



CYBERARK SECRETS MANAGER

(Agentless Central Credential Provider CCP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Phosphorus Cybersecurity, Inc.

Website: <https://phosphorus.io>

Name of Product: Phosphorus Enterprise

Version: 2020 (Spyglass)

Date: 27 May 2020 (Revised 21 May 2021)

PHOSPHORUS ENTERPRISE OVERVIEW

Phosphorus Enterprise (version 2020, aka Spyglass) for Linux provides secure credential management, firmware updates, patching, and alerts for all the devices in your home or office.

Version: 2020 (Spyglass)

KEY BENEFITS

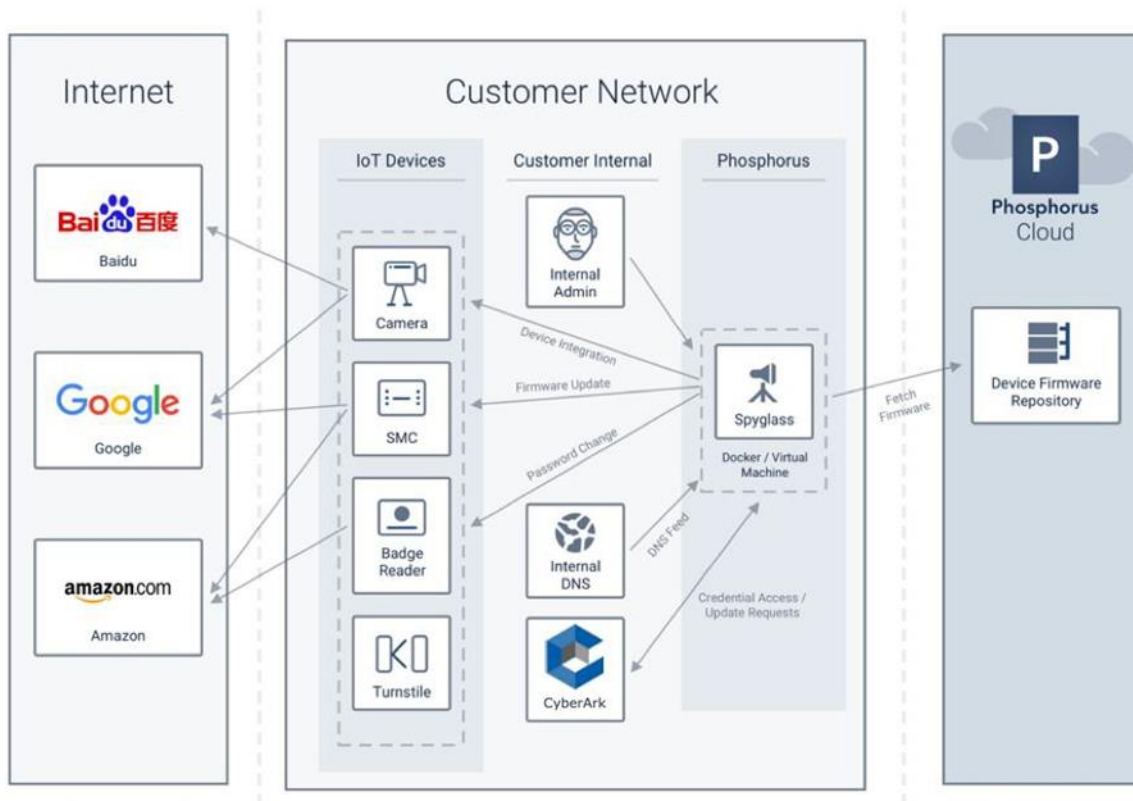
Benefits of Phosphorus Enterprise:

- Passively discovers, monitors, and manages large classes of IoT devices

Benefits of integrating Phosphorus Enterprise with CyberArk Secrets Manager:

- Acts as a one-to-many proxy for CyberArk's credential management, enabling support for many new IoT device types

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER INTEGRATION

CyberArk Secrets Manager is integrated through the Partner Product's initial configuration. The integration runs on the endpoint beside Phosphorus Enterprise or can be run from a central/mid-tier server that has network access to their endpoint server running Phosphorus Enterprise.

Phosphorus Enterprise is only installed on one server.

CREDENTIAL RETRIEVAL

- Credential retrieval is triggered anytime Phosphorus Enterprise needs to perform an authenticated interaction with a device. These interactions include password rotations, password verification, configuration auditing, and firmware updating
- During Phosphorus Enterprise installation and setup, credential retrieval frequency will be high. The system will need to test all credentials to confirm that they are valid for the end devices as well as perform basic configuration audits
- During typical use, credential retrieval frequency will be correlated to Phosphorus Enterprise system use and scheduled policies. Users can schedule configuration audits, firmware updates, and credential rotations (through CyberArk policies). Credentials will only be queried when needed to perform an operation

SECRETS MANAGER INSTALLATION

Refer to the “Credential Provider Implementation Guide” for CyberArk Agentless installation and configuration.

SECRETS MANAGER CONFIGURATION

The following sections provide details on Phosphorus Enterprise 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.

Add Application

Name: PhosphorusEnterprise

Description:

Business owner

First Name:

Last Name:

Email:

Phone:

Location: \

☐ Access Permitted: From: To:

☐ Expiration Date:

☐ Disabled

Add Cancel

☐ Specify the following information:

- In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: PhosphorusEnterprise
- 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. Partner should suggest the authentication details to secure the access by the partner's application.
- ☐ 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.
- ☐ Specify the Certificate Serial Number.

Instructions on how to get the Certificate Serial Number:

Windows:

Start -> certmgr.msc (Current User) -> expand Personal -> select Certificates -> double-click on certificate to open

Start -> certlm.msc (Local Computer) -> expand Personal -> select Certificates -> double-click on certificate to open

If the first two options do not work in your env:

Start -> mmc.msc -> File; Add/Remove Snap-in -> Certificates -> Add -> OK -> you may be prompted to choose Local Computer or Current User -> OK

Expand Certificates -> Personal -> Certificates -> Double-Click on a certificate to open.

Once the certificate is open -> Details tab -> Serial Number is in the list of values shown

Once the certificate is open

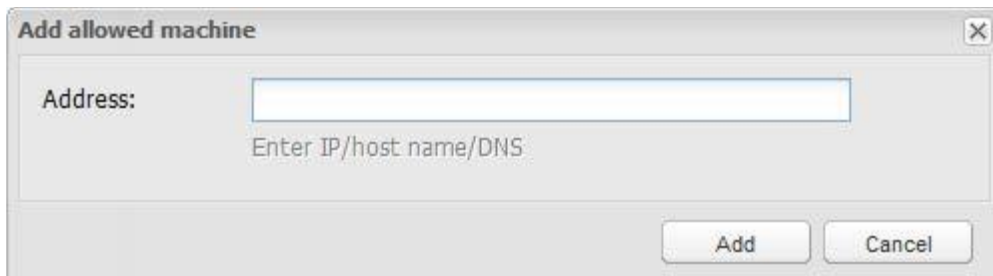
OpenSSL

openssl x509 -in <cert file name> -serial -noout

- This is the most secure way to authenticate the application for CCP
- The following are enhanced ways of authenticating

☐ Specify the application's Allowed Machines. This information enables Secrets Manager 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.



- 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.

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 provider user (where the Central Credential Provider is installed) 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:

Selected Search: Vault Display 1 result(s)

Name	Business Email	Full Name
 Prov_COMPONENTS		

☐ Access

- ☐ Use accounts
- ☒ Retrieve accounts
- ☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

- ☐ View Audit log
- ☒ View Safe Members

☐ Workflow

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

Add Safe Member

Search: PhosphorusEnterp

Search In: Vault

Search

Selected Search: Vault

Display 1 result(s)

Name	Business Email	Full Name
 PhosphorusEnterprise		

☐ 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**.

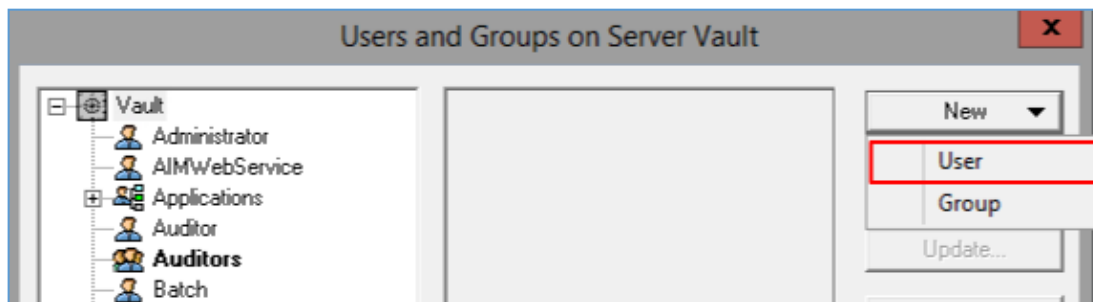
PHOSPHORUS ENTERPRISE INSTALLATION & INTEGRATION CONFIGURATION

Refer to <https://docs.phosphorus.io> for Phosphorus Enterprise installation.

The Phosphorus integration requires a CyberArk user account in order to retrieve and create accounts which is then used to call WebServices API.

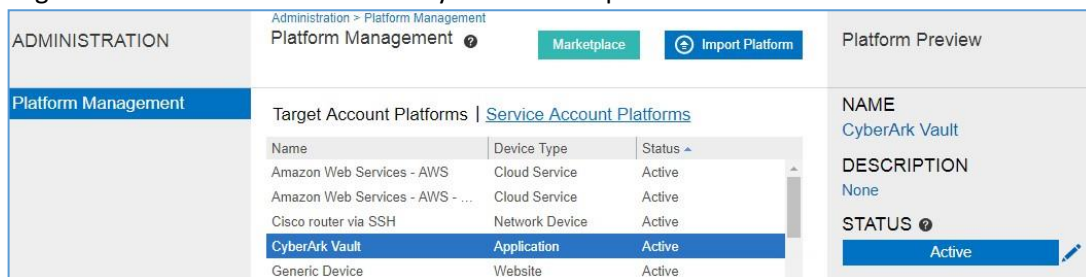
- 1) Create a CyberArk user on the PrivateArk Client. Click on Tools > Administrative Tools > Users

and Groups... Then Select New > User:



- The recommended User Name is **phosphorus_user**
- Ensure to give the user a password in the **Authentication** tab
- It is recommended to enable **Password Never Expires** in the **Authentication** tab
- Do **not** give this user any group memberships nor CyberArk privileges

2) Login to the PVWA and enable the CyberArk Vault platform:



- 3) Create a privileged account in the Phosphorus Safe in order to manage the user credential created in step #1:

The screenshot shows the 'Add Account' wizard. On the left, a progress bar indicates four steps: 1. Select system type, 2. Assign to platform, 3. Store in Safe, and 4. Define properties. Step 1 is active. The main area shows '1. Select system type' with two options: 'Network Device' and 'Application'. 'Application' is selected and highlighted with a red box. Below this, '2. Select platform' shows two options: 'CyberArk Vault' and 'RSA Authentication Manager'. 'CyberArk Vault' is selected and highlighted with a red box.

The **username** and **password** *must* match the account created in step #1. Ensure to enable

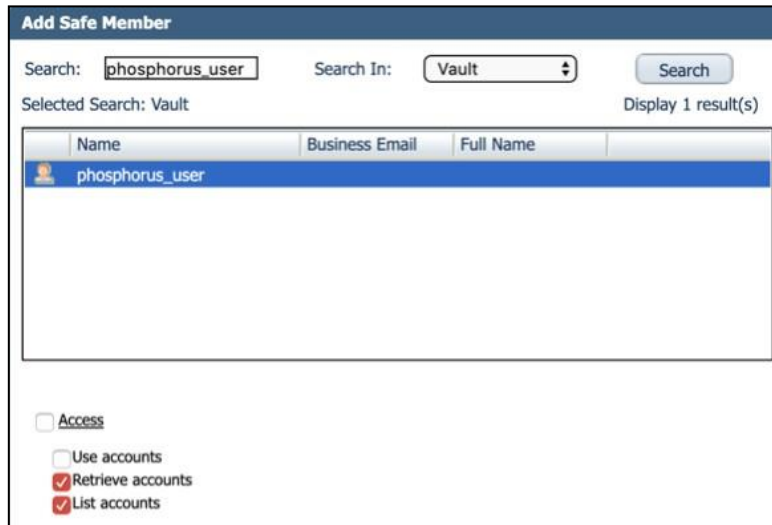
Customize account name and use the same value as the Username.

The screenshot shows the 'Add Account' wizard at step 4, 'Define account properties'. The progress bar on the left shows steps 1 through 4, with step 4 being the current step. The main area is titled '4. Define account properties' and contains 'Primary properties' with the following fields: 'Username' (phosphorus_user), 'Address' (N/A), 'Password (optional)' (masked with dots), and 'Confirm Password' (masked with dots). At the bottom, there is a checkbox labeled 'Customize account name' which is checked and highlighted with a red box. Below this checkbox is a text field containing 'phosphorus_user'.

- 4) Add the Phosphorus User as a Safe Member in the Phosphorus Safe with the following permissions:

- Retrieve accounts

- List accounts



Add Safe Member

Search: Search In:

Selected Search: Vault Display 1 result(s)

Name	Business Email	Full Name
 phosphorus_user		

☐ Access

☐ Use accounts

☒ Retrieve accounts

☒ List accounts

The Phosphorus Enterprise integration requires two platforms to be installed from the CyberArk marketplace.

1) PHOSPHORUS ENTERPRISE USERS

- <https://cyberark-customers.force.com/mplace/s/#a352J000000pdWOQAY-a392J000001h4NiQAI>

2) PHOSPHORUS END DEVICE USERS

- <https://cyberark-customers.force.com/mplace/s/#a352J000000pdWJQAY-a392J000001h4NdQAI>

Once both platforms are downloaded, go to **Administration > Platform Management** and import both platforms into CyberArk. When the platforms have been imported, the following configuration edits must be made:

Note: Depending on platform version, some of these configurations may already be set. Ensure the configuration options of the platforms match those shown here.

PHOSPHORUS ENTERPRISE USERS

Phosphorus Enterprise Users via REST

Search...
Go

- Target Account Platform
 - UI & Workflows
 - Automatic Password Management
 - General
 - Privileged Account Management
 - CPM Plug-in
 - Password Change
 - Password Verification
 - Notifications
 - Generate Password
 - Additional Policy Settings
 - General Properties

Name
Value

PromptsFilename

ProcessFilename

Port
443

protocol

ChangeCommand

ReconcileCommand

ConnectionCommand

DSN

ReconcileWinAccount
No

ReconcileWinExtraConnectionString
Trusted_Connection=yes;

UseSSL
IgnoreUntrustedCertificate

Phosphorus Enterprise Users via REST

Search...
Go

- Target Account Platform
 - UI & Workflows
 - Automatic Password Management
 - General
 - Privileged Account Management
 - CPM Plug-in
 - Password Change
 - Password Verification
 - Notifications
 - Generate Password
 - Additional Policy Settings
 - General Properties

Name
Value

PolicyID
PhosphorusEnterpriseUsers

PolicyName
Phosphorus Enterprise Users via REST

PolicyType
Regular

ImmediateInterval
1

Interval
1440

MaxConcurrentConnections
3

SearchForUsages
No

LooselyConnectedDevices
No

AllowedSafes
.*

Once the **Phosphorus Enterprise Users** platform has been configured, an account must be created.

- 1) Login to the PVWA and navigate to Accounts
- 2) Click 'Add account' [Add account](#)
- 3) For 'Select system type' select 'Imported Platforms'

1 Select system type
2 Assign to platform
3 Store in Safe
4 Define properties

1. Select system type

Azure web services

Database

Security Appliance

Network Device

Application

Remote Access

Directory

Website

Operating System

Misc

Cloud Service

Imported Platforms
Select

4) For 'Assign to platform' select 'Phosphorus Enterprise Users via REST'

The screenshot shows a configuration wizard with a sidebar on the left containing four steps: 1. Select system type (Imported Platforms), 2. Assign to platform, 3. Store in Safe, and 4. Define properties. Step 2 is currently active. The main area is titled '2. Select platform' and contains two selectable options: 'Phosphorus End Device Users via REST' and 'Phosphorus Enterprise Users via REST'. The second option is highlighted with a red rectangular border.

5) For 'Store in Safe' select the safe created in **Provisioning Accounts And Setting Permissions For Application Access Step #1**

The screenshot shows the same configuration wizard, but now step 3, 'Store in Safe', is active. The sidebar shows steps 1, 2, 3, and 4, with step 3 highlighted. The main area is titled '3. Select Safe' and contains two selectable options: 'PasswordManager' and 'PhosphorusSafe'. The second option, 'PhosphorusSafe', is highlighted with a red rectangular border.

6) For 'Define properties' specify the following account information

- a. **Address** is the URL of the PhosphorusEnterprise instance e.g. **spyglass.example.com**
 - i. Note: do not specify http/https or a port here. The port is defined in the platformconfiguration above
- b. **Username** is cyberark@phosphorus.io
- c. **Password** is **Cyberark1**
 - i. Note: This password can be changed via CyberArk PVWA in the PhosphorusSafe once the installation is complete
- d. Select **Customize account name** and specify cyberark@phosphorus.io
- e. Click 'Add'

PHOSPHORUS END DEVICE USERS

Phosphorus End Device Users via REST

Search... Go

- Target Account Platform
 - UI & Workflows
 - Automatic Password Management
 - General
 - Privileged Account Management
 - CPM Plug-in
 - Password Change
 - Password Verification
 - Notifications
 - Generate Password
 - Additional Policy Settings
 - General Properties

Properties

| Name | Value |
|-----------------------------------|----------------------------|
| PromptsFilename | |
| ProcessFilename | |
| Port | 443 |
| protocol | |
| ChangeCommand | |
| ReconcileCommand | |
| ConnectionCommand | |
| DSN | |
| ReconcilesWinAccount | No |
| ReconcileWinExtraConnectionString | Trusted_Connection=yes; |
| UseSSL | IgnoreUntrustedCertificate |
| RestartAppPool | No |

Phosphorus End Device Users via REST

Search... Go

- Target Account Platform
 - UI & Workflows
 - Automatic Password Management
 - General
 - Privileged Account Management
 - CPM Plug-in
 - Password Change
 - Password Verification
 - Notifications
 - Generate Password
 - Additional Policy Settings
 - General Properties

Properties

| Name | Value |
|--------------------------|--------------------------------------|
| PolicyID | PhosphorusEndDeviceUsers |
| PolicyName | Phosphorus End Device Users via REST |
| PolicyType | Regular |
| ImmediateInterval | 1 |
| Interval | 1440 |
| MaxConcurrentConnections | 3 |
| SearchForUsages | No |
| LooselyConnectedDevices | No |
| AllowedSafes | * |

Phosphorus End Device Users via REST

Search... Go

- Target Account Platform
 - UI & Workflows
 - Automatic Password Management
 - General
 - Privileged Account Management
 - CPM Plug-in
 - Password Change
 - Password Verification
 - Notifications
 - Generate Password
 - Additional Policy Settings
 - General Properties

Properties

| Name | Value |
|-------------------------------------|-------|
| AllowManualChange | Yes |
| PerformPeriodicChange | No |
| HeadStartInterval | 5 |
| FromHour | -1 |
| ToHour | -1 |
| ChangeNotificationPeriod | -1 |
| DaysNotifyPriorExpiration | 7 |
| ExecutionDays | |
| EnforcePasswordPolicyOnManualChange | No |
| EnforcePasswordVersionsHistory | 7 |

Target Account Platform

- UI & Workflows
 - Properties
 - Required
 - Optional

Add Property

Delete

Copy

Paste

Move Up

Move Down

Phosphorus End Device Users via REST

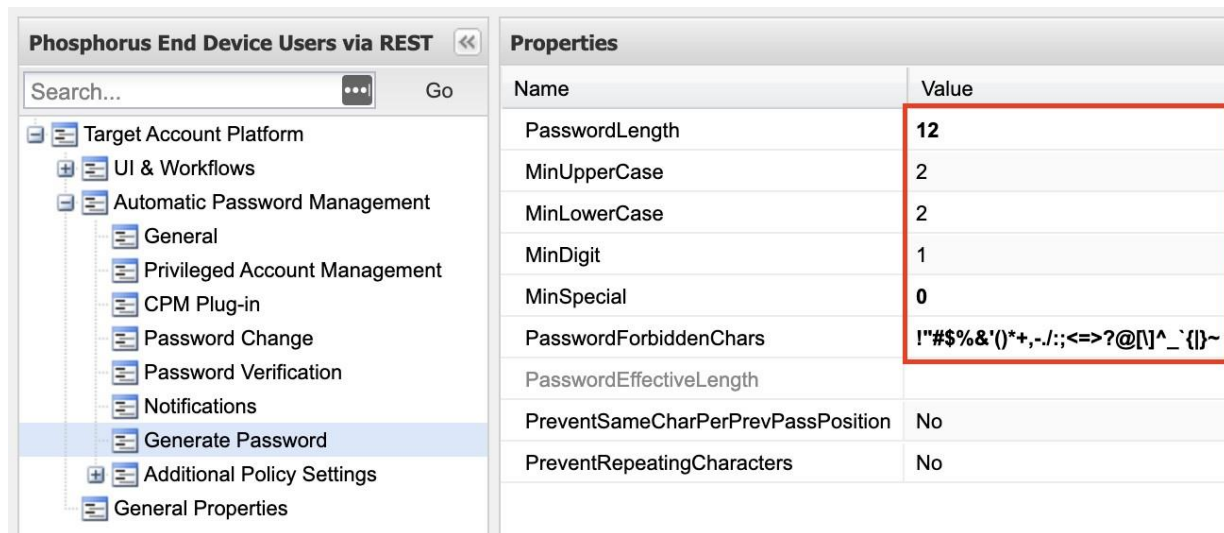
Search... Go

- Target Account Platform
 - UI & Workflows
 - Properties
 - Required
 - Optional
 - ExtraPass1Name
 - ExtraPass1Folder
 - ExtraPass1Safe

Properties

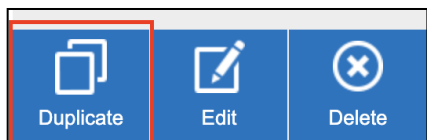
| Name | Value |
|-------------|----------------|
| Name | ExtraPass1Name |
| DisplayName | |
| ResolveFrom | |

PasswordForbiddenChars: !"#\$%&'()+,-./:;<=>?@[\\]^_`{|}~*



| Name | Value |
|------------------------------------|------------------------------------|
| PasswordLength | 12 |
| MinUpperCase | 2 |
| MinLowerCase | 2 |
| MinDigit | 1 |
| MinSpecial | 0 |
| PasswordForbiddenChars | !"#\$%&'()*+,-./:;<=>?@[\\]^_`{ }~ |
| PasswordEffectiveLength | |
| PreventSameCharPerPrevPassPosition | No |
| PreventRepeatingCharacters | No |

Note (optional): The above generic PasswordForbiddenChars policy is only necessary during Phosphorus Enterprises automatic account creation/enrollment. Once a device is enrolled, if more specific password policies are required, the PhosphorusEndDeviceUsers platform can be duplicated. The PasswordForbiddenChars of the duplicated platform can then be modified to meet the desired policy requirements and applied to the preexisting account(s).



Edit Account: Phosphorus End Device Users via REST-ExampleAccount-127.0.0.1

| | | | |
|--|---|------------|----------------------------------|
| Store in Safe: | PhosphorusSafe | Change to: | Imported Platforms |
| Device Type: | Imported Platforms | Change to: | PhosEndDeviceUsersDuplicateExamp |
| Platform Name: | Phosphorus End Device Users via REST | Change to: | |
| Address: | 127.0.0.1 | Change to: | |
| Username: | ExampleAccount | Change to: | |
| Required Properties: | | Change to: | |
| Optional Properties: | | Change to: | |
| ☐ ExtraPass1Name: | | Change to: | |
| ☐ ExtraPass1Folder: | | Change to: | |
| ☐ ExtraPass1Safe: | | Change to: | |
| ☐ Disable automatic management for this account | | Reason: | |

[Show advanced section](#)

Once Phosphorus Enterprise is installed, configure the integration:

1. Login to the Phosphorus Enterprise instance <https://spyglass.example.com/>
2. Navigate to the credential provider settings <https://spyglass.example.com/settings/provider>
3. Click the Create Provider button 
4. Select '**CyberArk**' from the Provider dropdown menu
5. In the '**Name**' field, specify a custom name for the provider. The recommended name is '**CyberArk**'
6. In the '**URL**' field, specify the URL for the login page of CyberArk
 - a. e.g. <https://cyberark.example.com:8000/PasswordVault>
7. In the '**Safe Name**' field, specify the name of the safe created in **Provisioning Accounts And Setting Permissions For Application Access Step #1**
 - a. The recommended Safe Name was '**PhosphorusSafe**'
8. In the '**App ID**' field, specify the Application Name/ID created in **Defining The Application ID (APPID) And Authentication Details Step #2**
 - a. The recommended Application ID was '**PhosphorusEnterprise**'
9. In the '**Username**' field, specify the username created in **CyberArk User Account Setup Step #1**
 - a. The recommended Username was '**PhosphorusUser**'
10. In the '**Endpoint**' field, specify the URL of the CyberArk API endpoint
 - a. e.g. <https://cyberark.example.com:8000>
11. (*optional*) Create a client certificate and add the certificate serial number to CyberArk (**Secrets Manager Configuration Step #5**). Place the client certificate file and certificate key file in **/opt/spyglass/conf/certs**.
 - a. In the '**Certificate**' field, specify the name of the certificate file
 - b. In the '**Certificate Key**' field, specify the name of the certificate key file
12. (*optional*) Select the 'Default Provider' checkbox to make this provider the main credential provider for Phosphorus Enterprise
13. Refer to <https://docs.phosphorus.io> for more detailed instructions and updates to this process

DISABLE SAFE CACHING (OPTIONAL)

By default, the CyberArk AIMWebService caches passwords. This means that the password returned by the AIMWebService can potentially be out-of-sync with the password in the Vault for several minutes. Phosphorus Enterprise is aware of this, and handles it, but this can cause password change operations to take several minutes while Phosphorus Enterprise waits for the passwords to sync.

By disabling the cache, password change operations will complete without delay. This is an **optional** configuration. To disable the cache:

1. In the server where the AIMWebService is installed, navigate to **C:\Program Files (x86)\CyberArk\ApplicationPasswordProvider** and open the file named **basic_appprovider.conf** using a text editor
2. Note the value of **AppProviderVaultParmsFile** parameter
3. Connect to the vault, and in the safe **AppProviderConf** open the file with the name of the **AppProviderVaultParmsFile** parameter
4. In the **[Cache]** section, set the value of **CacheLevel** to **None (CacheLevel=None)**
5. Save the file, and return it to the safe
6. Restart the service named **CyberArk Application Password Provider**

PARTNER CONTACT INFO

| | | |
|-------------------|-------|--|
| Business Contact | Name | Chris Rouland |
| | Email | chris@phosphorus.io |
| | Tel | 706-347-6874 |
| Technical Contact | Name | Thomas Ariano |
| | Email | thomas@phosphorus.io |
| | Tel | 678-451-5235 |
| Support Contact | Name | Phosphorus Support |
| | Email | contact@phosphorus.io |
| | Tel | 760-410-8997 |