Tenable.sc and CyberArk Enterprise Password Vault Integration Guide

Last Updated: May 22, 2021
Table of Contents

Welcome to Tenable.sc for CyberArk ................................................................. 3

Integrations ....................................................................................................... 4
  Windows Integration ...................................................................................... 5
  Database Integration .................................................................................... 9
  Add the Credential to the Scan .................................................................. 13

SSH (Privilege Escalation) Integration ......................................................... 17

Additional Information ................................................................................ 22
  CyberArk Domain and DNS Support .......................................................... 23
  Retrieving Addresses to Scan from CyberArk .......................................... 24
  Debugging CyberArk ................................................................................. 25
  About Tenable ............................................................................................. 26
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 documenting where credentials are stored 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.
Integrations

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

Windows Integration

SSH Integration
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. See the [Tenable.sc User Guide](https://tenable.com/products/tenable-sc/user-guide) to get detailed descriptions for each option.
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.
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.

   ![Credentials Page](image)

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

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

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. See the [Tenable.sc User Guide](https://www.tenable.com/support/user-guide) to view detailed descriptions for each option.
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.
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**.

   ![Active Scans window](image)

   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**.
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.

**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.
Additional Information

CyberArk Domain and DNS Support

Retrieving Addresses to Scan from CyberArk

Debugging CyberArk Issues

About Tenable
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.