



CYBERARK SECRETS MANAGER

(Agent Based Credential Provider CP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Radiant Logic, Inc.

Website: www.radiantlogic.com

Name of Product: RadiantOne

Version: v7.3.5

Date: June 2019 (Revised 20 May 2021)

RADIANT LOGIC SOLUTION OVERVIEW

Radiant Logic, Inc. is the market-leading provider of Identity and Context Virtualization solutions. Since pioneering the first virtual directory, Radiant Logic has evolved its groundbreaking technology into an enterprise-grade solution, enabling Fortune 1000 companies around the world to solve their toughest identity and data management challenges.

RadiantOne provides secure access to identity and contextual views built out of heterogeneous applications and data sources. The RadiantOne Identity and Context Virtualization platform v7.2 enables authentication and fine-grained authorization for identity management and context-driven applications. RadiantOne delivers fast ROI by reducing administrative effort, simplifying integration tasks, extending the value of existing IT investments, and enabling future identity and data management initiatives.

Customers in a wide range of sectors, including government, defense, banking, and manufacturing, rely on Radiant Logic's RadiantOne Identity and Context Virtualization platform to speed deployment, solve integration challenges, and cut costs for identity and context management projects.

Version: v7.3.5

KEY BENEFITS

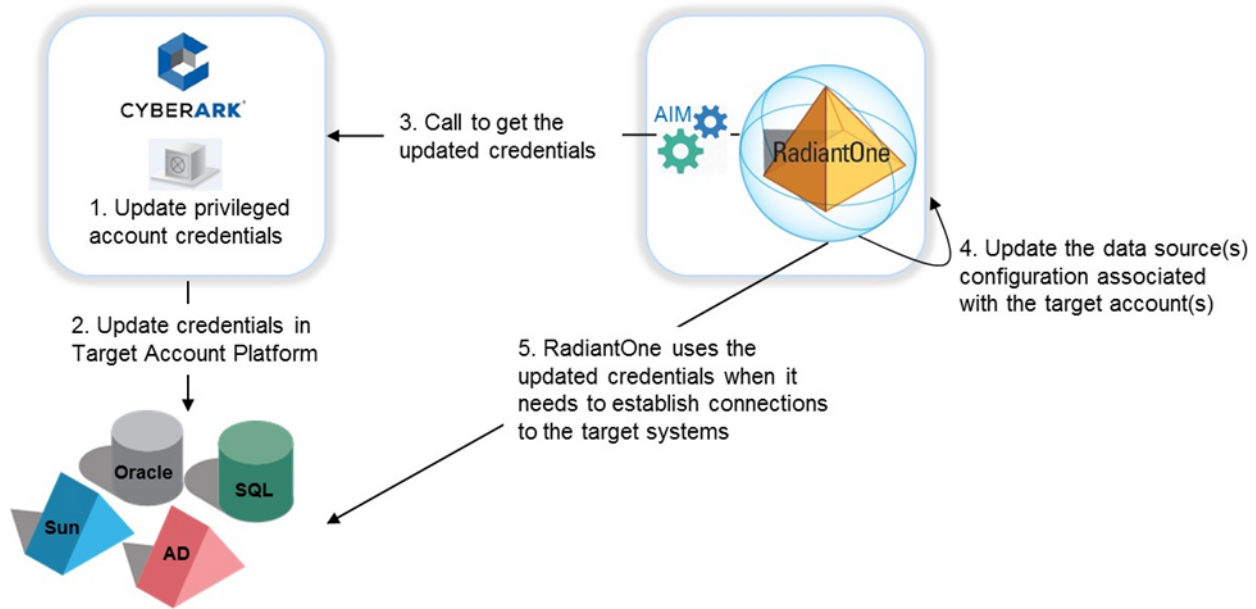
Benefits of RadiantOne:

- Connects to many different heterogeneous data sources to provide a single, aggregated identity reference list that applications can consume to identify, authenticate and authorize end users
- Acts as a client, connecting to various backends with service/privileged accounts that are stored in configuration files

Benefits of integrating RadiantOne with CyberArk Secrets Manager:

- Can leverage CyberArk as the authoritative source for the credentials needed to connect to backend data stores
- Privileged accounts are managed in CyberArk, and RadiantOne can pull the credentials from CyberArk to update its local configuration as needed

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



1. Credentials are updated in CyberArk.
2. CyberArk updates the credentials in the Target Account Platform.
3. A task is triggered in RadiantOne to get the updated credentials from CyberArk.
4. The task updates the corresponding configuration files in RadiantOne.
5. RadiantOne leverages the updated credentials the next time it needs to establish a connection to the target systems.

CREDENTIAL RETRIEVAL

The RadiantOne task can be scheduled to run as frequently as needed to pull the credentials from CyberArk. This integration is available on the following platforms:

Windows 2012 R2 Server

Windows 2016 Server

Red Hat Linux ES 5 or above

Red Hat 8 or above

SUSE Linux Enterprise v10 or above

Ubuntu 9 or above

SECRETS MANAGER INSTALLATION

Refer to the “Credential Provider and ASCP Implementation Guide” for CyberArk Agent based installation and configuration.

Install CyberArk Secrets Manager on the machine where RadiantOne is installed. If RadiantOne is deployed in a cluster, install CyberArk Secrets Manager on all nodes.

SECRETS MANAGER CONFIGURATION

The following sections provide details on RadiantOne configuration with CyberArk Secrets Manager.

DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

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

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

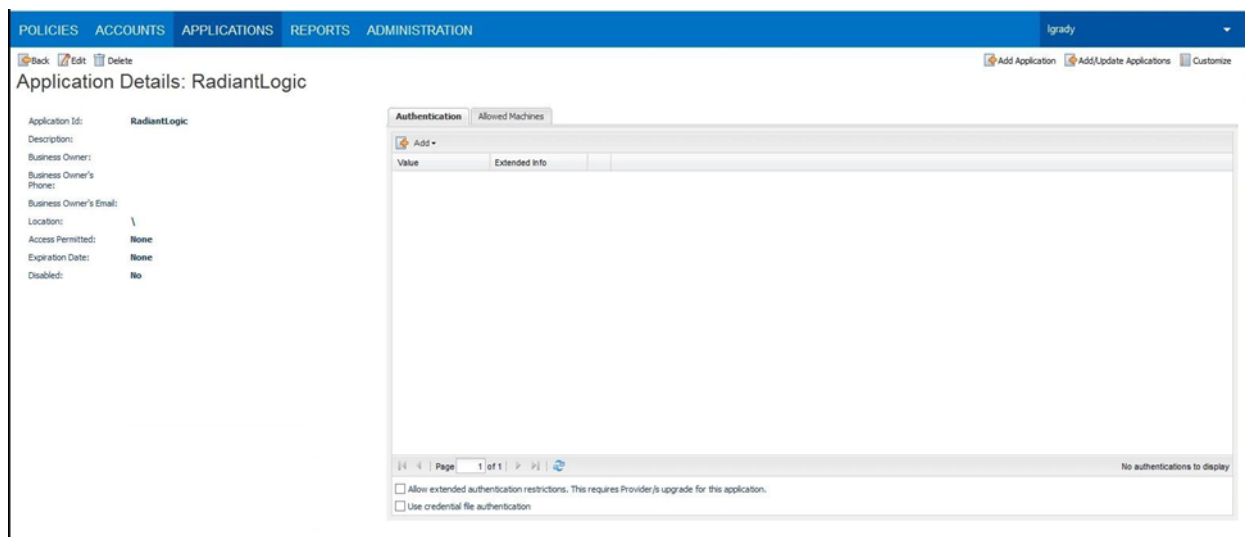
The screenshot shows the 'Add Application' dialog box. It has a title bar with a close button (X). The form contains the following fields and sections:

- Name:** A text box containing 'RadiantLogic'.
- Description:** A text box containing 'Radiant Logic app to pull passwords from CyberArk.'.
- Business owner:** A section header.
- First Name:** An empty text box.
- Last Name:** An empty text box.
- Email:** An empty text box.
- Phone:** An empty text box.
- Location:** A dropdown menu showing a backslash character (\).
- Access Permitted:** A checkbox followed by 'From:' and a dropdown menu, and 'To:' and a dropdown menu.
- Expiration Date:** A checkbox followed by a date picker icon.
- Disabled:** A checkbox.
- Buttons:** 'Add' and 'Cancel' buttons at the bottom right.

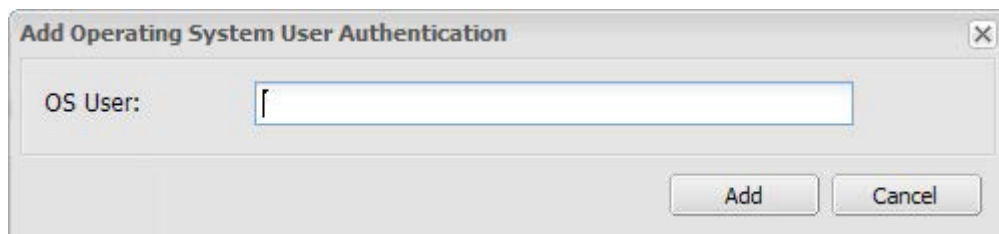
- ☐ Specify the following information:

- In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: RadiantLogic
- In the **Description** box, 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 **Location** box, 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.

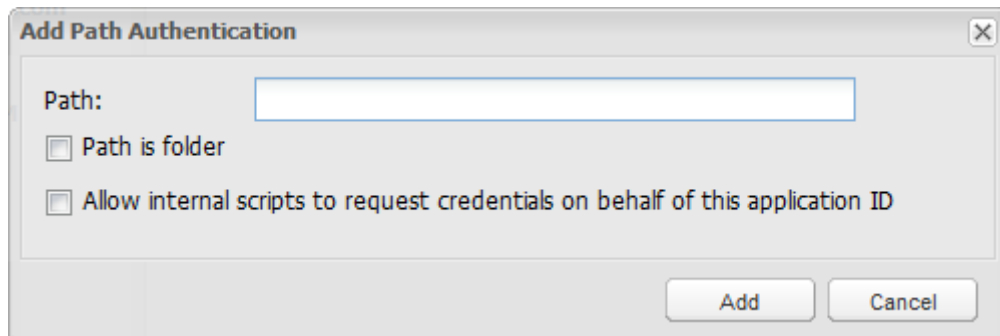
- ☐ Click **Add**. The application is added and is displayed in the Application Details page.



- ☐ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.
- ☐ 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.
- ☐ Select **OS user**. The Add Operating System User Authentication window appears.



- ☐ Specify the name of the OS user who will run the application, then click **Add**. The OS user is listed in the Authentication tab.
- ☐ Select **Path**. The Add Path Authentication window appears.



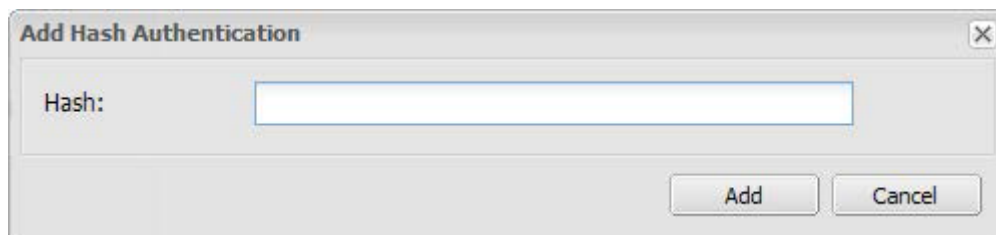
Add Path Authentication

Path:

☐ Path is folder

☐ Allow internal scripts to request credentials on behalf of this application ID

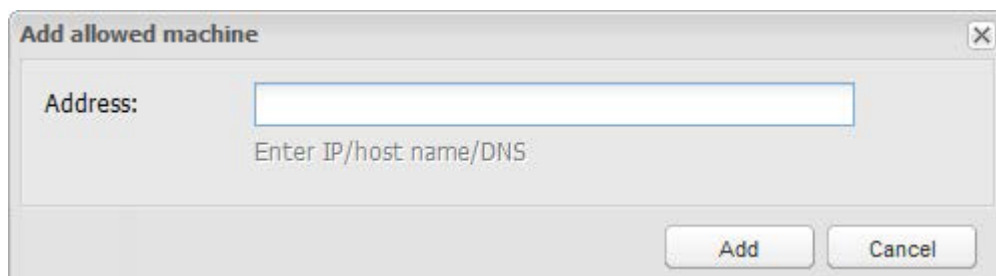
- ☐ In the **Path** box, specify the path where the application will run. To indicate that the specified path is a folder, select **Path is folder**. To allow internal scripts to retrieve the application password for this application, select **Allow internal scripts to request credentials on behalf of this application ID**.
- ☐ Click **Add**. The Path is added as an authentication characteristic with the information that you specified.
- ☐ Specify a hash:
 - Run the AIMGetAppInfo utility to calculate the application's unique hash. Copy the hash value that is returned by the utility.
 - In the PVWA, select **Hash**. The Add Hash window appears.



Add Hash Authentication

Hash:

- 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.
- Click **Add**. The Hash is added as an authentication characteristic with the information that you specified.
- ☐ 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

- In the **Address** box, 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 Secrets Manager 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.

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 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.

☐ 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

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

- Retrieve accounts

Add Safe Member

Search:

Search In: Vault

Search

Selected Search:

Display 26 result(s)

	Name	Business Email	Full Name
	lgrady		
	RadiantLogic		
	vds		
	Backup		
	Operator		
	DR		
	Backup Users		

☐ Access

☐ Use accounts

☒ Retrieve accounts

☐ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☐ View Audit log

☐ View Safe Members

☐ Workflow

Add

Close

- ☐ 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**.

RADIANT LOGIC INSTALLATION & INTEGRATION CONFIGURATION

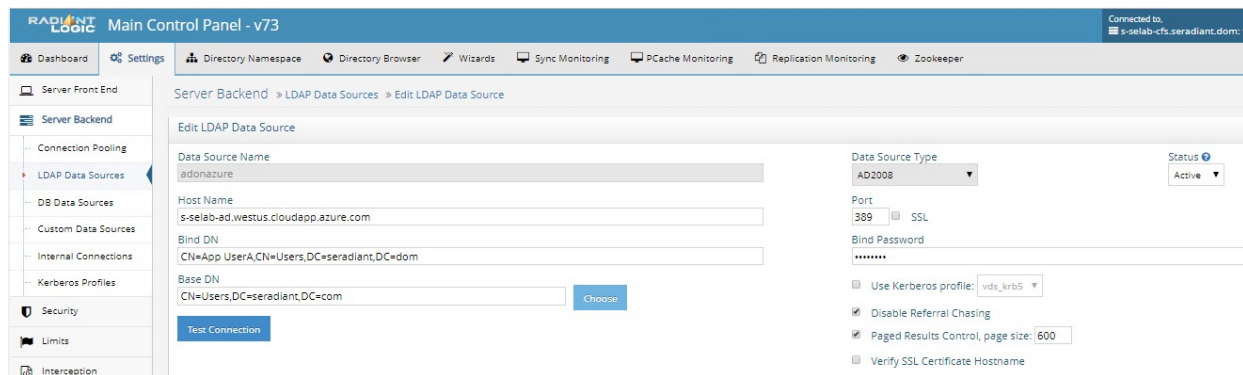
Refer to Radiant Logic's RadiantOne Installation Guide for RadiantOne installation.

DATA SOURCE CONFIGURATION

Configure a RadiantOne data source using credentials that correspond to an Account configured in CyberArk. If RadiantOne is deployed in a cluster, create the data source on one node as it is automatically shared across all nodes.

1. From the RadiantOne Main Control Panel, log in with a RadiantOne administrator account.

2. From the Settings tab > Server Backend section, create data sources for the backend data stores. The example below corresponds to a MS Active Directory (the same MS Active Directory configured as a Target Account Platform in CyberArk).



Note – During the period of time when a password in CyberArk changes and the RadiantOne password synchronization task hasn't run yet, RadiantOne connections to the backend target system will fail. Depending on the password policy in the backend target system, too many unsuccessful connection attempts with a wrong password could temporarily lock the service account. If this account is shared across many client applications, they will all be affected by the locked account. To limit the impact of this potential issue, it is recommended to use a service account dedicated to RadiantOne for the user credentials configured in the data source.

3. Click Save.

CYBERARK TASK CONFIGURATION

The CyberArk configuration files are included with RadiantOne. The files described in this section are located in <RLI_HOME>/config/cyberark/pull_plugin.

IMPORTANT NOTE - If RadiantOne is deployed in a cluster, the following steps should be performed on every node (one at a time).

1. Save cyberark-schedule.bat (cyberark-schedule.sh for Linux platforms) and testcyber.cfg to <RLI_HOME>/vds/bin/advanced. Save javapasswordsdk-9.5.10.jar into <RLI_HOME>/lib.

2. Restart RadiantOne FID.

3. Open the RadiantOne Main Control Panel > Dashboard tab and click on the  button associated with the RadiantOne node. The Server Control Panel launches.

4. In the Server Control Panel, go to the Tasks tab.

5. Click  to restart the task scheduler.

6. Edit testcyber.cfg and configure your safe name, CyberArk folder, CyberArk reason, and then list your RadiantOne data sources using the following syntax (all data sources must correspond to accounts in the same CyberArk safe. You need a testcyber.cfg file for each CyberArk safe):

<RadiantOne data source name>,<name of the password object in CyberArk associated with the account corresponding to the backend>.

Add as many data sources as you want to using this syntax:

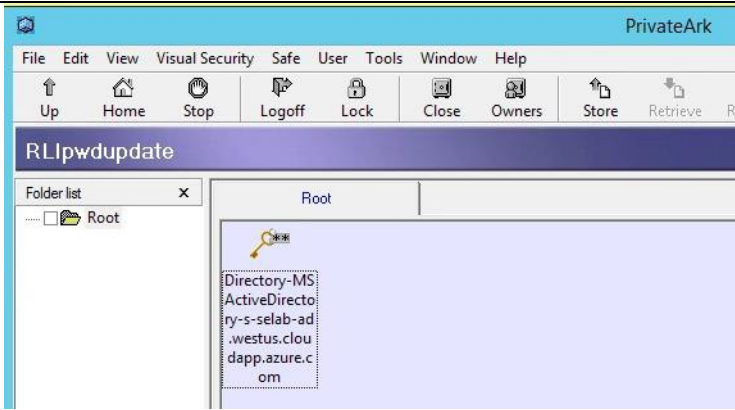
VDS_DATASOURCE.<Next#InSequence>=<data_source_name_in_RadiantOne>,<password_object_name_in_CyberArk>

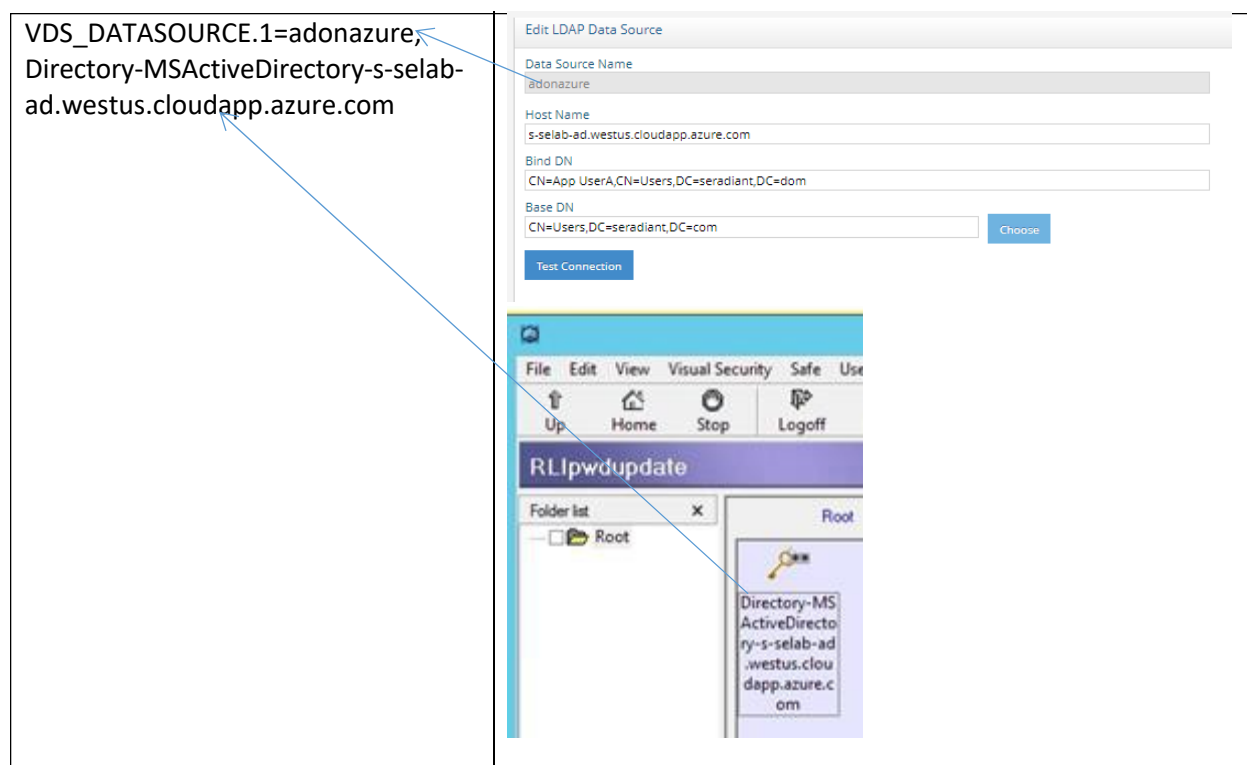
An example of testcyber.cfg is shown below, along with a screen shot of the corresponding configuration in CyberArk.

CYBERARK_APPID=RadiantLogicCYBERARK_SAFE=RLIpwdupdateCYBERARK_FOLDER=Root

CYBERARK_REASON=vds password update test

VDS_DATASOURCE.1=adonazure,Directory-MSActiveDirectory-s-selab-ad.westus.cloudapp.azure.com

Sample Setting in testcyber.cfg	Corresponding Setting in CyberArk
CYBERARK_SAFE=RLIpwdupdate CYBERARK_FOLDER=Root	
CYBERARK_REASON=vds password update test	No corresponding setting in CyberArk.



Note – you can add new data source mappings to the testcyber.cfg file at any time. Every time the task runs, it reads from the corresponding testcyber.cfg file. All accounts that share the same safe in CyberArk should be configured in the same testcyber.cfg file.

7. Create one testcyber.cfg file for each CyberArk safe configured; testcyber.cfg, testcyber1.cfg, testcyber2.cfg...etc.

8. The syntax of the command to configure the RadiantOne task is:
 cyberark-schedule.bat [conf_file] [TaskName]

On the RadiantOne server, open a command prompt and run the following command (examples are shown for Windows platforms). This command configures a task in RadiantOne named: CyberArk RLIpwdupdate Safe

```
cyberark-schedule.bat c:\radiantone\vds\bin\advanced\testcyber.cfg "CyberArkRLIpwdupdateSafe"
```

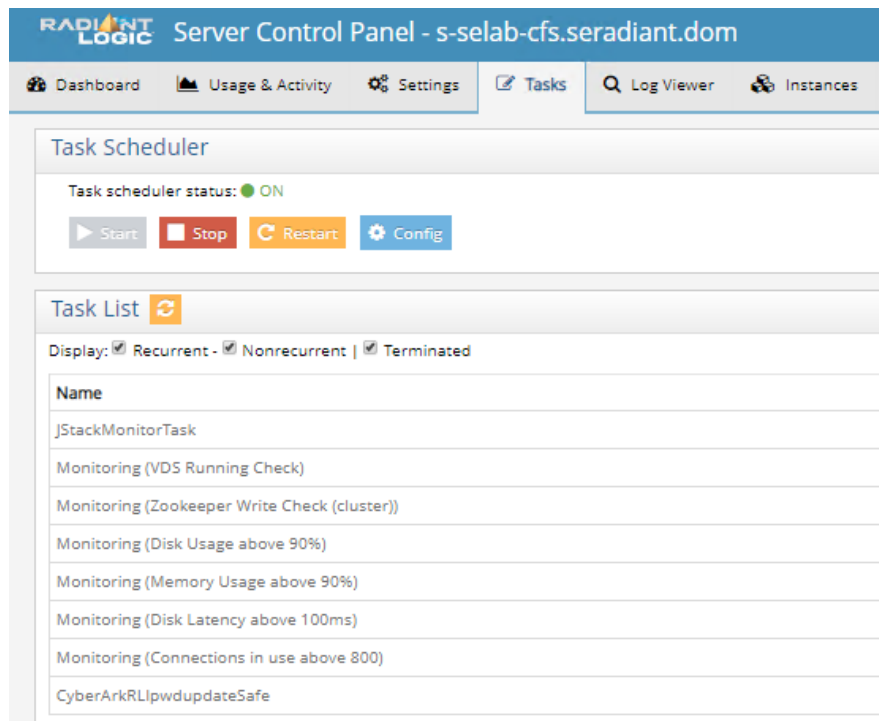
9. Repeat step 4 for each testcyber.cfg file you've configured (testcyber1.cfg, testcyber2.cfg...etc.) with a unique task name for each configuration file.

```
cyberark-schedule.bat c:\radiantone\vds\bin\advanced\testcyber1.cfg CyberArkXXXSafe
cyberark-schedule.bat c:\radiantone\vds\bin\advanced\testcyber2.cfg CyberArkYYYSafe
```

10. Open the RadiantOne Main Control Panel > Dashboard tab and click on the  button associated with the RadiantOne FID leader node (noted with ). The Server Control Panel launches.

11. Click on the Tasks tab.

12. Check the option to display the “Terminated” tasks. You should see tasks corresponding to the names configured in the previous steps. The configured tasks access CyberArk and retrieve the password(s) associated with the account(s) in CyberArk that correspond to the data source(s) configured in RadiantOne.



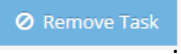
13. The task(s) can be scheduled to run as often as you want to get the credentials from CyberArk. To schedule a task as reoccurring, click the  button next to the task.

14. Check the Recurrent option.

15. Enter the execution interval which is the frequency you want to pull the credentials from CyberArk.

16. Click Reschedule Task.

17. (Optional) If you have deployed RadiantOne in a cluster, remember to perform the steps above on every node so the task is properly configured on each node. Although the task is configured on every node, it will only run on the current leader node.

Note – to remove the task, click the  button and then click . The task must not be recurrent in order to remove it.

PARTNER CONTACT INFO

Business Contact	Name	Eric Ross
	Email	eross@radiantlogic.com
	Tel	415-798-5661
Technical Contact	Name	Lisa Grady
	Email	lgrady@radiantlogic.com
	Tel	415-209-6800x5622
Support Contact	Name	
	Email	support@radiantlogic.com
	Tel	415-209-6800 (Press 2 for Technical Support)