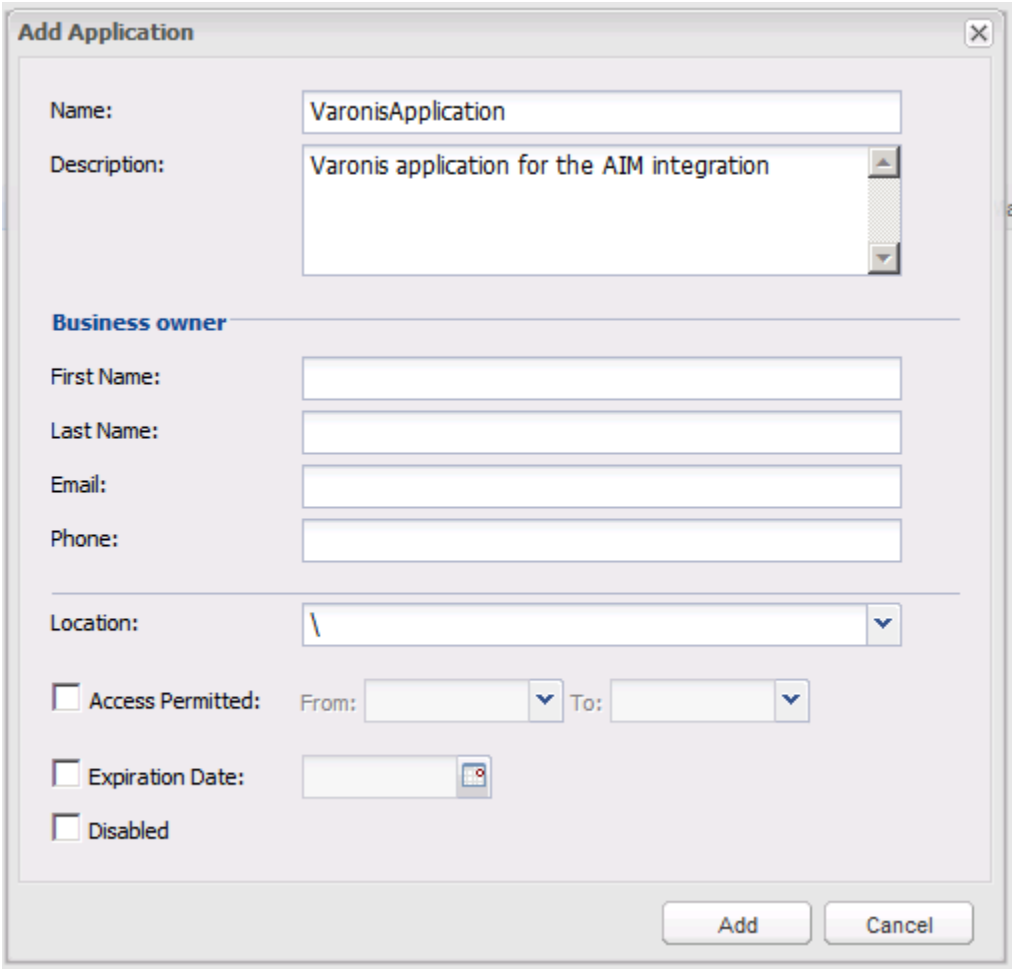
AIM CONFIGURATION

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

The Varonis Application (AppID) must be defined in order to setup access to the accounts it needs. This AppID is used by different Varonis components to retrieve credentials from the CyberArk Vault.

These are the instructions to manually define the Application manually via CyberArk's PVWA (Password Vault Web Access) Interface:

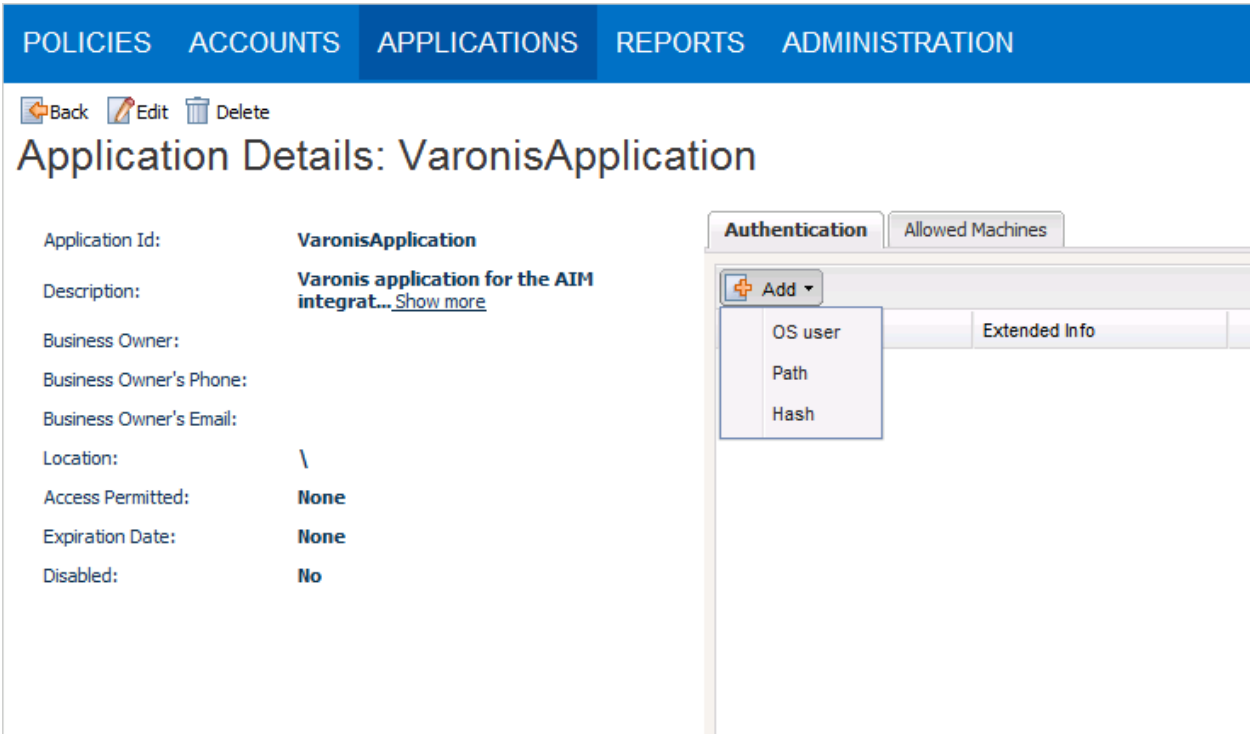
1. Logged in as user allowed to managed applications (it requires Manage Users authorization), in from the Applications tab, click **Add Application**; the Add Application page appears:.



2. Specify the following information:
    - In the Name edit box, specify the unique name (AppID) of the application.
      VARONIS AppID = **VaronisApplication**

- 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.

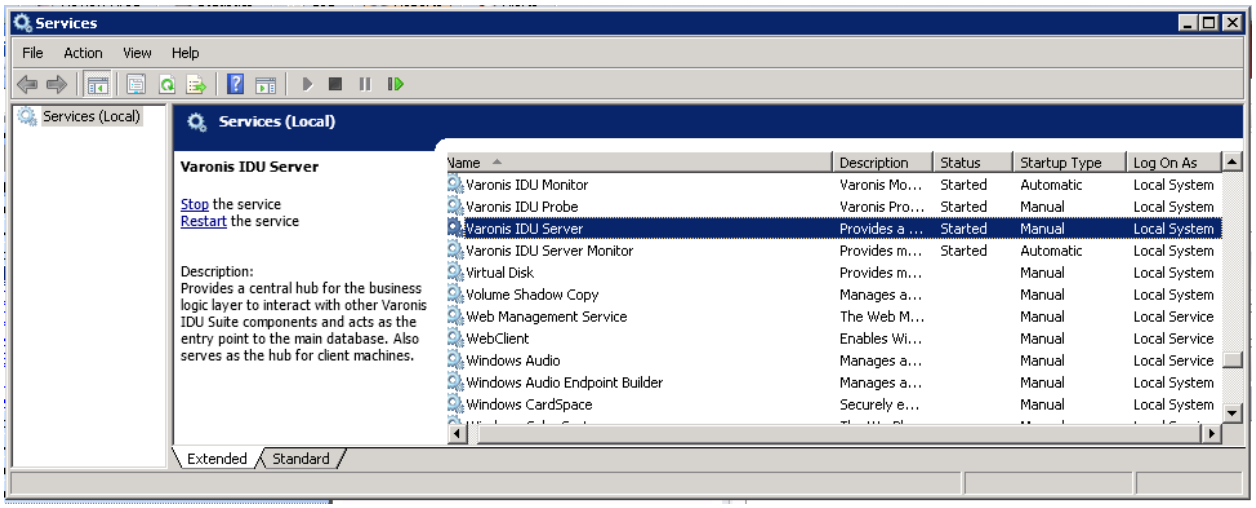


- **Allowing extended authentication restrictions** (found at the bottom of the screen). This enables you to specify an unlimited number of machines and Windows domain OS users for a single application. Please check this box.
- The integration supports usage of any of the extended authentication restrictions.

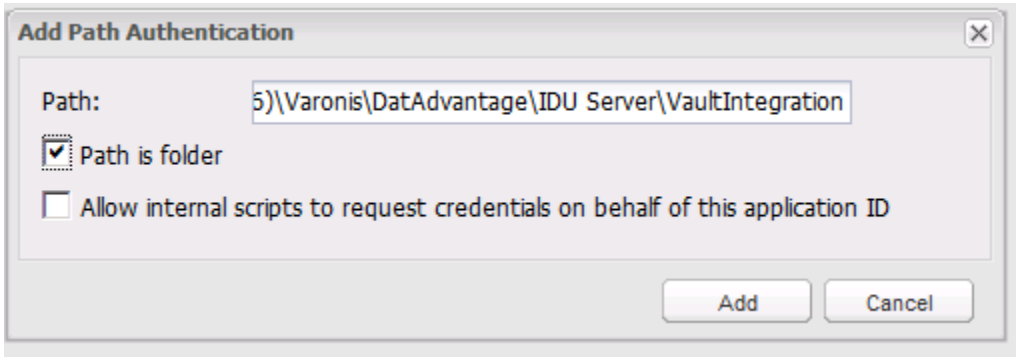
4. Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password.
    - In the Authentication tab, click **Add**; a drop-down list of authentication characteristics is displayed.
    - Select the authentication characteristic to specify.
5. Specify the OS user:

a. Select **OS user**; the Add Operating System User Authentication window appears.

b. Specify the name of the OS user who will run the application, then click **Add**; the OS user is listed in the Authentication tab. The user running the Varonis IDU Service on the IDU machine. By default, **Local System**.



6. Specify the application path:
   a. Select **Path**; the Add Path Authentication window appears.

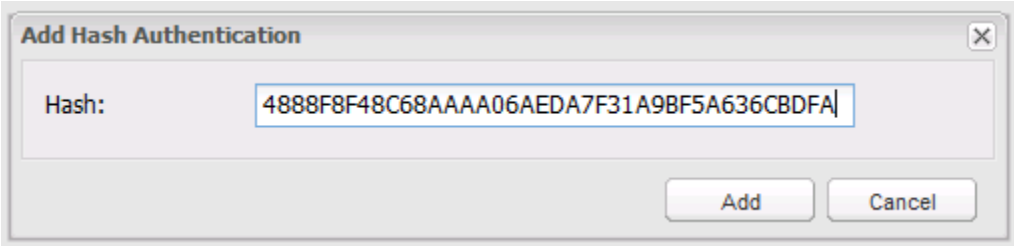


b. Specify the path where the application will run: C:\Program Files (x86)\Varonis\DatAdvantage\IDU Server\VaultIntegration.

c. To indicate that the specified path is a folder, select **Path is folder**.

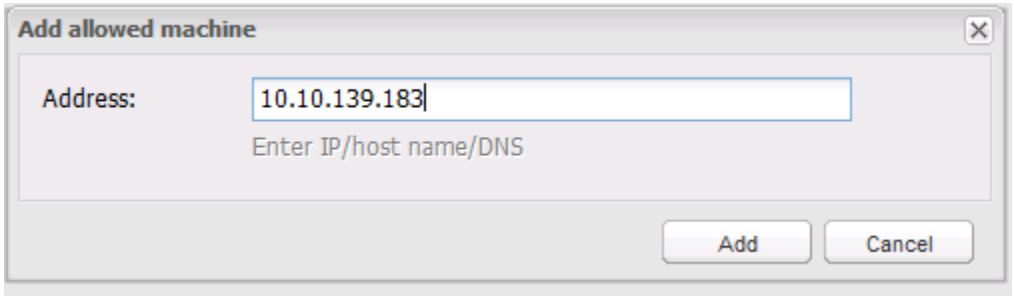
d. To allow internal scripts to retrieve the application password for this application, select **Allow internal scripts to request credentials on behalf of this application ID**.
e. Click **Add**; the Path is added as an authentication characteristic with the information that you specified.

7. Specify a hash:
a. Run the AIMGetAppInfo utility with the full path to the Varonis executable to calculate the application's unique hash.
b. Copy the hash value that is returned by the utility.
c. In the PVWA, select **Hash**; the Add Hash window appears.

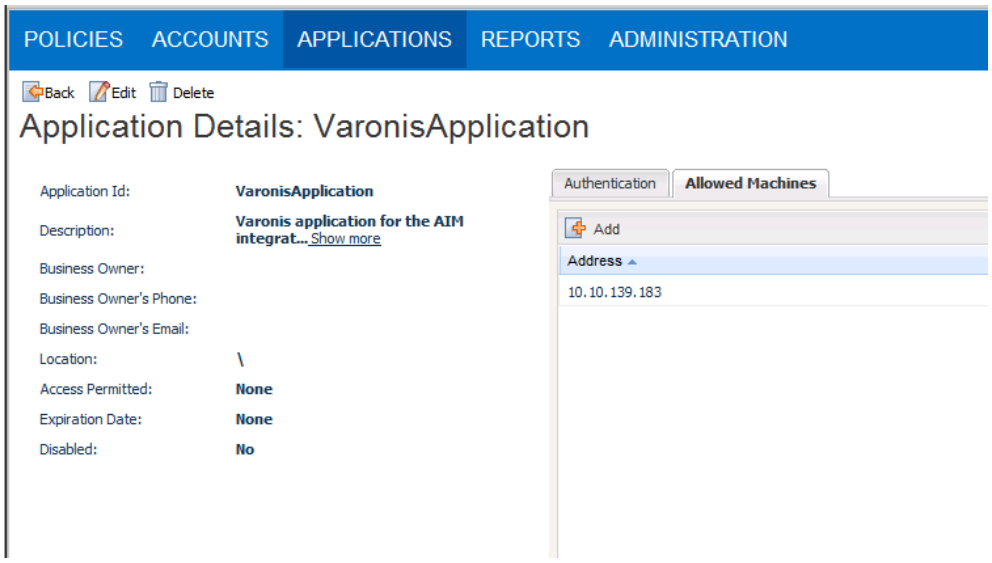


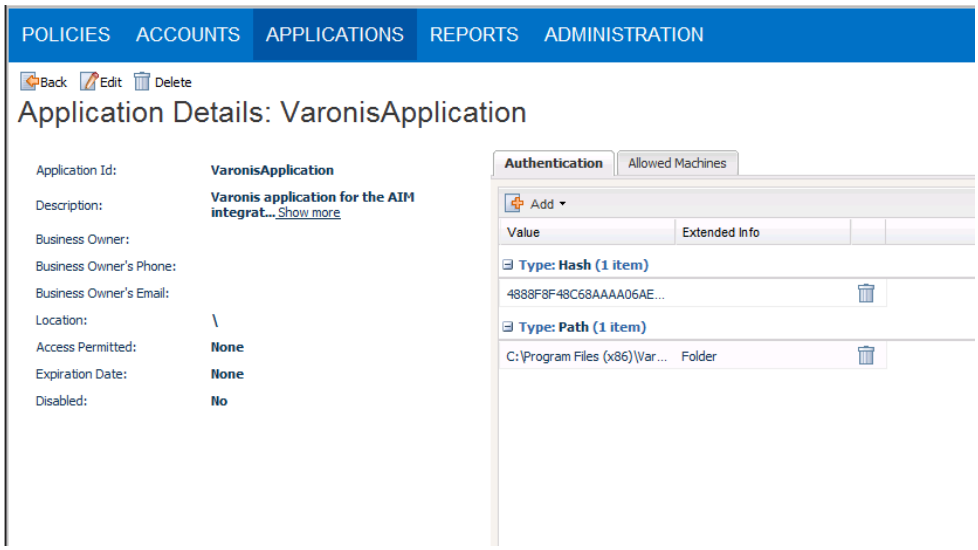
d. In the Hash edit box, paste the application's unique hash value, or specify multiple hash values with a semi-colon. You can add additional information in a comment after each hash value specified for an application by specifying '#' after the hash value, followed by the comment.
For example, OE883B7OD5B6E3EE37D37198049C9507C8383DB6 **#app2**
Note: The comment must not include a colon or a semicolon.
e. Click **Add**; the Hash is added as an authentication characteristic with the information that you specified.

8. 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.



   - Specify the IP/hostname/DNS of the Varonis IDU 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 AIM Credential Providers were installed.





PROVISIONING ACCOUNTS AND SETTING PERMISSIONS FOR APPLICATION ACCESS

For the Varonis/CyberArk Integration 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).

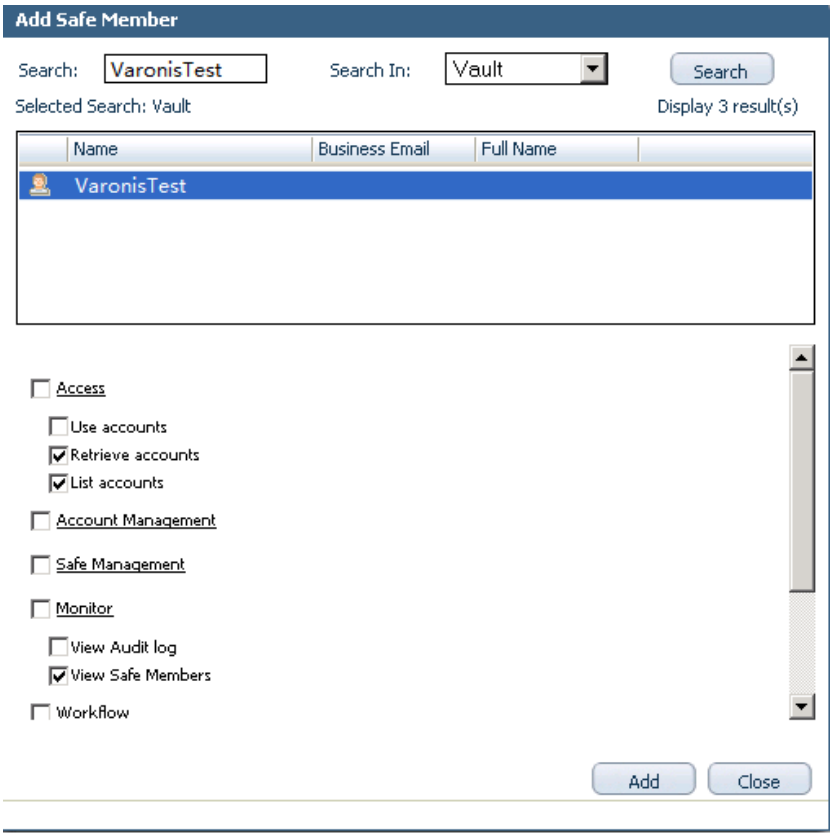
1. In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:
   - **Manually** – Add accounts manually one at a time, and specify all the account details.
   - **Automatically** – Add multiple accounts automatically using the Password Upload feature.

For this step, you require the **Add accounts** authorization in the Password Safe.

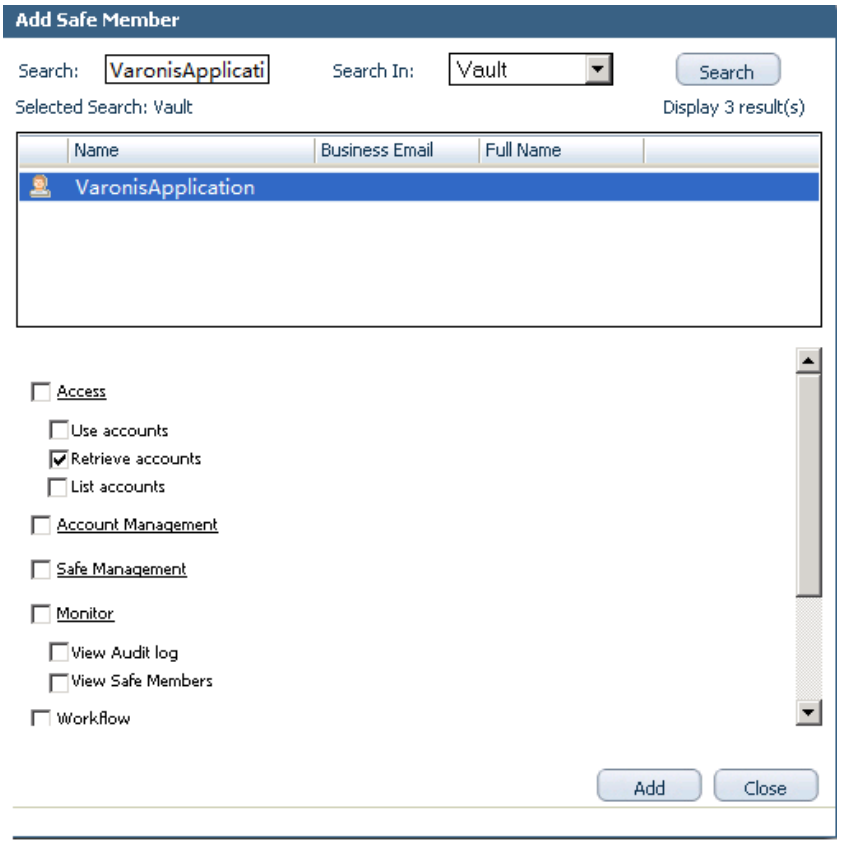
For more information about adding and managing privileged accounts, refer to **the Privileged Account Security Implementation Guide.**

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:
        - Retrieve accounts
        - List 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:
        - 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.

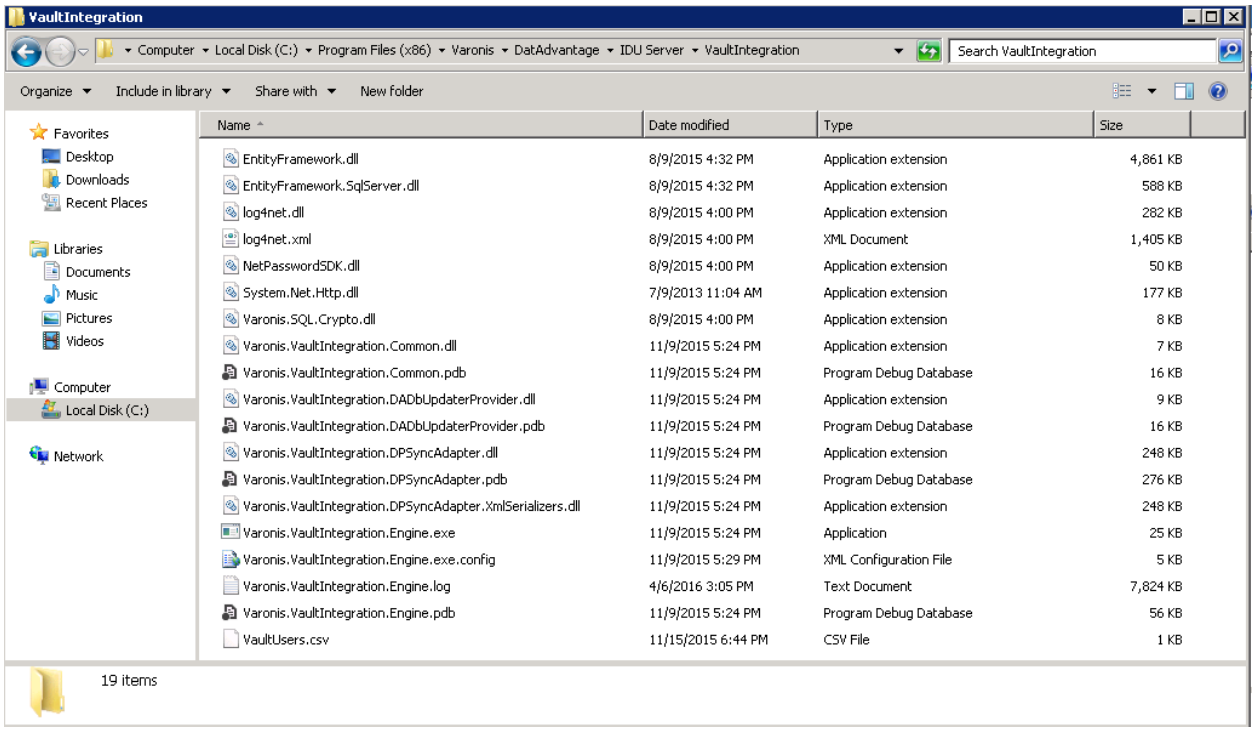
For more information about configuring Safe Members, refer to the **Privileged Account Security Implementation Guide.**

VARONIS PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

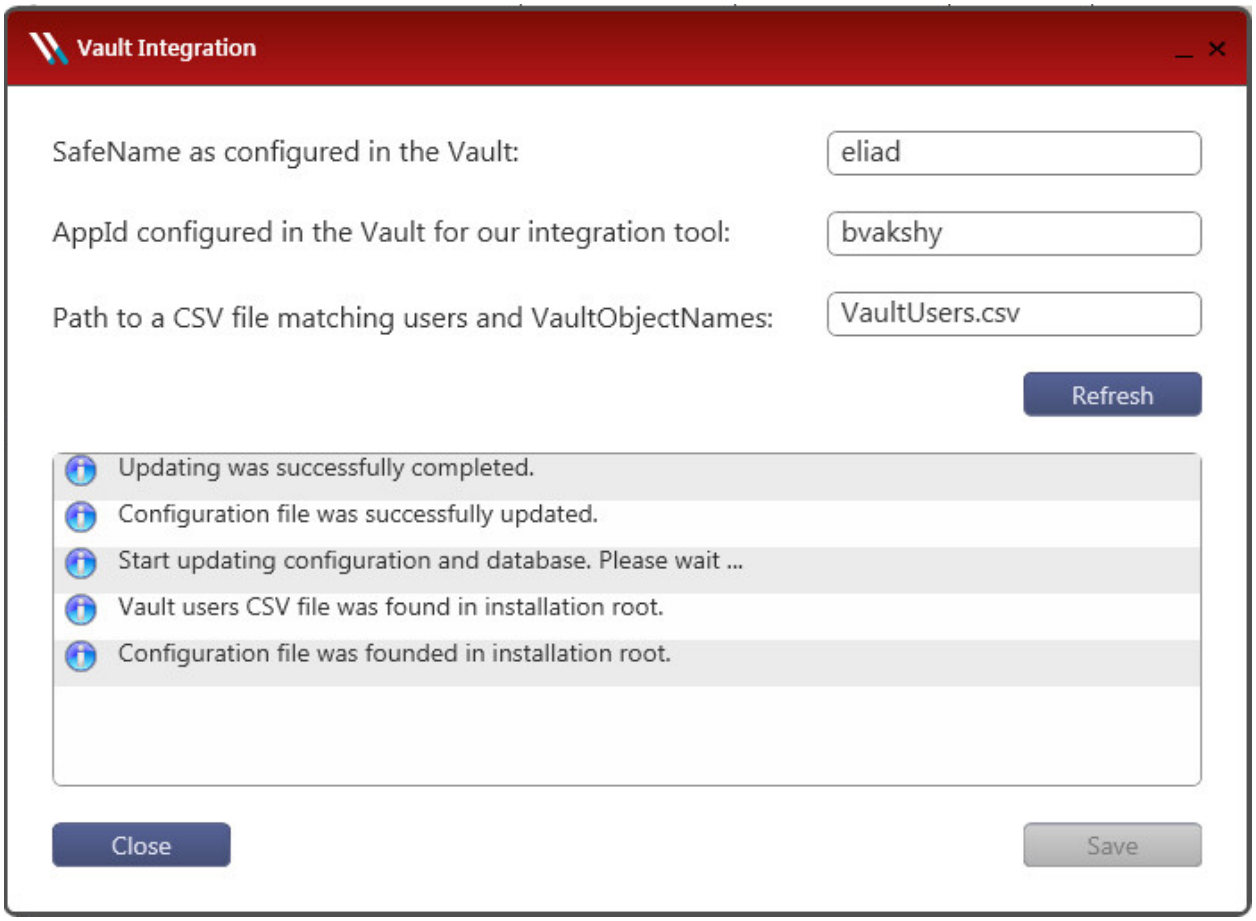
Refer to 'Metadata framework installation guide' for Varonis Products installation.

Configure CyberArk support in Varonis product:

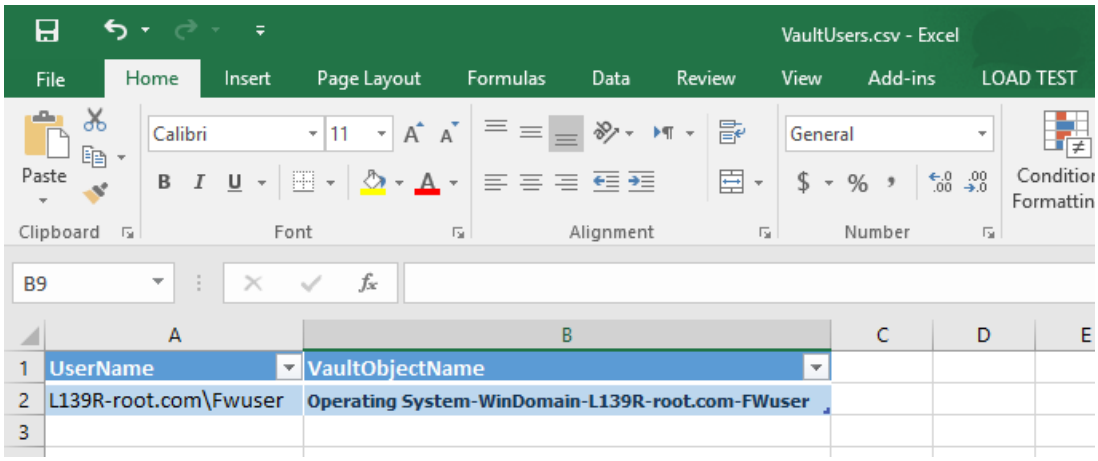
1. Open :\Program Files (x86)\Varonis\DatAdvantage\IDU Server\VaultIntegration

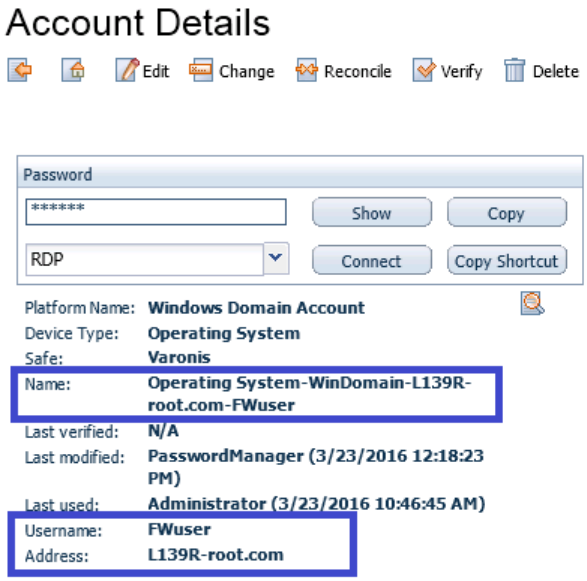


2. Open Varonis.VaultIntegration.UI.exe to configure the safe name holding the Varonis users, the AppId and the path to the CSV.

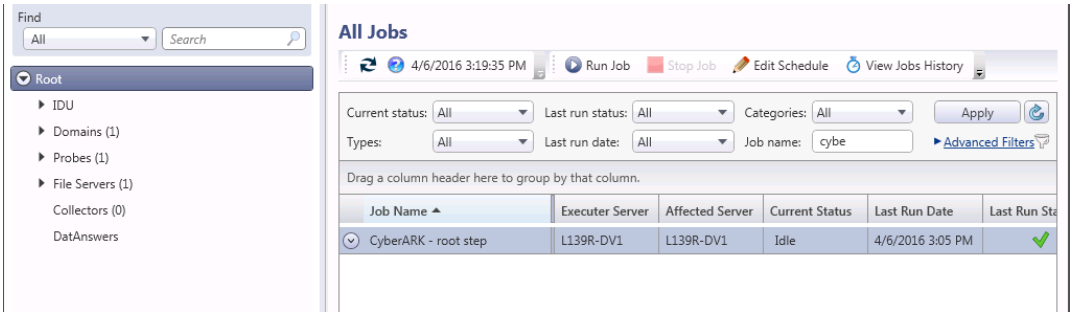


3. Inside Folder VaultIntegration you'll find the file VaultUsers.csv.
   This file contains mapping between Vault ObjectName and userName in our system.
   You should edit it and add mapping for each user you want to be updated by the Vault.
   Format is: UserName as is kept in the Varonis DB, Object name of the user as is kept in the CyberArk vault.
   Note ("Varonis/userA", "userA@Varonis.com" and "Varonis.com/userA" is not the same), best will be to write the user with netbios domain name and also fqdn.
   For Unix local user you should write the following syntax:
   [UnixHost]\[LocalUser] for Example: Centos5.8\root





4. You may change the frequency of the polling job, via MC:



PARTNER CONTACT INFO

Business Contact	Name	Hanni Barry
	Email	hbarry@varonis.com
	Tel	+972732706469
Technical Contact	Name	Elena Svirinovsky
	Email	esvirinovsky@varonis.com
	Tel	+972732706214
Support Contact	Name	Varonis Support
	Email	support@varonis.com
	Tel	