CYBERARK SECRETS MANAGER

CSM INTEGRATION - TECHNICAL DOCUMENTATION

Data443 Risk Mitigation, Inc.

www.data443.com

Data Identification Manager

21.2.7.4

August 30, 2021

DATA IDENTIFICATION MANAGER SOLUTION OVERVIEW

Data Identification Manager is a data classification, governance and compliance platform. It classifies structured and unstructured datasets using a centralized policy rule set. It also performs eDiscovery activities across the same data estate. Data Identification Manager will utilize the CyberArk platform to retrieve permissioned access to Databases (initially) and then expand to retrieve credentials for other senstivie data stores. Data Identification Manager will use these accesses to crawl the data contents, perform classification against the dataset and optionally perform eDiscovery and Governance actions.

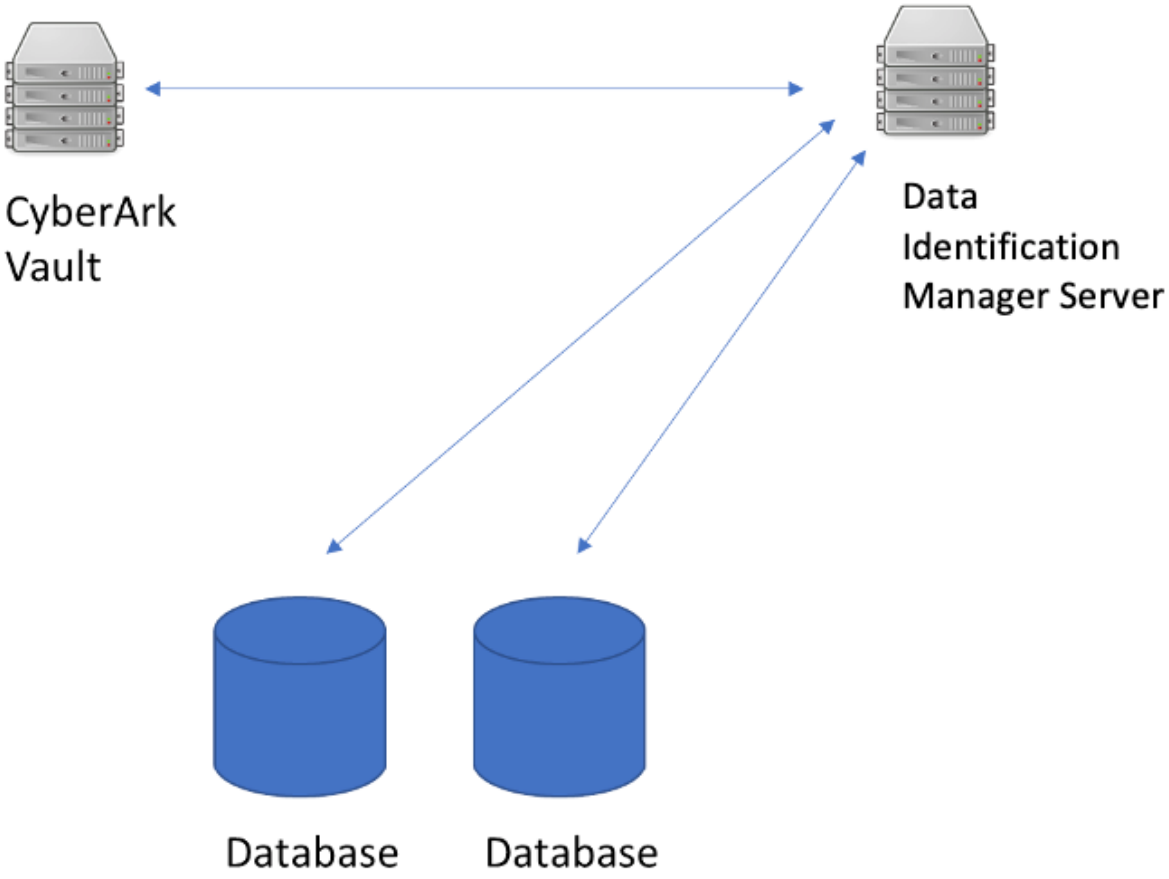
Data Identification Manager is available via cloud and hybrid on-premise deployment options. Version 21.2.7.4 onwards supports the CyberArk integration.

KEY BENEFITS

Data Identification Manager is the only product on the market to perform Data Classification, Governance, eDiscovery and Privacy Compliance (including GDPR) activities across over 400 Database types, 200 file types and Laptop/Desktop, Server, NAS/SAN and Cloud data repositories.

Integrating with CSM provides the customer the ability to leverage their existing investment in CSM and further enhances (or conforms to their) existing security policy framework – namely protecting access control to sensitive datastores. All customers with CSM in place will require Data Identification Manager to utilize the access control framework supported by the product.

DATA IDENTIFICATION MAANGER DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



I. Integration Description:

- CSM is integrated into our admin console which handles scheduling and data targets
- Location of integration: we have an ASP Service running on IIS which does API calls out
- Typically we will have n IIS servers that handle inbound Data Identification Manager traffic, and 1 dedicated to outbound classification jobs. This main server will be the one communicating with CSM.

II. CSM Interaction:

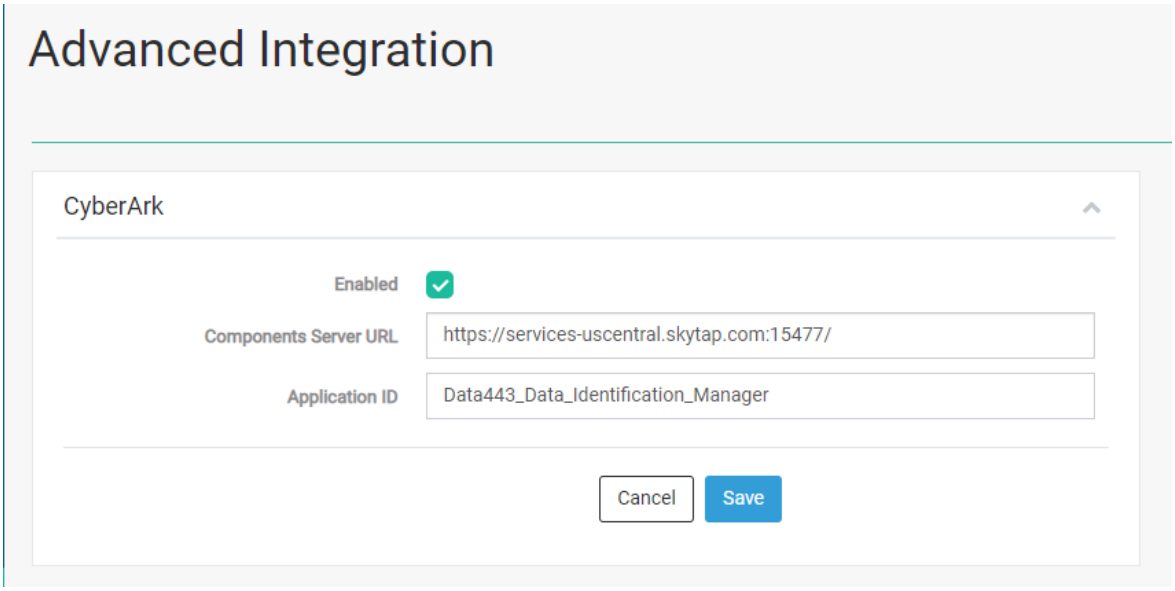
- Data Source Target Definition:
    - Data Identification Manager Administrator will indicate the datasource managed by CSM in the main console

    - This includes the name of the resource
    - Scan times are also defined in this panel
        - Scans are timed events
- Based on the interval defined by the administrator, Data Identification Manager will trigger the retrieval of credentials via CCP calls
    - Data Identification Manager will request the target FQDN/IP, and username/password combination
    - Data Identification Manager will then connect directly to the target and perform its activities

CSM INSTALLATION

Refer to the Central Credential Provider Implementation guide for installation.

Data Identification Manager requires only the CCP server URL and application ID to be configured

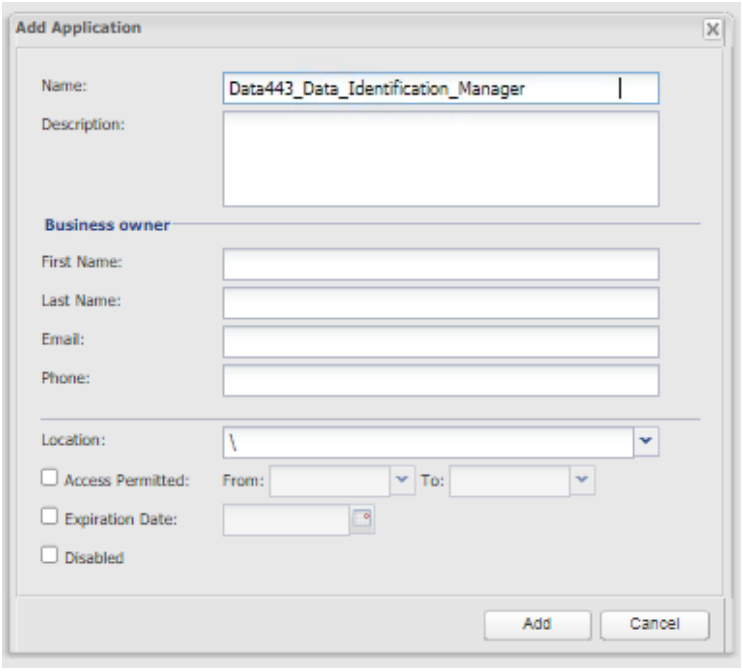


CSM CONFIGURATION

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

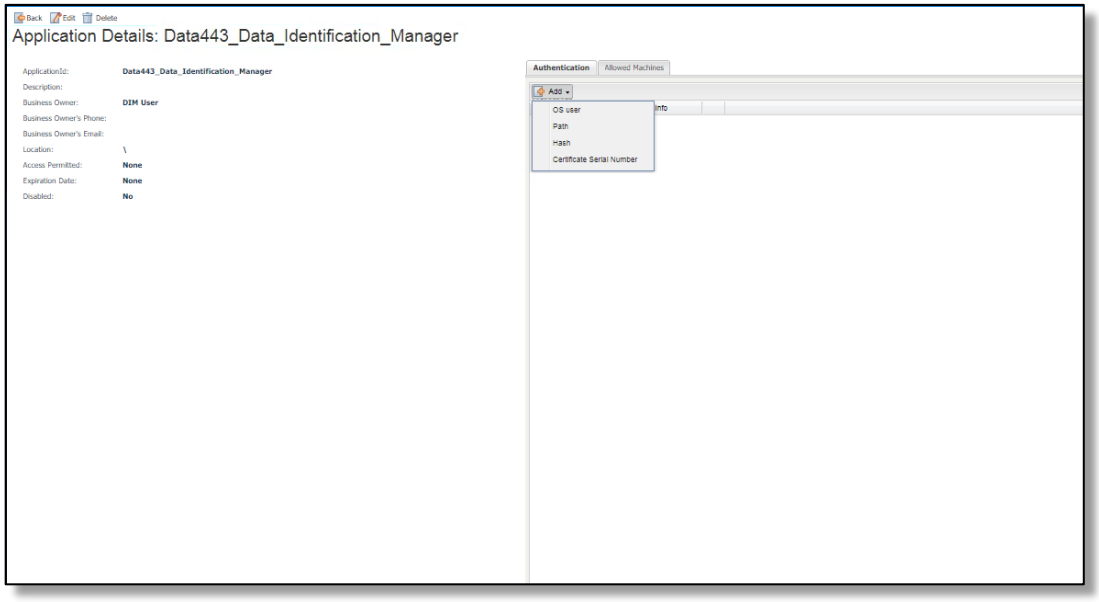
To define the Application, here are the instructions to define it manually via CyberArk's PVWA (Password Vault Web Access) Interface:

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



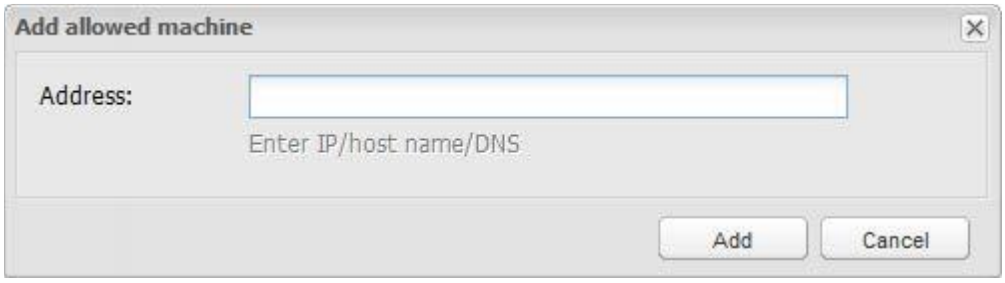
3. Specify the following information:
    - In the Name edit box, specify **Data443_Data_Identification_Manager**
    - In the Description, specify a short description of the application that will help you identify it.
    - In the Business owner section, specify contact information about the application's 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.

4. Click **Add**; the application is added and is displayed in the Application Details page.



- **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.

5. 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 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 CSM 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).

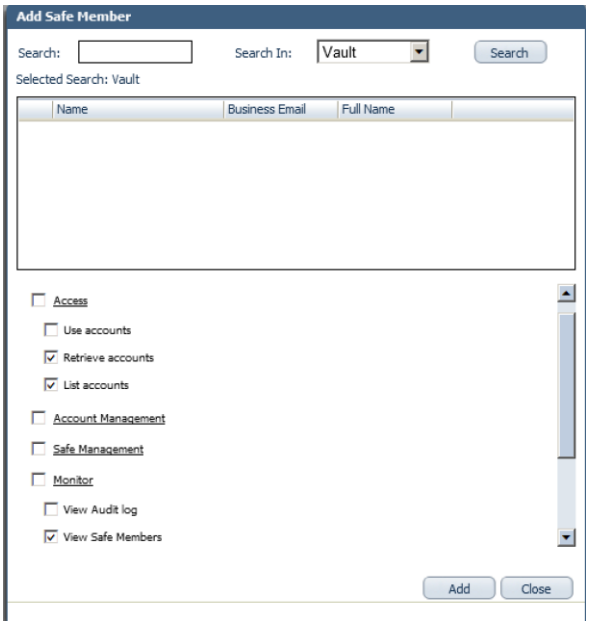
1. In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:
   - **Manually** – Add accounts manually one at a time, and specify all the account details.
   - **Automatically** – Add multiple accounts automatically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

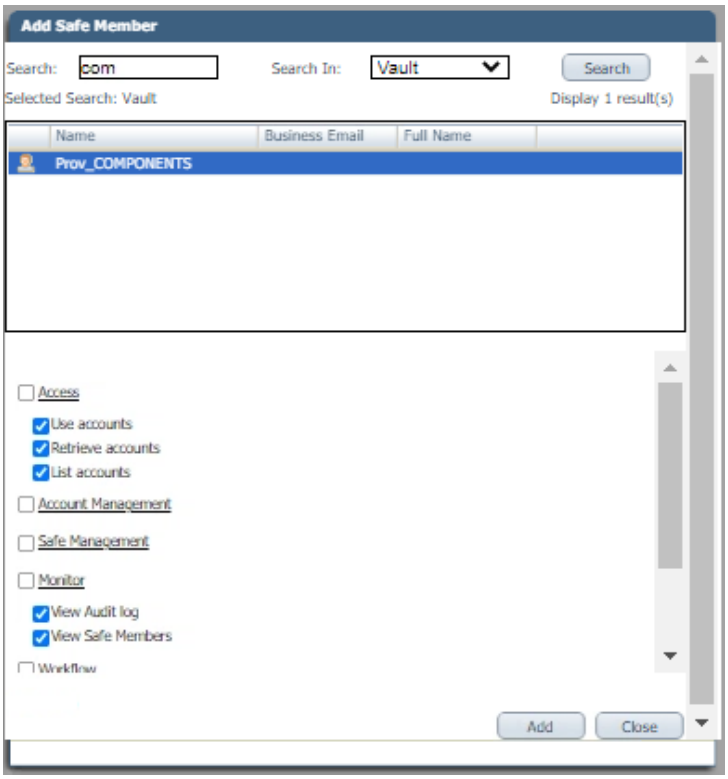
2. Add the Credential Provider and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.
   i. Add the Provider user as a Safe 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.



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

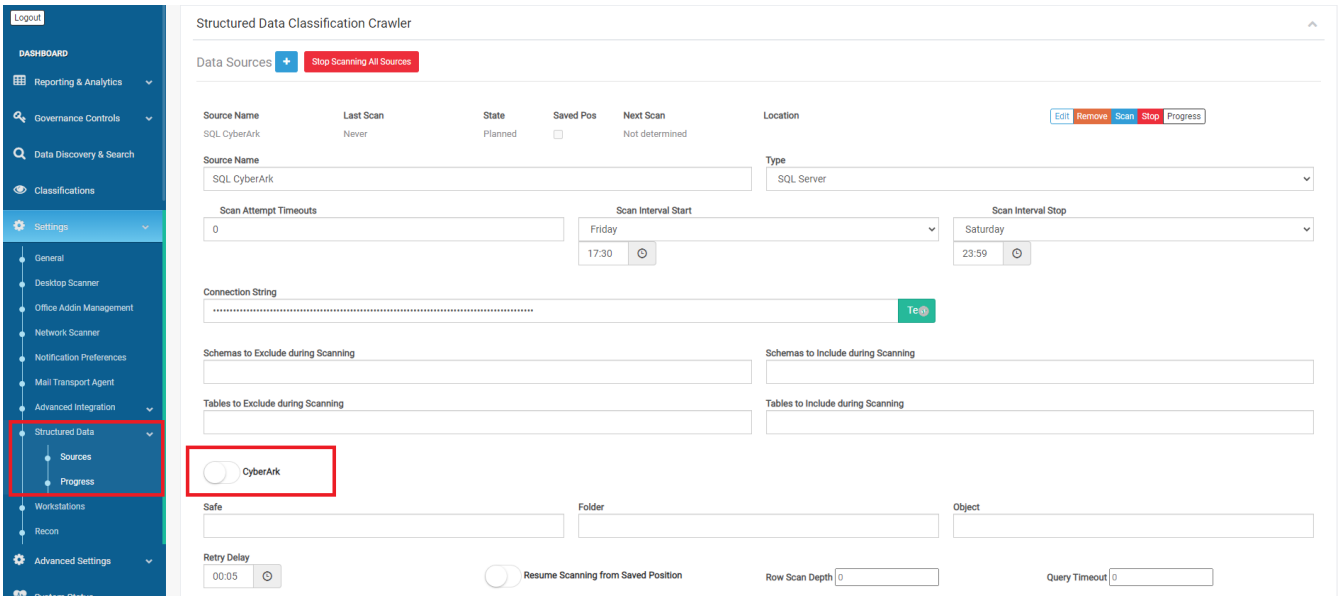
- Retrieve accounts
- Use accounts
- List accounts



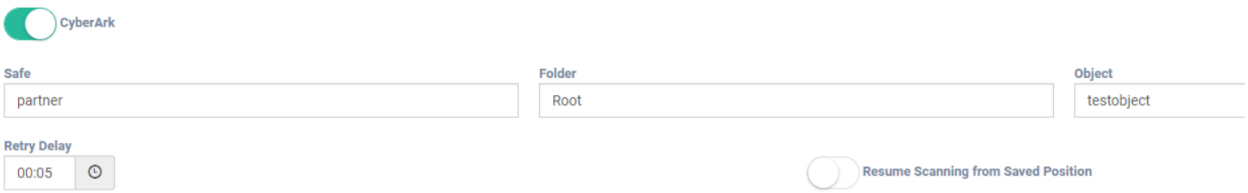
iii. If the Safe is configured for object level access, make sure that both the Provider user and the application have access to the password(s) to retrieve.

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

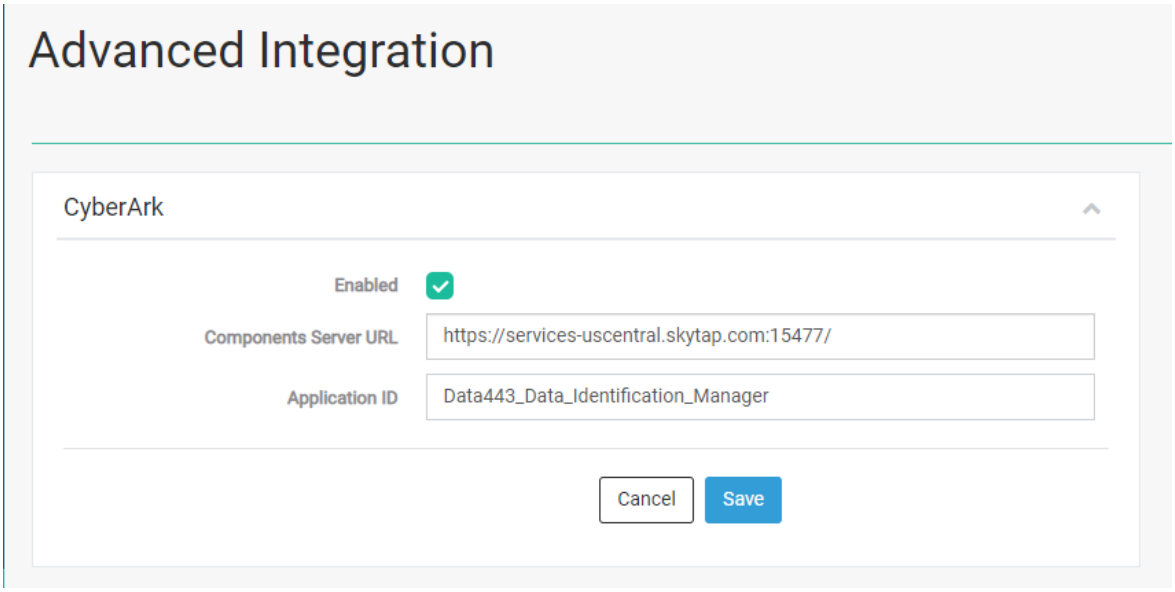
1. Configure the details on the Settings >> Advanced Integrations page
2. You will need 3 pieces of key information in order to configure CyberArk for your structured data source.
    a. Folder - This is “Root” unless you changed it to something else
    b. Safe - The safe that the account resides in
    c. Object - The name of the account we are getting connection string for
3. To enable CyberArk integration for a structured data source go to the structured data sources settings page, and click edit on the structured data source you want to integrate CyberArk with, or create a new structured data source. On either of these interfaces there should be a slider that enables or disables CyberArk.



4. Once enabled three text boxes will appear
    a. Safe: Enter the safe information
    b. Folder: Enter the Folder information
    c. Object: Enter the Object information



5. Save once all fields have been updated



Common use cases:

1. Database Connectivity Credentials
    a. The user will specify: username, address, platform
    b. Safe name – optional but recommended for increasing performance

2. Future: Admin accounts for high value Data Storage services (Shares, etc.)
   The user will specify: username & platform
    a. Safe name – optional but recommended for increasing performance

PARTNER CONTACT INFO

Business Contact	Name	Partner Relations
	Email	partner@data443.com
	Tel	9195261070
Technical Contact	Name	Damien Ostler
	Email	damien.ostler@data443.com
	Tel	9195261070
Support Contact	Name	Support Email
	Email	support@data443.com
	Tel	9195261070