



CYBERARK SECRETS MANAGER

(Agentless Central Credential Provider CCP)

SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: Beyond Security

Website: www.beyondsecurity.com

Name of Product: beSECURE

Version: 9.8.5

Date: 5 September 2019 (Revised 27 October 2020)

BEYOND SECURITY OVERVIEW

beSECURE™ (AVDS) is a vulnerability assessment and management solution. beSECURE is a flexible, accurate, low maintenance Vulnerability Assessment and Management solution that delivers solid security improvements:

- Continually scan for network and application vulnerabilities
- Daily updates and specialized testing methodologies to catch 99.99% of detectable vulnerabilities
- Data driven, flexible reporting options to empower remediation teams
- *Bug bounty program* for any discovered proven false positives!
- Complete organizational control
- Designed to get you the most accurate and fastest possible improvement in network security customized for your organization's needs.

beSECURE cloud and deployed versions starting from version 9.8.5 support integration with CyberArk Secrets Manager. With this integration, customers of both beSECURE and CyberArk can benefit from increased security by leveraging beSECURE ability to continuously scan targets running Windows and UNIX and leveraging CyberArk robust password management capabilities.

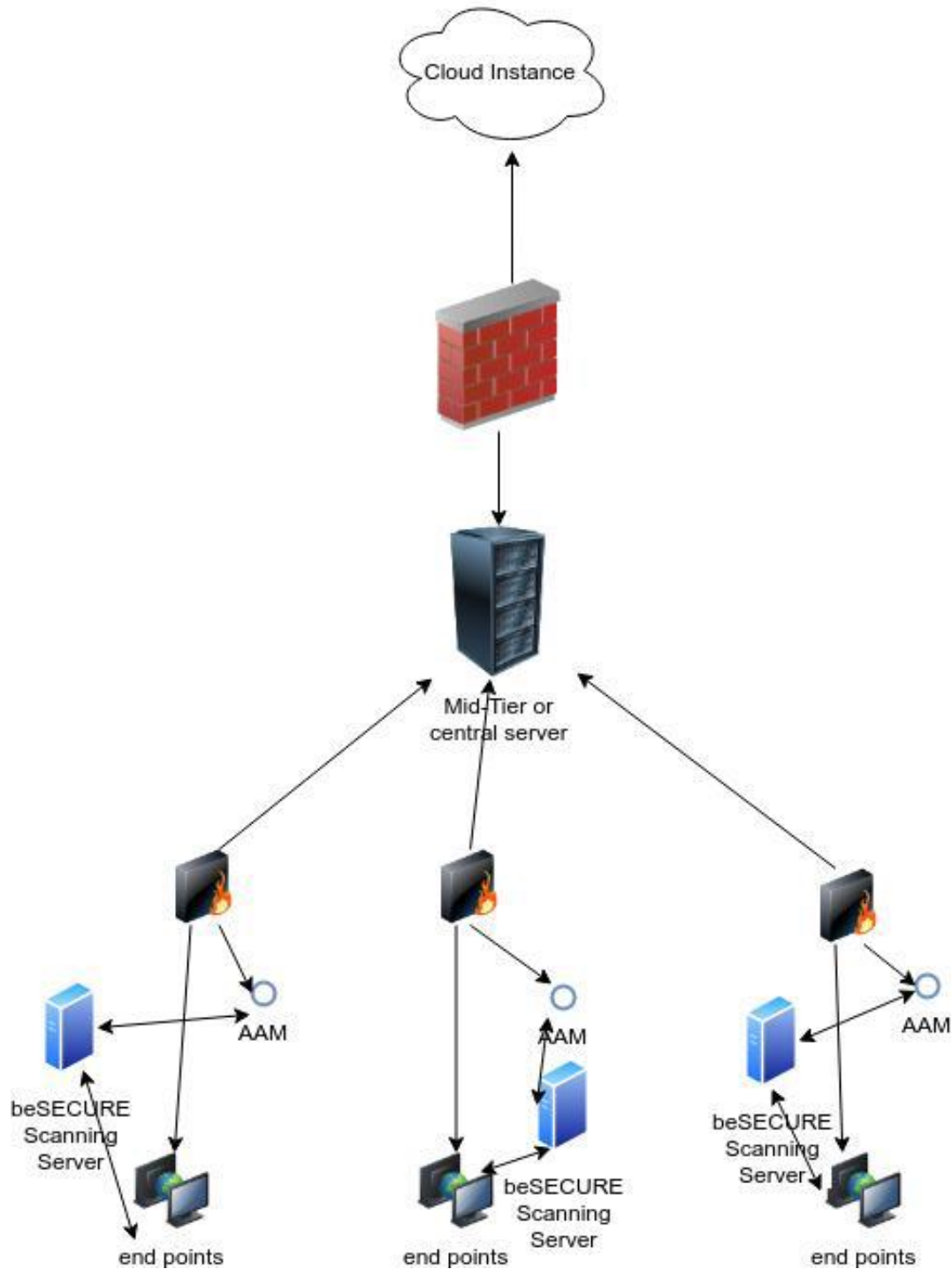
Version: 9.8.5

KEY BENEFITS

By utilizing the credentials retrieved from CyberArk using Secrets Manager the beSECURE administrator can perform more in-depth, credentials based, vulnerability scans on servers and workstations, without exposing those credentials to additional management systems and without needing to update the beSECURE scanning configuration when credentials are changed or updated.

This seamless integration provides the immediate ability to perform beSECURE credentials-based scans on any server whose credentials are in the Secrets Manager system.

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



SECRETS MANAGER INTEGRATION

beSECURE performs authenticated Windows (via SMB) and UNIX (via SSH) scans, where the aim of the scan is to provide up-to-date security posture information about the target by examining it for security vulnerability, policy violations, lack of mitigations, legacy software, and more.

CREDENTIAL RETRIEVAL

beSECURE can either store the authentication credentials locally on the scanning device or on a third-party server – in this case CyberArk.

The beSECURE integration with Secrets Manager takes part on the scanner device, that may be in several physical locations or virtual locations on the customer's premises.

A typical customer would have one or more scanner at their location, depending on the size and frequency of the scans being performed by the beSECURE system.

After an administrator configures a scan to utilize Secrets Manager credentials rather than stored credentials, the settings of the scan change such that every time a scan initiates, before the scan begins to perform the actual scan the scanner will contact the Secrets Manager server and retrieved the relevant credentials for use.

Scans are usually done daily, therefore one request for credentials will be performed at the beginning of the scan.

For Windows, the Username and Password for login is required, the provided user should have Administrative of Power User privileges as Files and Registry access is required in order to assess the security posture of the scanned device.

For UNIX, a Root or root equivalent user access is required, a non-root user is possible for use but sudo access permissions is required in that case. The UNIX user should be able to access files under the /etc/ folder, the list of installed packages (fore example, dpkg or rpm), running processes, and more.

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 Beyond Security 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: beSECURE

Description: Beyond Security's beSECURE integration with AAM
Allows beSECURE's scanners to access remote systems without storing locally credentials for the targets being scanned.

Business owner

First Name:

Last Name:

Email: support@beyondsecurity.com

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: beSECURE
- 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.

Back Edit Delete

Application Details: beSECURE

ApplicationId: beSECURE
Description:
Business Owner:
Business Owner's Phone:
Business Owner's Email: support@beyondsecurity.com
Location: \
Access Permitted: None
Expiration Date: None
Disabled: No

Authentication Allowed Machines

Add ▾

Value	Extended Info
-------	---------------

- ☐ 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.

Add Operating System User Authentication

OS User:

Add Cancel

- ☐ 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.

Add Certificate Serial Number Authentication

Value Extended Info

SN:

Add Cancel

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

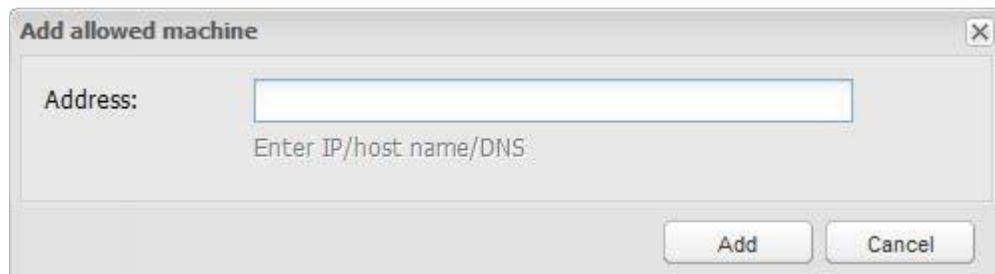
OpenSSL

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:

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:

Search

Selected Search: Vault

Display 1 result(s)

	Name	Business Email	Full Name
	beSECURE	support@beyond...	

☐ Access

☐ Use accounts
 ☒ Retrieve accounts
 ☐ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☐ View Audit log
 ☐ View Safe Members

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**.

BEYOND SECURITY INSTALLATION & INTEGRATION CONFIGURATION

Refer to Beyond Security for Beyond Security installation.

To configure beSECURE, follow the following steps:

Configure beSECURE's Credentials Storage to utilize the third-party CyberArk Secrets Manager for its passwords, login to beSECURE and access the Credentials Storage page:

Storage Location: CyberArk Application Identity Manager (AAM) ▼

CyberArk Application Identity Manager (Application Access Manager)

CyberArk IP Address or FQDN (and port if differs 443): services-uscentral.skytap.com:12091

AppID: BeyondSecurity

Query: ? Safe=Test;Folder=Root;Object=linux2

Here you need to create a new Credentials Storage that utilizes under the “Storage Location” the “CyberArk Application Access Manager” followed by the:

- FQDN or IP address of the server - either a deployed solution or a cloud-based solution followed by a Port number if the 443 port is not used, for example: services-uscentral.skytap.com:12091)
- AppID - The Application ID you have configured in CyberArk for beSECURE to use, in this case we used “beSECURE”. You can review which Applications have been configured by accessing the Applications page and searching for the relevant ApplicationID:
- Query - This should be a valid CyberArk Secrets Manager query of the form **Property=Value;Property=Value; ... Property=Value** which are the values seen in the CyberArk system (under the “Advanced” information view of the account you created). For example: **Safe=Test;Folder=Root;Query=linux2**

Finally, paste the Certificate and Key information into the UI:

Settings Permissions Other

ID: 182F1BED

Name: CyberARK

Authentication Storage: CyberArk Application Identity Manager (AAM) ▼

CyberArk Application Identity Manager (Application Access Manager)

CyberArk IP Address or FQDN (and port if differs 443): services-uscentral.skytap.com:12091

AppID: BeyondSecurity

Query: ? Safe=Test;Folder=root;Object=windows1

Client Side Certificate: ?

Serial Number: Certificate has not been provided

```
-----BEGIN PRIVATE KEY-----
MIIEQgIBADANBgkqhkiG9w0BAQFAASCCSwwggAqAgEAAoICAQCvng8y7MPudZcFS
jG8NcNwRfhdJn1kyc+C2BIsNiNy21bWsaMo3Fg9BdoPyVYarVMGK3PaUQNM
+Ud1wYoUEddz61vXPUL1/jvRCKx7p1iPxIEdiaU2y7vwr4bXhUdtfJuziyz2pVm2
muUfVfz9F2aoDItbwD1hz/2X81wgE2A0Pk8q4c01JX6Ah/cpd6R+vpkn868iUc
i0V1VeDvBAQ+FASTAZ9QZvqvdrGe75Jbk2Fko1ReZHY8zo2i0diVG4xx4ga1v518
cDOCYB3wfiKz/qwtH1X08gsAt0PaG3cHI2Dozvx8vqULtMeK/FD6AmvCG+LxsE1g
swxfFhB2e9W02cdC+1Sve780sCbzuxejZX8VshIG152H81YwdCs0pozFFtmZAIW
rBN0/UKTSFX/aIU9LVnC3gQ8qAB1RD82ZbwpabAlmU1/0qPvnm3b4ELTxzu408+u
juxiHLpxH5GaeW/b688BMcInF2Ma1Vki86X0XKgeYah5famb5vNoZ21duBx3dcJw
0KMxeh2eU0n66cMbzWRNg8mhrBG1LWf9uR/K11Tkrk188R2Xu+4C3uvF92Z9bAP
/p85SwZyxWn2IFY2nt2LiUD2tUVINPe0sC4t08fNuEvNG6LZ2pf.01kpQRzyve1Y
xTehFDcUjRmBK3czfz01ebk5a/v0IDAQABAoICAQYNa133XyYAYukC1RDkWPcg
qYy5SVmsukm3dXY/BeZpRXBQ8I05TU2i+gg2huPUT1Z6PQMZGgRuhVWktW/aBZVU
```

The certificate and key information should look like so:

-----BEGIN PRIVATE KEY-----

MIIJQgIBADANBgkqhkiG9w0BAQEFAASCCSwwggkoAgEAAoICAQCvhg8yMPUdZcFS

...

Ci2ZII/iARhKliLQ5+j1IS/MIHBcog==

-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----

MIIFPzCCAyegAwIBAgIJIAOxNGjwJQqOTMA0GCSqGSIb3DQEBCwUAMDYxEjAQBgNV

...

opz9

-----END CERTIFICATE-----

If you have a p12 certificate instead of a PEM file, you can use this command to extract the two components from it:

```
openssl pkcs12 -in path.p12 -out newfile.crt.pem -clcerts -nokeys
```

```
openssl pkcs12 -in path.p12 -out newfile.key.pem -nocerts -nodes
```

To verify that the information has been placed correctly after clicking “Modify” check that the Serial Number displayed is correct:

Settings | Permissions | Other

ID: 182F1BED

Name: CyberARK

Authentication Storage: CyberArk Application Identity Manager (AAM)

CyberArk Application Identity Manager (Application Access Manager)

CyberArk IP Address or FQDN (and port if differs 443): services-uscentral.skytap.com:12091

AppID: BeyondSecurity

Query: ? Safe=Test;Folder=root;Object=windows1

Client Side Certificate: ? Serial Number: EC4D1A3C2342A393

PARTNER CONTACT INFO

Business Contact	Name	Noam Rathaus
	Email	noamr@beyondsecurity.com
	Tel	

Technical Contact	Name	
	Email	support@beyondsecurity.com
	Tel	
Support Contact	Name	
	Email	support@beyondsecurity.com
	Tel	