Tenable.sc and CyberArk Enterprise Password Vault Integration Guide

Last Updated: May 18, 2023

Table of Contents

Welcome to Tenable.sc for CyberArk

This document provides information and steps for integrating Tenable.sc with CyberArk Enterprise Password Vault (CyberArk).

Security administrators know that conducting network vulnerability assessments means getting access to and navigating an ever-changing sea of usernames, passwords, and privileges. By integrating CyberArk with Tenable.sc, customers have more choice and flexibility.

The benefits of integrating Tenable.sc with CyberArk include:

- Credential updates directly in Tenable.sc, requiring less management.
- Reduced time and effort to document credential storage locations in the organizational environment.
- Automatic enforcement of security policies in specific departments or business unit requirements, simplifying compliance.
- Reduced risk of unsecured privileged accounts and credentials across the enterprise.

Note: Tenable.sc only supports integrations with CyberArk versions 12.x, 11.x, 10.x, and CyberArk Legacy version 9.x.

CyberArk Vault Integration

Configure CyberArk with either Database, SSH, or Windows. Click the corresponding link to view the configuration steps.

Database Integration

SSH Privilege Escalation Integration

Windows Integration

Database Integration

To configure database integration:

1. Log in to Tenable.sc.
2. In the top navigation bar, click **Scans** > **Credentials**.

   The **Credentials** page appears.
3. In the top right corner, click **+Add**.

   The **Add Credential** page appears.
4. In the **Database** section, click **Oracle Database**.

   The **Add Credential** page appears.
5. Enter a descriptive **Name**.
6. (Optional) Enter a **Description**.
7. (Optional) Select a **Tag**.
8. In the **Oracle Database Credential** section, select **CyberArk**.

   The **CyberArk** field options appear.

9. Configure each field for the **Oracle Database** authentication.

Option	Description	Required
CyberArk Host	The IP address or FQDN name for the CyberArk AIM Web Service. This can be the host, or the host with a custom URL added on in a single string.	yes
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443.	yes
AppID AppId	The Application ID associated with the CyberArk API connection.	yes
Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host.	no
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	yes, if private key is applied
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	yes, if private key is applied
Get credential by	The method with which your CyberArk API credentials are retrieved. Can be **Username**, **Identifier**, or **Address**. **Note:** The frequency of queries for **Username** is one query per target. The frequency of queries for **Identifier** is one query per chunk. This feature requires all targets have the same identifier. **Note:** The **Username** option also adds the **Address** parameter of the API query and assigns the target IP of the resolved host to the **Address** parameter. This may lead to fail-	yes

Option	Description	Required
	ure to fetch credentials if the CyberArk Account Details **Address** field contains a value other than the target IP address.	
Username	(If **Get credential by** is **Username**) The username of the CyberArk user to request a password from.	no
Safe	The CyberArk safe the credential should be retrieved from.	no
Account Name	(If **Get credential by** is **Identifier**) The unique account name or identifier assigned to the CyberArk API credential.	no
Use SSL	If enabled, the scanner uses SSL through IIS for secure communications. Enable this option if CyberArk is configured to support SSL through IIS.	no
Verify SSL Certificate	If enabled, the scanner validates the SSL certificate. Enable this option if CyberArk is configured to support SSL through IIS and you want to validate the certificate.	no

Note: The **Username** option also adds the **Address** parameter of the API query and assigns the target IP of the resolved host to the **Address** parameter. This may lead to failure to fetch credentials if the CyberArk Account Details **Address** field contains a value other than the target IP address.

Caution: Tenable strongly recommends encrypting communication between the Tenable.sc scanner and the CyberArk AIM gateway using HTTPS and/or client certificates. For information on securing the connection, refer to Tenable.sc User Guide and the **Central Credential Provider Implementation Guide** located at cyberark.com (login required).

10. Click **Submit**.

Next Steps

1. Complete the steps for Add the Credential to the Scan.

SSH Privilege Escalation Integration

To configure SSH integration:

1. Log in to Tenable.sc.
2. In the top navigation bar, click **Scanning**.

   A menu appears.
3. Click **Credentials**.

   The **Credentials** page appears.
4. In the SSH section, click **CyberArk Vault**.

   The **Add Credential** page appears.
5. In the **CyberArk Vault Credentials** section, click **Privilege Escalation**.

   The **Privilege Escalation** options appear.

Option	Description	Required
CyberArk Host	The IP address or FQDN name for the CyberArk AIM Web Service.	yes
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443.	yes
AppID AppId	The Application ID associated with the CyberArk API connection.	yes
Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host.	no
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	yes, if private key is applied
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	yes, if private key is applied

Option	Description	Required
Get credential by	The method with which your CyberArk API credentials are retrieved. Can be **Username**, **Identifier**, or **Address**. **Note:** The frequency of queries for **Username** is one query per target. The frequency of queries for **Identifier** is one query per chunk. This feature requires all targets have the same identifier. **Note:** The **Username** option also adds the **Address** parameter of the API query and assigns the target IP of the resolved host to the **Address** parameter. This may lead to failure to fetch credentials if the CyberArk Account Details **Address** field contains a value other than the target IP address.	yes
Username	(If **Get credential by** is **Username**) The username of the CyberArk user to request a password from.	no
Safe	The CyberArk safe the credential should be retrieved from.	no
Address	The option should only be used if the Address value is unique to a single CyberArk account credential.	no
Account Name	(If **Get credential by** is **Identifier**) The unique account name or identifier assigned to the CyberArk API credential.	no
Use SSL	If enabled, the scanner uses SSL through IIS for secure communications. Enable this option if CyberArk is configured to support	no

Option	Description	Required
	SSL through IIS.	
Verify SSL Certificate	If enabled, the scanner validates the SSL certificate. Enable this option if CyberArk is configured to support SSL through IIS and you want to validate the certificate.	no

Note: The **Username** option also adds the **Address** parameter of the API query and assigns the target IP of the resolved host to the **Address** parameter. This may lead to failure to fetch credentials if the CyberArk Account Details **Address** field contains a value other than the target IP address.

Note: Multiple options for Privilege Escalation are supported, including *su*, *su+sudo* and *sudo*. If **sudo** is selected, additional fields for **sudo user**, **CyberArk Account Details Name** and **Location of sudo** (directory) are provided and can be completed to support authentication and privilege escalation through CyberArk. See the Tenable.sc User Guide for additional information about the supported privilege escalation types and their accompanying fields.

6. Configure each field for **SSH** authentication. See Tenable.sc User Guide to get detailed descriptions for each option.
7. Click **Submit**.
8. Next, follow the steps for Add the Credential to the Scan.

Windows Integration

To configure Windows integration:

1. Log in to Tenable.sc.
2. In the top navigation bar, click **Scanning**.

   A menu appears.
3. Click **Credentials**.

   The **Credentials** page appears.
4. Click **+Add** at the top of the screen.

   The **Add Credential** page appears.
5. In the **Windows** section, click **CyberArk Vault**.

   The **Add Credential** page appears.

6. Configure each field for **Windows** authentication.

Option	Description	Required
CyberArk Host	The IP address or FQDN name for the CyberArk AIM Web Service. This can be the host, or the host with a custom URL added on in a single string.	yes
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443.	yes
AppID AppId	The Application ID associated with the CyberArk API connection.	yes
Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host.	no
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	yes, if private key is applied
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	yes, if private key is applied
Get credential by	The method with which your CyberArk API credentials are retrieved. Can be **Username**, **Identifier**, or **Address**. **Note:** The frequency of queries for **Username** is one query per target. The frequency of queries for **Identifier** is one query per chunk. This feature requires all targets have the same identifier. **Note:** The **Username** option also adds the **Address** parameter of the API query and assigns the target IP of the resolved host to the **Address** parameter. This may lead to fail-	yes

Option	Description	Required
	ure to fetch credentials if the CyberArk Account Details **Address** field contains a value other than the target IP address.	
Username	(If **Get credential by** is **Username**) The username of the CyberArk user to request a password from.	no
Safe	The CyberArk safe the credential should be retrieved from.	no
Address	The option should only be used if the Address value is unique to a single CyberArk account credential.	no
Account Name	(If **Get credential by** is **Identifier**) The unique account name or identifier assigned to the CyberArk API credential.	no
Use SSL	If enabled, the scanner uses SSL through IIS for secure communications. Enable this option if CyberArk is configured to support SSL through IIS.	no
Verify SSL Certificate	If enabled, the scanner validates the SSL certificate. Enable this option if CyberArk is configured to support SSL through IIS and you want to validate the certificate.	no

Note: The **Username** option also adds the **Address** parameter of the API query and assigns the target IP of the resolved host to the **Address** parameter. This may lead to failure to fetch credentials if the CyberArk Account Details **Address** field contains a value other than the target IP address.

Caution: Tenable strongly recommends encrypting communication between the Tenable.sc scanner and the CyberArk AIM gateway using HTTPS and/or client certificates. For information on securing

the connection, refer to Tenable.sc User Guide and the **Central Credential Provider Implementation Guide** located at cyberark.com (login required).

7. Click **Submit**.
8. Next, follow the steps for Add the Credential to the Scan.

CyberArk Vault (Legacy) Integration

Configure CyberArk with either Windows or SSH. Click the corresponding link to view the configuration steps.

Database (Legacy) Integration

SSH (Legacy) Privilege Escalation Integration

Windows (Legacy) Integration

Database (Legacy) Integration

To configure database integration:

1. Log in to Tenable.sc.
2. In the top navigation bar, click **Scans** > **Credentials**.

   The **Credentials** page appears.
3. In the top right corner, click **+Add**.

   The **Add Credential** page appears.
4. In the **Database** section, click **Oracle Database**.

   The **Add Credential** page appears.
5. Enter a descriptive **Name**.
6. (Optional) Enter a **Description**.
7. (Optional) Select a **Tag**.
8. In the **Oracle Database Credential** section, select **CyberArk**.

   The **CyberArk** field options appear.

9. Configure each field for the **Oracle Database** authentication.

Option	Database Types	Description	Required
Username	All	The target system's username.	yes
Central Credential Provider Host	All	The CyberArk Central Credential Provider IP/DNS address.	yes
Central Credential Provider Port	All	The port on which the CyberArk Central Credential Provider is listening.	yes
CyberArk AIM Service URL	All	The URL of the AIM service. By default, this field uses `/AIMWebservice/v1.1/AIM.asmx`.	no
Central Credential Provider Username	All	If the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field for authentication.	no
Central Credential Provider Password	All	If the CyberArk Central Credential Provider is configured to use basic authentication, you can fill in this field for authentication.	no
CyberArk Safe	All	The safe on the CyberArk Central Credential Provider server that contained the authentication information you would like to retrieve.	no
CyberArk Client Certificate	All	The file that contains the PEM certificate used to communicate with the CyberArk host.	no

Option	Database Types	Description	Required
CyberArk Client Certificate Private Key	All	The file that contains the PEM private key for the client certificate.	no
CyberArk Client Certificate Private Key Passphrase	All	The passphrase for the private key, if your authentication implementation requires it.	no
CyberArk AppId	All	The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.	yes
CyberArk Folder	All	The folder on the CyberArk Central Credential Provider server that contains the authentication information you would like to retrieve.	no
CyberArk Account Details Name	All	The unique name of the credential you want to retrieve from CyberArk.	yes
PolicyId	All	The PolicyID assigned to the credentials that you want to retrieve from the CyberArk Central Credential Provider.	no
Use SSL	All	If CyberArk Central Credential Provider is configured to support SSL through IIS check for secure communication.	no

Option	Database Types	Description	Required
Verify SSL Certificate	All	If CyberArk Central Credential Provider is configured to support SSL through IIS and you want to validate the certificate, select this option. Refer to the custom_CA.inc documentation for how to use self-signed certificates.	no
Database Port	All	The port on which Tenable Vulnerability ManagementTenable.sc communicates with the database.	yes
Database Name	DB2 PostgreSQL	The name of the database.	no
Auth type	Oracle SQL Server Sybase ASE	SQL Server values include: • Windows • SQL Oracle values include: Sybase ASE values include: • RSA • Plain Text	yes
Instance Name	SQL Server	The name for your database instance.	no
Service type	Oracle	Valid values include: • SID • SERVICE_NAME	yes

Option	Database Types	Description	Required
Service	Oracle	The SID value for your database instance or a SERVICE_NAME value. The **Service** value you enter must match your parameter selection for the **Service Type** option.	no

Caution: Tenable strongly recommends encrypting communication between the Tenable.sc scanner and the CyberArk AIM gateway using HTTPS and/or client certificates. For information on securing the connection, refer to Tenable.sc User Guide and the **Central Credential Provider Implementation Guide** located at cyberark.com (login required).

10. Click **Submit**.

Next Steps

1. Complete the steps for Add the Credential to the Scan.

SSH (Legacy) Privilege Escalation Integration

To configure SSH integration:

1. Log in to Tenable.sc.
2. In the top navigation bar, click **Scanning**.

   A menu appears.
3. Click **Credentials**.

   The **Credentials** page appears.
4. In the SSH section, click **CyberArk Vault**.

   The **Add Credential** page appears.
5. In the **CyberArk Vault Credentials** section, click **Privilege Escalation**.

   The **Privilege Escalation** options appear.

Option	Description	Required
Username	The username of the target system.	yes
CyberArk AIM Service URL	The URL for the CyberArk AIM web service. By default, Tenable Vulnerability Management uses `/AIMWebservice/v1.1/AIM.asmx`.	no
Central Credential Provider Host	The CyberArk Central Credential Provider IP/DNS address.	yes
Central Credential Provider Port	The port on which the CyberArk Central Credential Provider is listening.	yes
Central Credential Provider Username	The username of the vault, if the CyberArk Central Credential Provider is configured to use basic authentication.	no

Option	Description	Required
Central Credential Provider Password	The password of the vault, if the CyberArk Central Credential Provider is configured to use basic authentication.	no
Safe	The safe on the CyberArk Central Credential Provider server that contained the authentication information that you want to retrieve.	yes
CyberArk Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host.	no
CyberArk Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	no
CyberArk Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	no
AppId	The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.	yes
Folder	The folder on the CyberArk Central Credential Provider server that contains the authentication information that you want to retrieve.	yes
PolicyId	The PolicyID assigned to the credentials that you want to retrieve from the CyberArk Central Credential Provider.	no
Use SSL	If CyberArk Central Credential Provider is configured to support SSL through IIS check for secure communication.	no

Option	Description	Required
Verify SSL Certificate	If CyberArk Central Credential Provider is configured to support SSL through IIS and you want to validate the certificate check this. Refer to custom_CA.inc documentation for how to use self-signed certificates.	no
CyberArk Account Details Name	The unique name of the credential you want to retrieve from CyberArk.	no
CyberArk Address	The domain for the user account.	no
CyberArk elevate privileges with	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your selection determines the specific options you must configure. For more information, see Privilege Escalation.	no
Custom password prompt	The password prompt used by the target host. Only use this setting when an interactive SSH session fails due to Tenable Vulnerability Management receiving an unrecognized password prompt on the target host's interactive SSH shell.	no

Note: Multiple options for Privilege Escalation are supported, including *su*, *su+sudo* and *sudo*. If **sudo** is selected, additional fields for **sudo user**, **CyberArk Account Details Name** and **Location of sudo** (directory) are provided and can be completed to support authentication and privilege escalation through CyberArk. See the Tenable.sc User Guide for additional information about the supported privilege escalation types and their accompanying fields.

6. Configure each field for **SSH** authentication. See Tenable.sc User Guide to get detailed descriptions for each option.
7. Click **Submit**.
8. Next, follow the steps for Add the Credential to the Scan.

Windows (Legacy) Integration

To configure Windows integration:

1. Log in to Tenable.sc.
2. In the top navigation bar, click **Scanning**.

   A menu appears.
3. Click **Credentials**.

   The **Credentials** page appears.
4. Click **+Add** at the top of the screen.

   The **Add Credential** page appears.
5. In the **Windows** section, click **CyberArk Vault**.

   The **Add Credential** page appears.
6. Configure each field for **Windows** authentication. See the Tenable.sc User Guide to get detailed descriptions for each option.

Option	Description	Required
Username	The username of the target system.	yes
CyberArk AIM Service URL	The URL for the CyberArk AIM web service. By default, Tenable Vulnerability Management uses `/AIMWebservice/v1.1/AIM.asmx`.	no
Domain	The domain to which the username belongs.	no
Central Credential Provider Host	The CyberArk Central Credential Provider IP/DNS address.	yes
Central Credential Provider Port	The port on which the CyberArk Central Credential Provider is listening.	yes

Option	Description	Required
Central Credential Provider Username	The username of the vault, if the CyberArk Central Credential Provider is configured to use basic authentication.	no
Central Credential Provider Password	The password of the vault, if the CyberArk Central Credential Provider is configured to use basic authentication.	no
Safe	The safe on the CyberArk Central Credential Provider server that contained the authentication information that you want to retrieve.	yes
CyberArk Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host.	no
CyberArk Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	no
CyberArk Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	no
AppId	The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.	yes
Folder	The folder on the CyberArk Central Credential Provider server that contains the authentication information that you want to retrieve.	yes
PolicyId	The PolicyID assigned to the credentials that you want to retrieve from the CyberArk Central Credential Provider.	no

Option	Description	Required
Use SSL	If CyberArk Central Credential Provider is configured to support SSL through IIS check for secure communication.	no
Verify SSL Certificate	If CyberArk Central Credential Provider is configured to support SSL through IIS and you want to validate the certificate check this. Refer to custom_CA.inc documentation for how to use self-signed certificates.	no
CyberArk Account Details Name	The unique name of the credential you want to retrieve from CyberArk.	no

Caution: Tenable strongly recommends encrypting communication between the Tenable.sc scanner and the CyberArk AIM gateway using HTTPS and/or client certificates. For information on securing the connection, refer to Tenable.sc User Guide and the **Central Credential Provider Implementation Guide** located at cyberark.com (login required).

7. Click **Submit**.
8. Next, follow the steps for Add the Credential to the Scan.

Add the Credential to the Scan

To add a credential to the scan:

1. In the top navigation bar in Tenable.sc, click **Scans**.

   A drop-down menu appears.

2. Select **Active Scans**.

   The **Active Scans** window opens.

3. In the top right corner, click **+Add**.

   The **Add Active Scan** window opens.

4. In the left column, click **Credentials**.

   The **Scan Credentials** section appears.

5. In the **Scan Credentials** section, click **+Add Credential**.

   A drop-down appears.

6. Select the system type.

   The **Select Credential** option appears.

7. Click **Select Credential**.

   A drop-down appears.

8. Select the previously created credential.

9. Enter information for the **General**, **Settings**, **Targets**, and **Post Scan** sections.

10. Click **Submit**.

Additional Information

CyberArk Domain and DNS Support

Tenable's support for CyberArk allows Tenable.sc to use its target list to query CyberArk Enterprise Password Vault for the target system's credentials, and Tenable.sc can use a flexible system to allow for DNS and domain support.

Retrieving Addresses to Scan from CyberArk

Tenable.sc is able to use a feature in CyberArk to pull a list of targets to scan. Below is a description of how to pull the target system values and how to use them.

Note: The following method of target address retrieval cannot be done from the default administrator account. You must create an account that is a member of the PVWAMonitor group to generate the following reports.

1. Click on Report at the top of the CyberArk Enterprise Password Vault web interface.
2. Click **Generate Report** at the top of the Report page.
3. Choose **Privileged Account Inventory**.
4. Click **Next**.
5. Specify the search parameters for the systems you want to scan.
6. Click **Next**.
7. Click **Finish**.
8. Download the CSV or XLS report.
9. Confirm the targets for Tenable.sc to scan.
10. Confirm the values can all be resolved by Tenable.sc.
11. Copy the values from the **Target system address** column.
12. Enter the values into Tenable.sc. Either:
    a. Paste the values from addresses into the target list in Tenable.sc.
    b. Paste the values into a file and use a file target list in Tenable.sc.

Debugging CyberArk

To enable debugging when you configure a scan in Tenable.sc:

1. In Tenable.sc, click **Scans** > **Active Scans**.
2. In the row for the scan where you want to run a diagnostic scan, click the ⚙ menu.

   The actions menu appears.
3. Click **Run Diagnostic Scan**.

If a debug output for the system exists in the debug log, one or more of the following files will be present:

- logins.nasl: Used for Windows credentials. Shows higher level failures in Windows authentication
- logins.nasl~CyberArk: Used to output specific CyberArk-related debug information
- ssh_settings: Used for SSH credentials. Shows higher level failures in SSH authentication
- ssh_settings~CyberArk: Used to output specific CyberArk-related debug information

About Tenable

Tenable transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail, and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting tenable.com.