Tenable Security Center and CyberArk Enterprise Password Vault Integration Guide

Last Updated: March 20, 2024

Table of Contents

Welcome to Tenable Security Center for CyberArk

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

The benefits of integrating Tenable Security Center with CyberArk include:

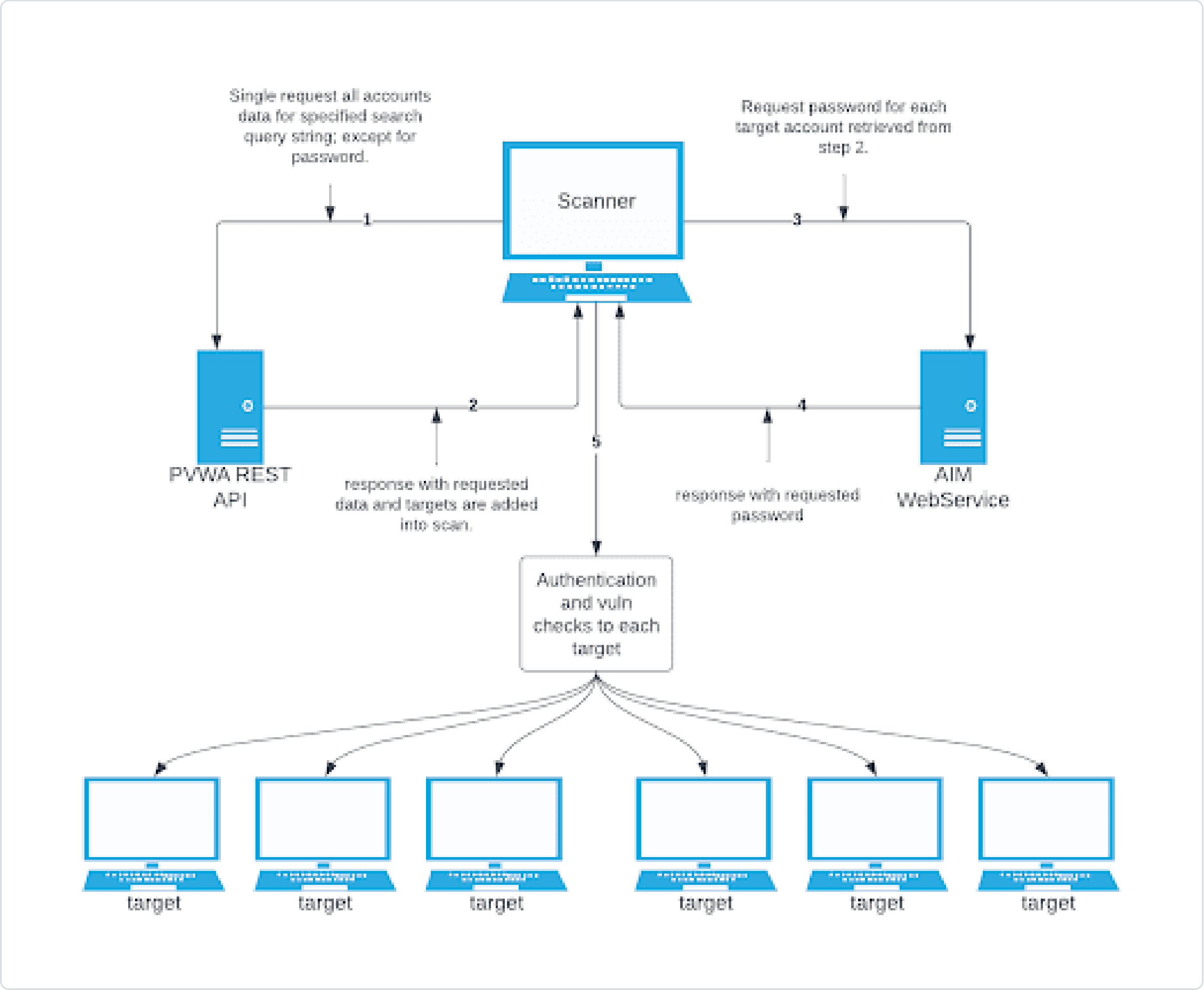
- Credential updates directly in Tenable Security Center, requiring less management.
- Reduced time and effort to document credential storage locations in the organizational environment.
- Automatic enforcement of security policies in specific departments or business unit requirements, simplifying compliance.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

> **Note:** Tenable Security Center only supports integrations with CyberArk versions 13.x, 12.x, 11.x, 10.x, and CyberArk Legacy version 9.x.

CyberArk Dynamic Scanning

You can now take advantage of a significant improvement to Tenable's CyberArk integration which gathers bulk account information for specific target groups without entering multiple targets. You need to enter only one target in the settings (which is arbitrary and not used as an actual target). This target is used to kick off the process of collection and nothing more. You can configure up to five unique credentials in a scan policy that represent specific target groups.

The integration feature takes advantage of CyberArk's Password Vault Web Access (PVWA) REST API, by gathering bulk account information for a large volume of hosts, automatically adding them to the scan, and requesting the password on a host-by-host basis from CCP/AIM Web Service application. You must have a CyberArk version that contains the PVWA REST API to use this feature.


Single request all accounts data for specified search query string; except for password.
Request password for each target account retrieved from step 2.
Scanner
1
3
2
4
5
PVWA REST API
response with requested data and targets are added into scan.
response with requested password
AIM WebService
Authentication and vuln checks to each target
target
target
target
target
target
target

Collection

The initial collection of accounts (except the password) is done once and on the arbitrary target/host entered in the target settings of the scan policy mentioned in the beginning of each section (SSH, Windows, and Database). Logs for the collection can be found in the **Debugging Log Reporting** on this particular host in the following logs:

- Database = `pam_database_auto_collect.nbin~CyberArk`
- SSH = `pam_ssh_auto_collect.nbin~CyberArk`
- Windows = `pam_smb_auto_collect.nbin~CyberArk`

Adding targets to the scan automatically

After the collection process, the integration performs automatic addition of the hosts and necessary host's knowledge bases (KBs). Before adding hosts to the scan, the integration checks that an `address` value was present. This process is contingent upon that value. In addition, the integration tries to resolve that host (address value) within your network. Once it determines that a resolvable host (address value) is present, the integration adds the host (and certain data gathered as KBs) used to query the password and/or used for authentication to the host. As a supplemental log for identifying successfully resolved hosts against unsuccessfully resolved hosts, the integration provides logs present on the arbitrary host:

- Database = `pam_database_auto_collect.log`
- SSH = `pam_ssh_auto_collect.log`
- Windows = `pam_smb_auto_collect.log`

Database example:

```
[2023-07-19 17:24:35] Start injecting kb's and hosts for 4 accounts.
[2023-07-19 17:24:35] Attempting to resolve host from CyberArk Address : 172.26.25.107
[2023-07-19 17:24:35] Attempting to resolve host from CyberArk Address : 172.26.28.153
[2023-07-19 17:24:35] Attempting to resolve host from CyberArk Address : 172.26.25.107
[2023-07-19 17:24:35] Attempting to resolve host from CyberArk Address : auditmsss2016
[2023-07-19 17:24:35] Failed to resolve host from CyberArk Address : auditmsss2016
[2023-07-19 17:24:35] End injecting kb's and hosts
Number of hosts retrieved from CyberArk : 4
Number of hosts failed to resolve : 1
List of failed hosts. CyberArk Address  : make_nested_list(
  'auditmsss2016'
)
[2023-07-19 17:24:35] Auto-collection of database hosts complete for : CyberArk
```

In the example database log, we have a host auditmsss2016 that Tenable Nessus could not resolve on the network. This host is not added to the scan. An error returned from the function fqdn_resolv() triggers the creation of separate logs that show more detail called:

- Database = pam_database_auto_collect_resolv_func.log
- SSH = pam_ssh_auto_collect_resolv_func.log
- Windows = pam_smb_auto_collect_resolv_func.log

In addition, you can see in the example log that we have a duplicate host. The Tenable Nessus engine handles that naturally, so more than one record does not appear in the host table.

Password collection

After the collection and addition of host and KBs is complete, the authentication process kicks off on each of the hosts. To eliminate the possibility of requesting a password for either the arbitrary host (input by the user) or a host not containing the necessary query parameters, a condition is set in place within logins, ssh_settings, and database_settings to avoid this. Host by host, the integration calls AIM Web Service for the password using four unique query parameters that avoid requesting a password for the wrong target: safe, object, username, and address. As far as logs go, this is no different (on the host level) than “normal.”

- Database = database_settings.nasl~CyberArk
- SSH = ssh_settings.nasl~CyberArk
- Windows = logins.nasl~CyberArk

Configuration methods:

- Database Auto-Discovery
- SSH Auto-Discovery
- Windows Auto-Discovery

Database Auto-Discovery

You need to configure new user interface field properties in addition to the default account properties in CyberArk and PrivateArk, as database authentication requires additional data. `Port` and `Database` are already available, but some database platforms in CyberArk need these added to the user interface properties. `AuthType` and `ServiceType` are new, so you must add them to PrivateArk first, then configure them to the applicable database platform type user interface properties in CyberArk Web console.

> **Note:** The Address field in the CyberArk Account Details for an account/host must contain a valid IP/FQDN and must be resolvable on the user's network. This value is vetted during the collection and discovery process. Address values that are null or unresolvable will not be added to the scan.

> **Note:** All Database Type in Tenable are supported. (Oracle, DB2, Cassandra, MySQL, PostgreSQL, Sybase ASE, MongoDB, and SQL Server)

View the following tables for necessary fields and Database Types they apply to.

Oracle

Field name	Description	Field value
Port	The port database instance is running on.	Example: 1521
AuthType	Method to authenticate to database.	SYSDBA or SYSOPER or NORMAL
Database	Instance or database name.	Example: orcl
ServiceType	Type of service on database.	SID or SERVICE_NAME

MongoDB

Field name	Description	Field value
Port	The port database instance is running on.	Example: 27017
Database	Instance or database name.	Example: MongoDB 5

PostgreSQL

Field name	Description	Field value
Port	The port database instance is running on.	Example: 5432
Database	Instance or database name.	Example: Postgre

Cassandra

Field name	Description	Field value
Port	The port database instance is running on.	Example: 9042

DB2

Field name	Description	Field value
Port	The port database instance is running on.	Example: 50000
Database	Instance or database name.	Example: DB2_admin

MySQL

Field name	Description	Field value
Port	The port database instance is running on.	Example: 3306

SQL Server

Field name	Description	Field value
Port	The port database instance is running on.	Example: 1433
AuthType	Method to authenticate to database.	Windows or SQL
Database	Instance or database name.	Example: SQLEXPRESS

Requirements:

- CyberArk account
- Nessus Manager account

To configure database auto-discovery:

1. Log in to Tenable Security Center.
2. Click **Scans**.

   The **My Scans** page appears.
3. Click **+ New Scan.**

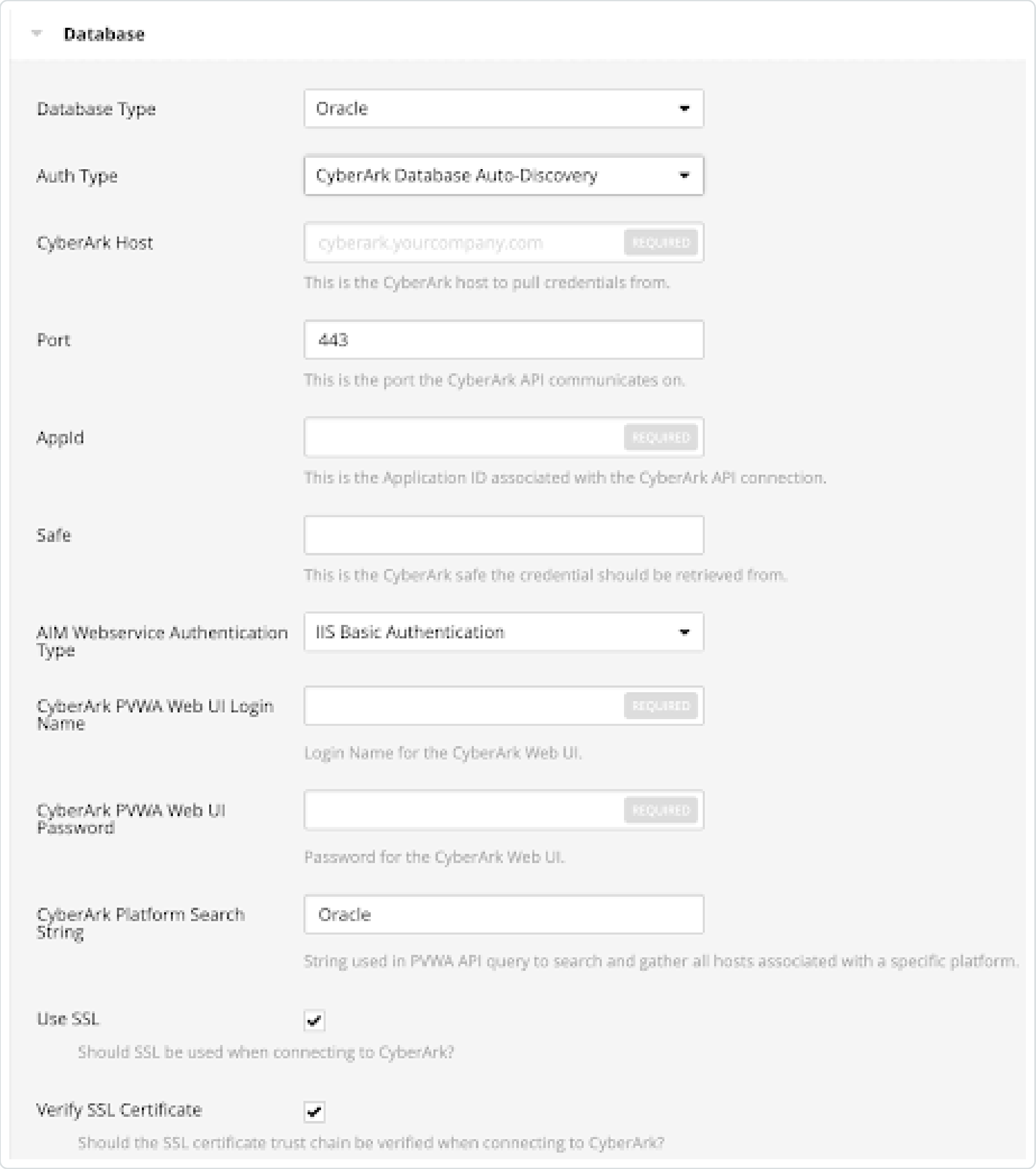
   The **Scan Templates** page appears.
4. Select a **Scan Template**. For demonstration, the **Advanced Network Scan** template is used.

   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) Add a description, folder location, scanner location, and specify target groups.
8. Click the **Credentials** tab.

   The **Credentials** pane appears.
9. Click the **Database** option.

   The **Database** options appear.
10. From the **Database Type** drop-down, select **Oracle**.
11. From the **Auth Type** drop-down, select **CyberArk Database Auto-Discovery**.

    The **CyberArk Database Auto-Discovery** field options appear:



Database

Database Type	Oracle
Auth Type	CyberArk Database Auto-Discovery
CyberArk Host	cyberark.yourcompany.com REQUIRED This is the CyberArk host to pull credentials from.
Port	443 This is the port the CyberArk API communicates on.
AppId	REQUIRED This is the Application ID associated with the CyberArk API connection.
Safe	 This is the CyberArk safe the credential should be retrieved from.
AIM Webservice Authentication Type	IIS Basic Authentication
CyberArk PVWA Web UI Login Name	REQUIRED Login Name for the CyberArk Web UI.
CyberArk PVWA Web UI Password	REQUIRED Password for the CyberArk Web UI.
CyberArk Platform Search String	Oracle String used in PVWA API query to search and gather all hosts associated with a specific platform.
Use SSL	☑ Should SSL be used when connecting to CyberArk?
Verify SSL Certificate	☑ Should the SSL certificate trust chain be verified when connecting to CyberArk?

12. Configure each field for the **Database** authentication.

Option	Description	Required
CyberArk Host	The IP address or FQDN name for the user’s CyberArk Instance.	yes

Option	Description	Required
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443.	yes
AppID	The Application ID associated with the CyberArk API connection.	yes
Safe	Users may optionally specify a Safe to gather account information and request passwords.	no
AIM Web Service Authentication Type	There are two authentication methods established in the feature. IIS Basic Authentication and Certificate Authentication. Certificate Authentication can be either encrypted or unencrypted.	yes
CyberArk PVWA Web UI Login Name	Username to log in to CyberArk web console. This is used to authenticate to the PVWA REST API and gather bulk account information.	yes
CyberArk PVWA Web UI Login Password	Password for the username to log in to CyberArk web console. This is used to authenticate to the PVWA REST API and gather bulk account information.	yes
CyberArk Platform Search String	String used in the PVWA REST API query parameters to gather bulk account information. For example, the user can enter `Oracle Admin TestSafe`, to gather all Oracle platform accounts containing a username `Admin` in a Safe called `TestSafe`. **Note:** This is a non-exact keyword search. A best practice would be to create a custom platform name in CyberArk and enter that value in this field to improve accuracy.	yes

Option	Description	Required
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.	yes
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

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 Security Center User Guide and the **Central Credential Provider Implementation Guide** located at cyberark.com (login required).

13. Click **Save**.

SSH Auto-Discovery

Note: The Address field in the CyberArk Account Details for an account/host must contain a valid IP/FQDN and must be resolvable on your network. This value is vetted during the collection and discovery process. Address values that are null, or unresolvable, are not added to the scan.

To configure SSH auto-discovery:

1. Log in to Tenable Security Center.
2. Click **Scans**.

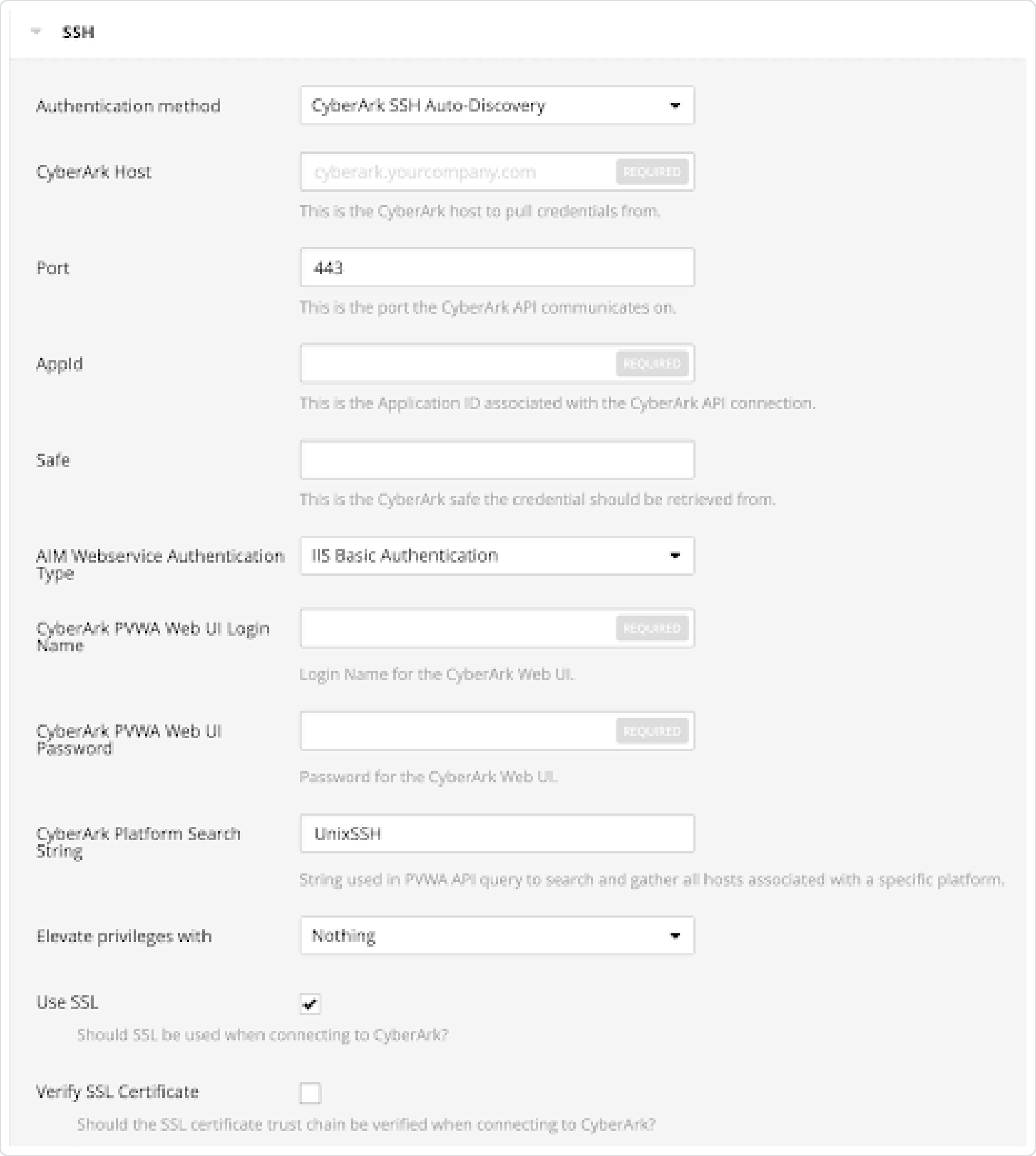
   The **My Scans** page appears.
3. Click **+ New Scan.**

   The **Scan Templates** page appears.
4. Select a **Scan Template**.

   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) Add a description, folder location, scanner location, and specify target groups.
8. Click the **Credentials** tab.

   The **Credentials** pane appears.
9. In the **Select a Credential** menu, select the **Host** drop-down..
10. Select **SSH**.
11. From the **Authentication Method** drop-down, select **CyberArk SSH Auto-Discovery**.

    The **CyberArk SSH Auto-Discovery** field options appear:



SSH

Authentication method: CyberArk SSH Auto-Discovery

CyberArk Host: cyberark.yourcompany.com REQUIRED
This is the CyberArk host to pull credentials from.

Port: 443
This is the port the CyberArk API communicates on.

AppId: REQUIRED
This is the Application ID associated with the CyberArk API connection.

Safe:
This is the CyberArk safe the credential should be retrieved from.

AIM Webservice Authentication Type: IIS Basic Authentication

CyberArk PVWA Web UI Login Name: REQUIRED
Login Name for the CyberArk Web UI.

CyberArk PVWA Web UI Password: REQUIRED
Password for the CyberArk Web UI.

CyberArk Platform Search String: UnixSSH
String used in PVWA API query to search and gather all hosts associated with a specific platform.

Elevate privileges with: Nothing

Use SSL ☑
Should SSL be used when connecting to CyberArk?

Verify SSL Certificate ☐
Should the SSL certificate trust chain be verified when connecting to CyberArk?

12. Configure each field for the **SSH** authentication.

Option	Description	Required
CyberArk Host	The IP address or FQDN name for the user's CyberArk Instance.	yes

Option	Description	Required
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443.	yes
AppID	The Application ID associated with the CyberArk API connection.	yes
Safe	Users may optionally specify a Safe to gather account information and request passwords.	no
AIM Web Service Authentication Type	There are two authentication methods established in the feature. **IIS Basic Authentication** and **Certificate Authentication**. Certificate Authentication can be either encrypted or unencrypted.	yes
CyberArk PVWA Web UI Login Name	Username to log in to CyberArk web console. This is used to authenticate to the PVWA REST API and gather bulk account information.	yes
CyberArk PVWA Web UI Login Password	Password for the username to log in to CyberArk web console. This is used to authenticate to the PVWA REST API and gather bulk account information.	yes
CyberArk Platform Search String	String used in the PVWA REST API query parameters to gather bulk account information. For example, the user can enter `UnixSSH Admin TestSafe`, to gather all UnixSSH platform accounts containing a username `Admin` in a Safe called `TestSafe`. **Note:** This is a non-exact keyword search. A best practice would be to create a custom platform name in CyberArk and enter that value in this field to improve accuracy.	yes

Option	Description	Required
Elevate Privileges with	Users can only select Nothing or sudo at this time.	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.	yes
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

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 Security Center User Guide and the **Central Credential Provider Implementation Guide** located at cyberark.com (login required).

13. Click **Save**.

Windows Auto-Discovery

> **Note:** The **Address** field in the CyberArk Account Details for an account/host must contain a valid IP/FQDN and must be resolvable on your network. This value is vetted during the collection and discovery process. Address values that are null or unresolvable will not be added to the scan.

> **Note:** Domain support is included, but CyberArk accounts must make use of the **Domain** field provided in account set up.

To configure windows auto-discovery:

1. Log in to Tenable Nessus Manager.
2. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.
3. Click the **Credentials** tab.

   The **Credentials** pane appears.
4. In the left navigation plane, click **Settings**.

   The **Settings** page appears.
5. Click the **Credentials** widget.

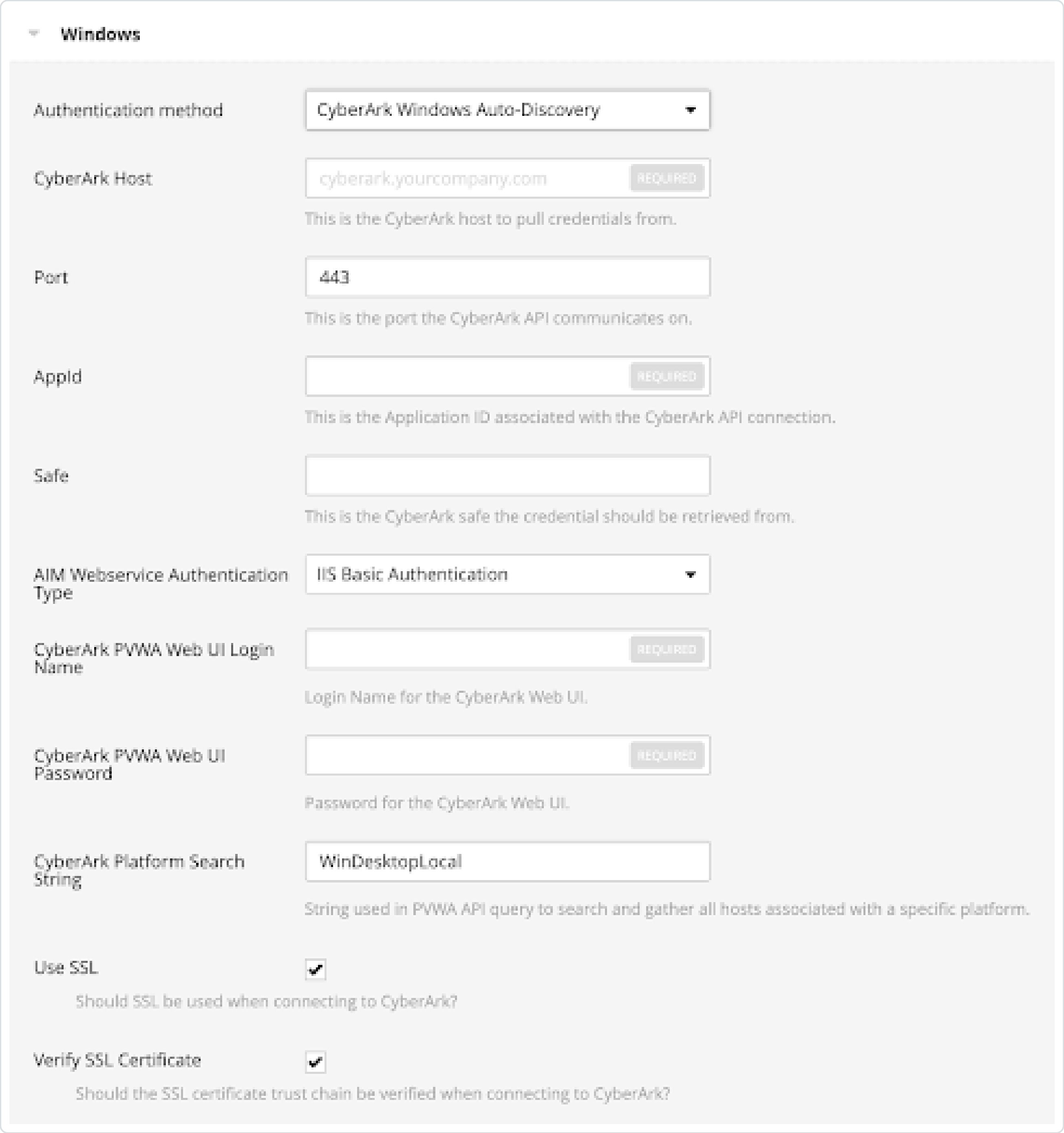
   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.
6. Click the ⊕ button next to the **Credentials** title.

   The credential form plane appears.
7. Click the **Host** option.

   The **Host** options appear.
8. In the **Host** section, click **Windows**.

   The selected credential options appear.
9. From the **Authentication Method** drop-down, select **CyberArk Windows Auto-Discovery**.

The **CyberArk Windows Auto-Discovery** field options appear:



Windows

Authentication method: CyberArk Windows Auto-Discovery

CyberArk Host: cyberark.yourcompany.com REQUIRED
This is the CyberArk host to pull credentials from.

Port: 443
This is the port the CyberArk API communicates on.

AppId: REQUIRED
This is the Application ID associated with the CyberArk API connection.

Safe:
This is the CyberArk safe the credential should be retrieved from.

AIM Webservice Authentication Type: IIS Basic Authentication

CyberArk PVWA Web UI Login Name: REQUIRED
Login Name for the CyberArk Web UI.

CyberArk PVWA Web UI Password: REQUIRED
Password for the CyberArk Web UI.

CyberArk Platform Search String: WinDesktopLocal
String used in PVWA API query to search and gather all hosts associated with a specific platform.

Use SSL ☑
Should SSL be used when connecting to CyberArk?

Verify SSL Certificate ☑
Should the SSL certificate trust chain be verified when connecting to CyberArk?

10. Configure each field for the **Windows** authentication.

Option	Description	Required
CyberArk Host	The IP address or FQDN name for the user's CyberArk Instance.	yes
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443.	yes
AppID	The Application ID associated with the CyberArk API connection.	yes
Safe	Users may optionally specify a Safe to gather account information and request passwords.	no
AIM Web Service Authentication Type	There are two authentication methods established in the feature. **IIS Basic Authentication** and **Certificate Authentication**. Certificate Authentication can be either encrypted or unencrypted.	yes
CyberArk PVWA Web UI Login Name	Username to log in to CyberArk web console. This is used to authenticate to the PVWA REST API and gather bulk account information.	yes
CyberArk PVWA Web UI Login Password	Password for the username to log in to CyberArk web console. This is used to authenticate to the PVWA REST API and gather bulk account information.	yes
CyberArk Platform Search String	String used in the PVWA REST API query parameters to gather bulk account information. For example, the user can enter `UnixSSH Admin TestSafe`, to gather all Windows platform accounts containing a username `Admin` in a Safe called `TestSafe`. **Note:** This is a non-exact keyword search. A best	yes

Option	Description	Required
	practice would be to create a custom platform name in CyberArk and enter that value in this field to improve accuracy.	
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.	yes
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

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 Security Center User Guide and the **Central Credential Provider Implementation Guide** located at cyberark.com (login required).

11. Click **Save**.

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 Security Center.
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**.

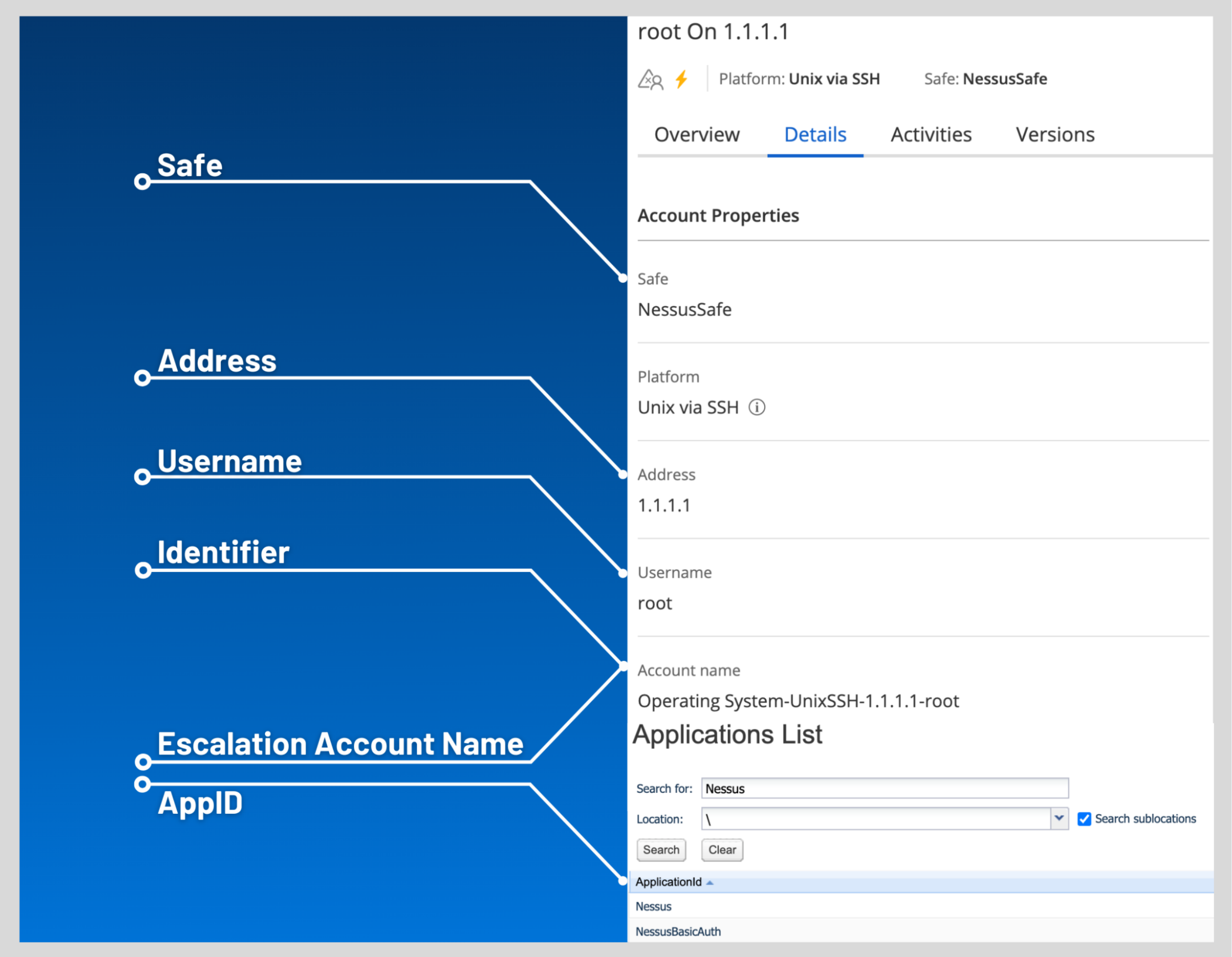
   The **CyberArk** field options appear.

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	yes

Option	Description	Required
	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.	
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

CyberArk credential field mapping to the CyberArk Accounts detail view in the CyberArk console:



root On 1.1.1.1

Platform: Unix via SSH Safe: NessusSafe

Account Properties

Safe
NessusSafe

Platform
Unix via SSH

Address
1.1.1.1

Username
root

Account name
Operating System-UnixSSH-1.1.1.1-root

Applications List

Search for: Nessus

Location: \

☑ Search sublocations

ApplicationId
Nessus
NessusBasicAuth

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 Security Center scanner and the CyberArk AIM gateway using HTTPS and/or client certificates. For information on securing the connection, refer to Tenable Security Center 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 Security Center.
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**.

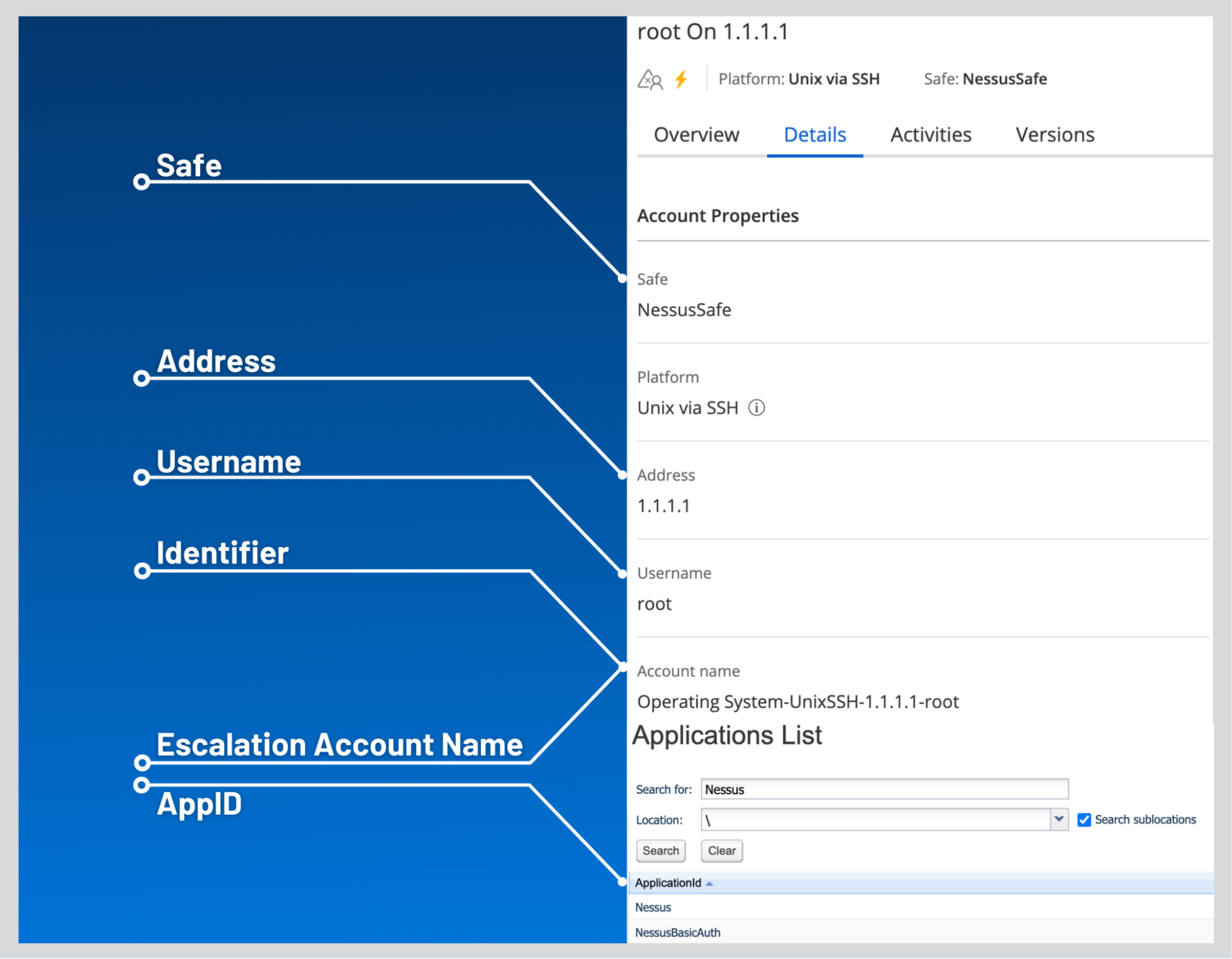
   The **Privilege Escalation** options appear.

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	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	The passphrase for the private key, if required.	yes, if private key is

Option	Description	Required
Private Key Passphrase		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 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 SSL through IIS.	no

Option	Description	Required
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

CyberArk credential field mapping to the CyberArk Accounts detail view in the CyberArk console:



root On 1.1.1.1

Platform: Unix via SSH Safe: NessusSafe

Account Properties

Safe
NessusSafe

Platform
Unix via SSH

Address
1.1.1.1

Username
root

Account name
Operating System-UnixSSH-1.1.1.1-root

Applications List

Search for: Nessus

Location: \ ☑ Search sublocations

ApplicationId
Nessus
NessusBasicAuth

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 Security Center User Guide for additional information about the supported privilege escalation types and their accompanying fields.

6. Configure each field for **SSH** authentication. See Tenable Security Center 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 Security Center.
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**.

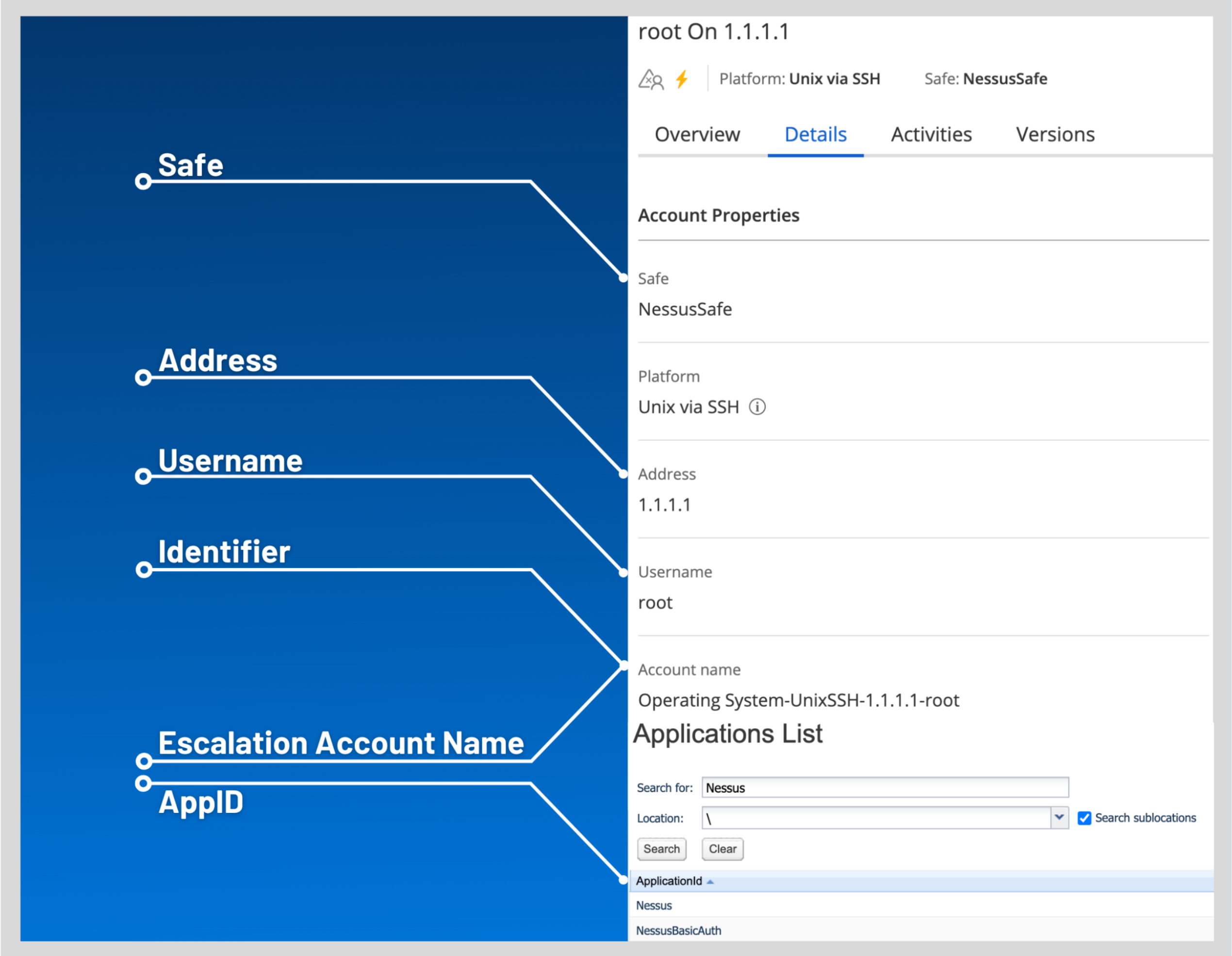
   The **Add Credential** page appears.

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	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	yes

Option	Description	Required
	lead to failure 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

CyberArk credential field mapping to the CyberArk Accounts detail view in the CyberArk console:



root On 1.1.1.1

Platform: **Unix via SSH** Safe: **NessusSafe**

Account Properties

Safe
NessusSafe

Platform
Unix via SSH ⓘ

Address
1.1.1.1

Username
root

Account name
Operating System-UnixSSH-1.1.1.1-root

Applications List

Search for: Nessus

Location: \

☑ Search sublocations

ApplicationId ▲
Nessus
NessusBasicAuth

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 Security Center scanner and the CyberArk AIM gateway using HTTPS and/or client certificates. For information on securing the connection, refer to Tenable Security Center 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 Security Center.
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	All	The file that contains the PEM certificate used to communicate with	no

Option	Database Types	Description	Required
Certificate		the CyberArk host.	
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	no

Option	Database Types	Description	Required
		Provider is configured to support SSL through IIS check for secure communication.	
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 Security Center 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

Option	Database Types	Description	Required
Service type	Oracle	Valid values include: • SID • SERVICE_NAME	yes
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 Security Center scanner and the CyberArk AIM gateway using HTTPS and/or client certificates. For information on securing the connection, refer to Tenable Security Center 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 Security Center.
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, Security Center for CyberArk 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

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
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.	no
Custom password prompt	The password prompt used by the target host. Only use this setting when an interactive SSH session fails due to Security Center for CyberArk 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 Security Center User Guide for additional information about the supported privilege escalation types and their accompanying fields.

6. Configure each field for **SSH** authentication. See Tenable Security Center 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 Security Center.
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 Security Center 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	yes

Option	Description	Required
	information that you want to retrieve.	
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
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 Security Center scanner and the CyberArk AIM gateway using HTTPS and/or client certificates. For information on securing the connection, refer to Tenable Security Center 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 Security Center, 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]

[Retrieving Addresses to Scan from CyberArk]

[Debugging CyberArk Issues]

[About Tenable]

CyberArk Domain and DNS Support

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

Retrieving Addresses to Scan from CyberArk

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

Debugging CyberArk

To enable debugging when you configure a scan in Tenable Security Center:

1. In Tenable Security Center, 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.