# Table of Contents

Welcome to Tenable.io for CyberArk ................................................................. 3

Integrations ........................................................................................................ 4
  Windows Integration ......................................................................................... 5
  Database Integration ....................................................................................... 9
  SSH Integration ............................................................................................. 14

Privilege Escalation with CyberArk Credentials ......................................... 20

Additional Information ..................................................................................... 24
  CyberArk Domain and DNS Support ............................................................... 25
  Tenable.io Priority Scanning for CyberArk ..................................................... 26
  Debugging CyberArk ..................................................................................... 27
  Retrieving Addresses to Scan from CyberArk .............................................. 29

About Tenable .................................................................................................. 30
Welcome to Tenable.io for CyberArk

This document provides information and steps for integrating Tenable.io 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.io, customers have more choice and flexibility.

The benefits of integrating Tenable.io with CyberArk include:

- Credential updates directly in Tenable.io, 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.

Note: Tenable.io only supports integrations with CyberArk versions 10.x and 11.x and CyberArk Legacy version 9.x.
Integrations

View one of the following options for CyberArk integration steps.

Windows Integration

SSH Integration
Windows Integration

To configure Tenable.io with CyberArk using Windows integration:

1. Log in to Tenable.io.

2. In the upper-left corner, click the button.

   The left navigation plane appears.

3. In the left navigation plane, click Settings.

   The Settings page appears.

4. Click the Credentials widget.

   The Credentials page appears. The credentials table lists the managed credentials you have permission to view.

5. Click the button next to the Credentials title.

   The credential form plane appears.

6. In the Host section, click Windows.

   The selected credential options appear.

7. In the Authentication Method drop-down, select CyberArk.

   The CyberArk options appear.

8. Configure the CyberArk credentials.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>CyberArk Host</td>
<td>The IP address or FQDN name for the CyberArk AIM Web Service.</td>
<td>yes</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Port</td>
<td>The port on which the CyberArk API communicates. By default, Tenable.io uses 443.</td>
<td>no</td>
</tr>
<tr>
<td>AppID</td>
<td>The Application ID associated with the CyberArk API connection.</td>
<td>yes</td>
</tr>
<tr>
<td>Client Certificate</td>
<td>The file that contains the PEM certificate used to communicate with the CyberArk host.</td>
<td>no</td>
</tr>
<tr>
<td>Client Certificate Priv-</td>
<td>The file that contains the PEM private key for the client certificate.</td>
<td>no</td>
</tr>
<tr>
<td>ate Key</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Certificate Priv-</td>
<td>The passphrase for the private key, if required.</td>
<td>yes, if private key requires</td>
</tr>
<tr>
<td>ate Key Passphrase</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Get credential by</td>
<td>The method with which your CyberArk API credentials are retrieved: <strong>Username</strong> or <strong>Identifier</strong></td>
<td>yes</td>
</tr>
<tr>
<td>Username</td>
<td>(If Get credential by is set to <strong>Username</strong>) The username of the CyberArk user to request a password from.</td>
<td>yes, for <strong>User- name</strong></td>
</tr>
<tr>
<td>Domain</td>
<td>(If Get credential by is set to <strong>Username</strong>) The domain to which the username belongs, if applicable.</td>
<td>no</td>
</tr>
<tr>
<td>Safe</td>
<td>(If Get credential by is set to <strong>Username</strong>) The CyberArk safe the credential should be retrieved from.</td>
<td>yes, for <strong>User- name</strong></td>
</tr>
<tr>
<td>Account Name</td>
<td>(If Get credential by is set to <strong>Identifier</strong>) The unique account name or identifier</td>
<td>yes, for <strong>Iden- tifier</strong></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td>assigned to the CyberArk API credential.</td>
<td></td>
</tr>
<tr>
<td>Use SSL</td>
<td>If enabled, the scanner uses SSL through IIS for secure communications. Enable this option if CyberArk is configured to support SSL through IIS.</td>
<td>no</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>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.</td>
<td>no</td>
</tr>
</tbody>
</table>

9. Click **Save**.

Verification

1. To verify the integration is working, click the **Launch** button to initiate an on-demand scan.

2. After the scan completes, click the scan to view the results.

3. Look for **Plugin ID 10394**. This validates that the authentication was successful. If the authen-
tication is not successful, refer to the [Debugging CyberArk Issues](#) section of this document.
Database Integration

To configure Database integration:

1. Log in to Tenable.io.

2. Click **Scans**.

   The **My Scans** page appears.

3. Click **+ New Scan**.

   The **Scan Templates** page appears.

4. Select a **Scan Template**. For demonstration, the **Advanced Network Scan** template is used.
The scan configuration page appears.

5. In the **Name** box, type a name for the scan.

6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.

7. (Optional) You can add a description, folder location, scanner location, and specify target groups.
8. Click the **Credentials** tab.

The **Credentials** options appear.
9. In the left-hand menu, click the **Database** drop-down.

10. Click the **Database** option.

    The **Database** options appear.

11. From the **Database Type** drop-down, select **Oracle**.

12. From the **Auth Type** drop-down, select **CyberArk**.

    The **CyberArk** field options appear.

13. Configure each field for the **Database** authentication. See the [Tenable.io User Guide](#) to view detailed descriptions for each option.

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

14. Click **Save**.
SSH Integration

To configure SSH integration:

1. Log in to Tenable.io.
2. Click **Scans**.
3. Click **+ New Scan**.
4. Select a **Scan Template**.
5. In the **Name** box, type a name for the scan.

6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.

7. (Optional) Add a description, folder location, scanner location, and specify target groups.

8. Click the **Credentials** tab.
   
The Credentials options appear.

9. In the left-hand menu, select **SSH**.

10. Click **Authentication method**.

    A drop-down appears.

11. Select **CyberArk**.

    The **CyberArk SSH** options appear.
12. Configure each field for **SSH** authentication.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username of the target system.</td>
<td>yes</td>
</tr>
<tr>
<td>CyberArk AIM Service URL</td>
<td>The URL for the CyberArk AIM web service. By default, Tenable.io uses /AIMweb-</td>
<td>no</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>service/v1.1/AIM.asmx.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Central Credential Provider Host</td>
<td>The CyberArk Central Credential Provider IP/DNS address.</td>
<td>yes</td>
</tr>
<tr>
<td>Central Credential Provider Port</td>
<td>The port on which the CyberArk Central Credential Provider is listening.</td>
<td>yes</td>
</tr>
<tr>
<td>Central Credential Provider Username</td>
<td>The username of the vault, if the CyberArk Central Credential Provider is configured to use basic authentication.</td>
<td>no</td>
</tr>
<tr>
<td>Central Credential Provider Password</td>
<td>The password of the vault, if the CyberArk Central Credential Provider is configured to use basic authentication.</td>
<td>no</td>
</tr>
<tr>
<td>Safe</td>
<td>The safe on the CyberArk Central Credential Provider server that contained the authentication information that you want to retrieve.</td>
<td>yes</td>
</tr>
<tr>
<td>CyberArk Client Certificate</td>
<td>The file that contains the PEM certificate used to communicate with the CyberArk host.</td>
<td>no</td>
</tr>
<tr>
<td>CyberArk Client Certificate Private Key</td>
<td>The file that contains the PEM private key for the client certificate.</td>
<td>no</td>
</tr>
<tr>
<td>CyberArk Client Certificate Private Key Passphrase</td>
<td>The passphrase for the private key, if required.</td>
<td>no</td>
</tr>
<tr>
<td>AppId</td>
<td>The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve</td>
<td>yes</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>the target password.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Folder</td>
<td>The folder on the CyberArk Central Credential Provider server that contains the authentication information that you want to retrieve.</td>
<td>yes</td>
</tr>
<tr>
<td>PolicyId</td>
<td>The PolicyID assigned to the credentials that you want to retrieve from the CyberArk Central Credential Provider.</td>
<td>no</td>
</tr>
<tr>
<td>Use SSL</td>
<td>If CyberArk Central Credential Provider is configured to support SSL through IIS check for secure communication.</td>
<td>no</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>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.</td>
<td>no</td>
</tr>
<tr>
<td>CyberArk Account Details Name</td>
<td>The unique name of the credential you want to retrieve from CyberArk.</td>
<td>no</td>
</tr>
<tr>
<td>CyberArk Address</td>
<td>The domain for the user account.</td>
<td>no</td>
</tr>
<tr>
<td>CyberArk elevate privileges with</td>
<td>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.</td>
<td>no</td>
</tr>
<tr>
<td>Custom password prompt</td>
<td>The password prompt used by the target host. Only use this setting when an interactive SSH session fails due to Tenable.io receiving an unrecognized pass-</td>
<td>no</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
<td>Required</td>
</tr>
<tr>
<td>----------</td>
<td>----------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td></td>
<td>word prompt on the target host's interactive SSH shell.</td>
<td></td>
</tr>
</tbody>
</table>

13. Click **Save**.

**Verification**

1. To verify the integration is working, click the **launch** button (highlighted below) to initiate an on-demand scan.

2. Once the scan has completed, select the completed scan and look for **Plugin ID 12634**, which validates that authentication was successful. If the authentication is not successful, refer to the **Debugging CyberArk Issues** section of this document.
Privilege Escalation with CyberArk Credentials

Tenable.io supports the use of privilege escalation, such as `su` and `sudo`, when using SSH through the CyberArk authentication method.

To configure SSH integration:
1. Select **SSH** as the **Type** and **CyberArk** as the **Authentication Method**.

2. An option for **CyberArk elevate privileges with** appears near the bottom of the configuration page.

   **Note:** Multiple options for privilege escalation are supported, including **su**, **su+sudo** and **sudo**. For example, if **sudo** is selected, additional fields for **sudo user**, **CyberArk Account Details Name** and
The location of `sudo` (directory) are provided and can be completed to support authentication and privilege escalation through CyberArk Password Vault.

**Note:** Additional information about all of the supported privilege escalation types and their accompanying fields can be found in the [Tenable.io User Guide](#).

![Configuration settings for CyberArk elevation of privilege](image)

**Note:** When asked for a CyberArk Account Details Name, perform the following steps to obtain the correct value:
1. Log in to CyberArk Password Vault.
2. Choose the secret (password) you wish to use.
3. Look at the name parameter (such as in the image below) in the Account Details page; this is the value to
Supply in the **CyberArk Account Details** Name field.

![Image of CyberArk Account Details](image-url)

- **Password**
- **SSH**

**Platform Name:** Unix via SSH
**Device Type:** Operating System
**Safe:** Unix Accounts
**Name:** Operating System-UnixSSH-172.26.22.201-root
**Last verified:** N/A
**Last modified:** Administrator (6/13/2016 10:32:35 PM)
**Last used:** Administrator (6/20/2016 11:32:29 AM)
**Address:** 172.26.22.201
**Username:** root
Additional Information

CyberArk Domain and DNS Support

Tenable.io Priority Scanning for CyberArk

Retrieving Addresses to Scan from CyberArk

Debugging CyberArk Issues
CyberArk Domain and DNS Support

Tenable’s support for CyberArk allows Tenable.io to use its target list to query CyberArk Enterprise Password Vault for the target system’s credentials, and Tenable.io can use a flexible system to allow for DNS and domain support. See Tenable.io Priority Scanning for CyberArk for explanation of the logic used by Tenable.io for scans using credentials from CyberArk Enterprise Password Vault.
Tenable.io Priority Scanning for CyberArk

Tenable.io sets a priority system that allows for flexible querying. The following is set out to describe the order Tenable.io tries values and the logic behind it.

1. Tenable.io will query CyberArk with the target value entered into the Tenable.io Targets configuration field. For example, if you put a FQDN in the target list, Tenable.io will query CyberArk with the address value of the FQDN. If you enter an IP address or range such as 192.0.2.1-20, Tenable.io will try to query using the IP address or IP range of the target system(s) in the CyberArk Address value. If the target system uses FQDN and can be resolved, then it will be contacted.

2. If the target value fails, Tenable.io will then look to see if there is a domain value (for a Windows system). If a domain value is present, Tenable.io will query CyberArk using the domain value for the address value to attempt to use domain credentials.

3. If the configured target value and the domain value both fail, Tenable.io will then pull the IP address of the system. If the IP address does not match one of the IP addresses supplied in the target list, Tenable.io will then query CyberArk using the IP address of the target itself. This is checked against the target value in the configuration to prevent querying CyberArk twice with the same value.
Debugging CyberArk

To enable debugging when you configure a scan in Tenable.io, go to Settings->Advanced->Debug Settings and Check Enable plugin debugging. If an issue is found, review the results of plugin Debugging Log Report (84239). If 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

Example of output:

[2015-11-17 22:17:04] HTTP/1.1 500 Internal Server Error returned
[2015-11-17 22:17:04] HTTP 500 : Server was unable to process request. ---
&gt; APPAP004E Password object matching query [Safe=Unix Accounts;UserName=credtester;Folder=Root;Address=192.0.2.26] was not found (Diagnostic Info: 5). Please check that there is a password object that answers your query in the Vault and that both the Provider and the application user have the appropriate permissions needed in order to use the password.
[2015-11-17 22:17:04] HTTP/1.1 500 Internal Server Error returned
[2015-11-17 22:17:04] HTTP 500 : Server was unable to process request. ---
&gt; APPAP004E Password object matching query [Safe=Unix Accounts;UserName=admin;Folder=Root;Address=192.0.2.26] was not found (Diagnostic Info: 5). Please check that there is a password object that answers your query in the Vault and that both the Provider and the application user have the appropriate permissions needed in order to use the password.
[2015-11-17 22:17:04] HTTP/1.1 500 Internal Server Error returned
[2015-11-17 22:17:04] HTTP 500 : Server was unable to process request. ---
&gt; APPAP229E Too many password objects matching query [Safe=Unix Accounts;UserName=admin;Folder=Root] were found: (Safe=Unix Accounts;Folder=Root:Object=Operating System-WinDesktopLocal-192.0.2.205-admin,
Safe=Unix Accounts;Folder=Root;Object=Operating System-WinDesktopLocal-192.0.2.66-admin and more. See trace log for more information. (Diagnostic Info: 41)

The Tenable.io Priority Scanning for CyberArk section shows that a single system may send multiple requests that fail before finding a successful one. Because of this, the output to the debugging log may not show an issue with the scan, but it can be used as an audit trail if there is an issue. To address issues using the log, look for the parameters to match the intended query and see what error output was reported for that query. For example, if you intended to scan target 192.0.2.66 using parameters of (Safe=Unix Accounts;UserName=admin;Folder=Root), then you could discern from the log above that the reason the scan failed is because there were too many matching items to this query, and therefore no results were returned.
Retrieving Addresses to Scan from CyberArk

Tenable.io 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.io to scan.
10. Confirm the values can all be resolved by Tenable.io.
11. Copy the values from the **Target system address** column.
12. Enter the values into Tenable.io. Either:
    a. Paste the values from addresses into the target list in Tenable.io.
    b. Paste the values into a file and use a file target list in Tenable.io.
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.