Tenable and CyberArk Enterprise Password Vault Integration Guide

Last Revised: April 01, 2026

Table of Contents

Welcome to Tenable for 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, customers have more choice and flexibility.

The benefits of integrating Tenable with CyberArk include:

- Credential updates directly in Tenable, 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.

What information does the CyberArk integration collect?

Tenable's CyberArk integration provides PAM support for the following credential types: SSH, Windows, Database, VMware, Nutanix and SNMPv3. For these credential types, the integration collects usernames, passwords, and SSH keys. The scanner uses these values to authenticate to the target(s) listed in the scan's settings, instead of these values needing to be manually entered.

To use the CyberArk integration, select CyberArk as the authentication method of one of the supported credential types.

Information collected with Auto-Discovery

CyberArk with Auto-Discovery is also available for Windows, SSH and Database credential types. For Auto-Discovery, the integration also collects host names or addresses, along with their respective credentials.

Tenable Nessus with CyberArk

Database Integration

Required User Role: Standard, Scan Manager, or Administrator

Tenable Nessus Manager provides full database support for CyberArk.

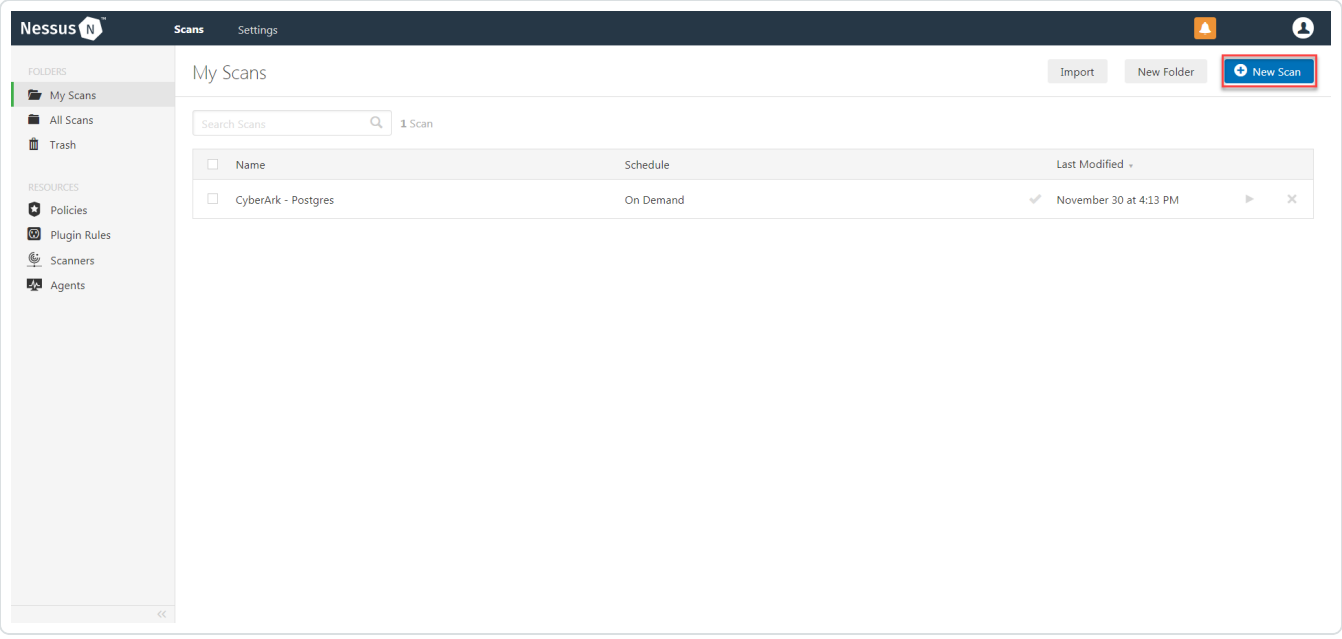
Before you begin:

- Ensure you have both a Tenable Nessus Manager and CyberArk account.

To configure Database integration:

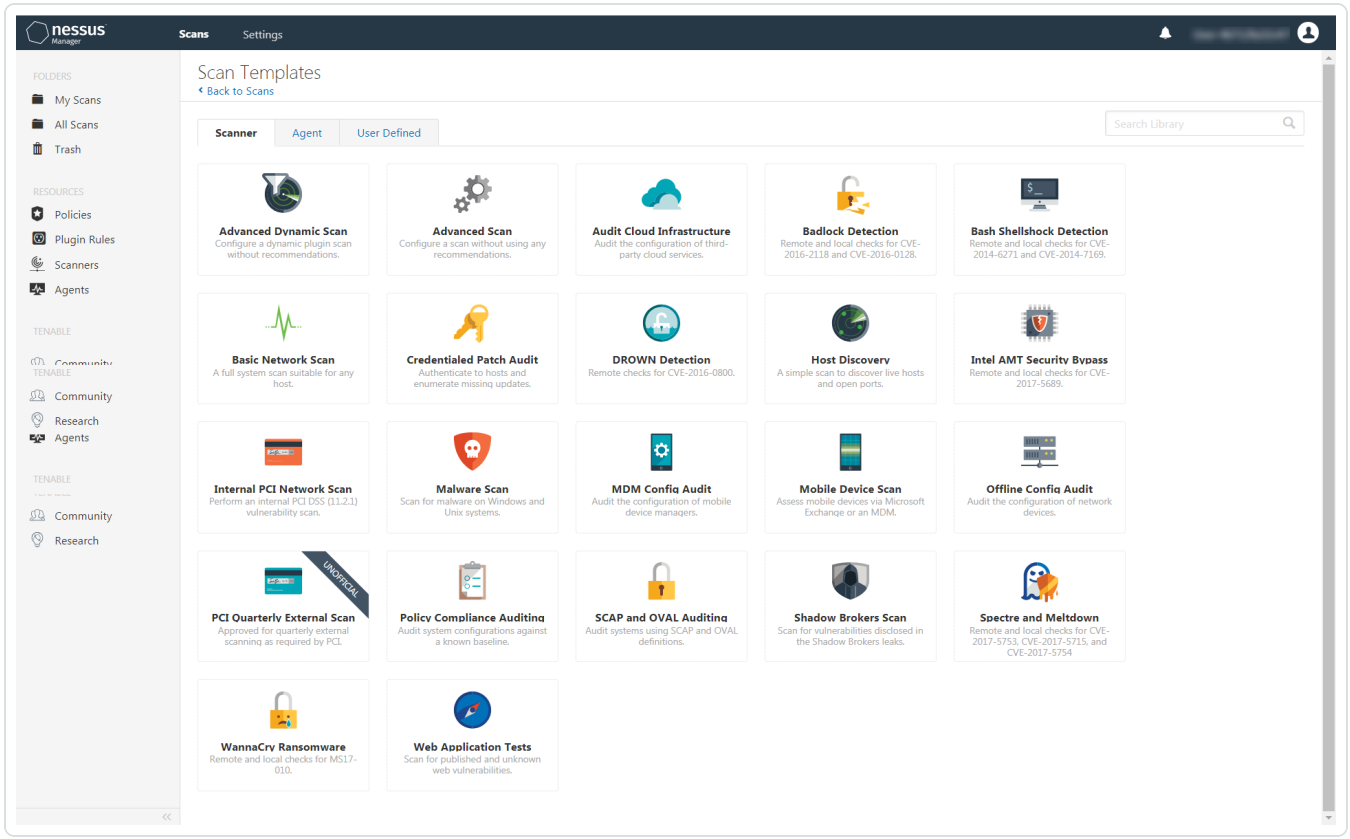
1. Log in to Tenable Nessus Manager.
2. In the left navigation plane, click **Scans**.

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



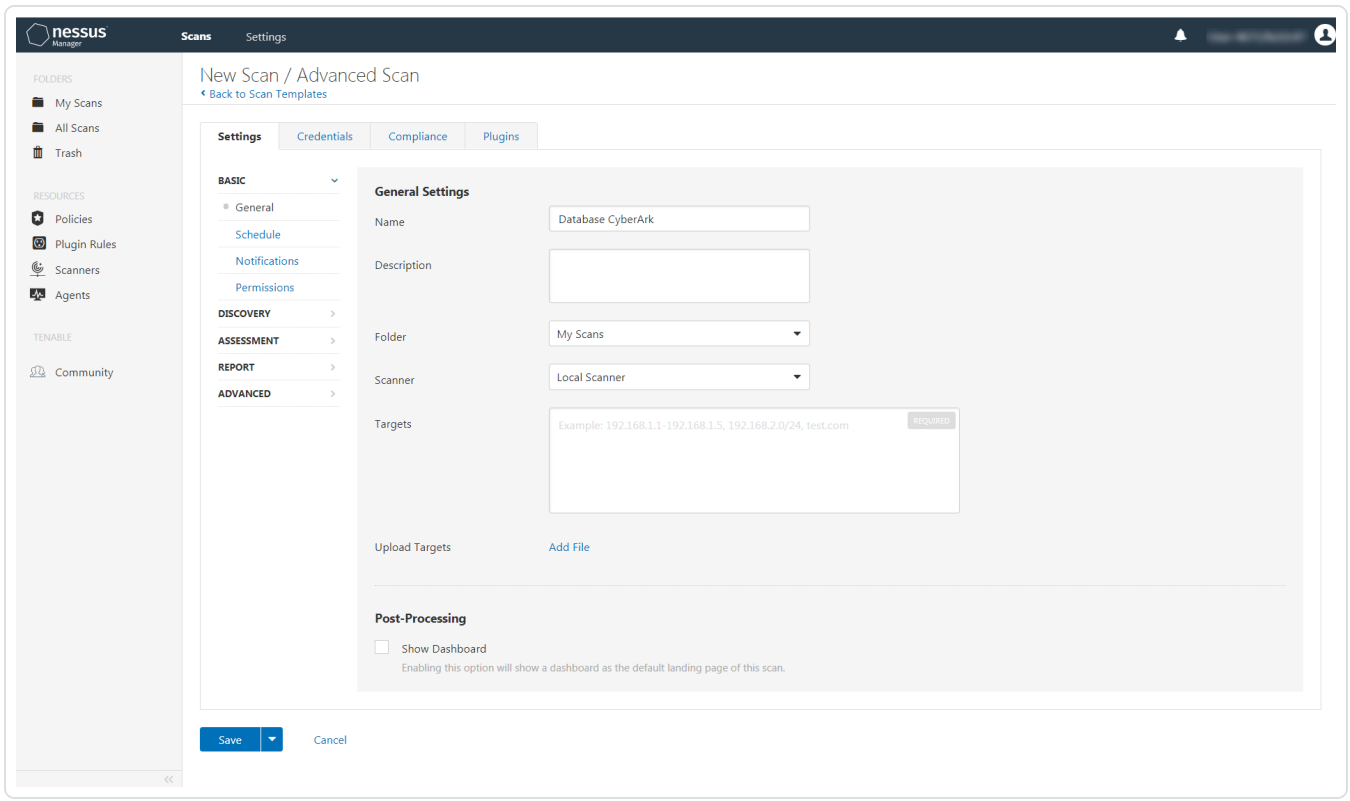
   The **Scan Templates** page appears.

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 **Categories** drop-down, select **Database**.

   The **Database** options appear.

10. Click **Database**.

    The **Database** options appear.

11. Click the **Database Type** drop-down.

12. The **Database** field options appear.

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

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

    The **CyberArk** field options appear.

15. Configure each field for the **Database** authentication. Refer to the Nessus User Guide to view detailed descriptions for each option.

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. **Note:** Customers self-hosting CyberArk CCP on a Windows Server 2022 and above should follow the guidance found in Tenable's Community post about CyberArk Client Certification Authentication Issue.	no
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	Yes, if the 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 **Address**, **Identifier**, **Parameters**, or **Username**. **Note:** For more information about the **Parameters** option, refer to the **Parameters Options** table.	yes

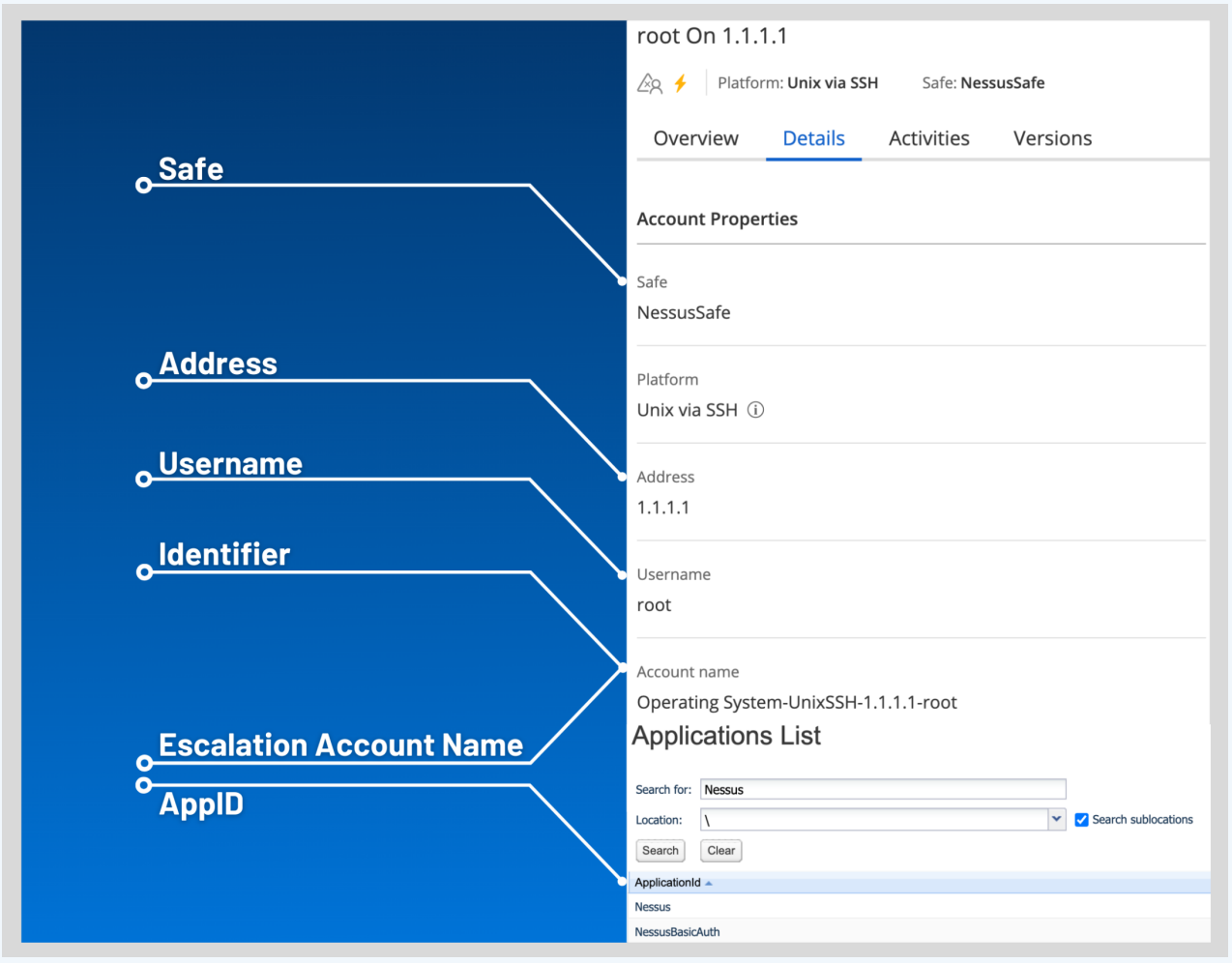
Option	Description	Required
	Note: The frequency of queries for **Username** is one query per target. The frequency of queries for **Identifier** is one query per chunk. This feature requires all targets have the same identifier.	
Username	(If **Get credential by** is set to **Username**) The username 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

Parameters Options

The following options can be specified when **Get Credential By** is set to **Parameters**. These request parameters allow for advanced filtering of accounts based on their properties. The options correspond to the various options supported by the CyberArk REST API, as found in CyberArk documentation. These options can be specified in many different combinations to filter account results by their properties. For example, specifying **Root** as the **Folder** option results in a REST API query containing `&Folder=Root`.

Option	Description	Required
Safe	The safe containing the credential.	no
Address	Limit the query to accounts matching the specified address.	no
Use Target IP Address	(Optional) When enabled, the integration appends the target address to the credential query, which limits the query to accounts matching the scan target's address. This is ignored if **Address** is set.	no
Username	The username of the credential.	no
Account Name	The unique identifier assigned to the credential.	no
Folder	The folder of the credential.	no
Database	The database of the credential.	no
Query	Specify a custom "free query" using account properties. When this method is specified, all other search criteria are ignored.	no
Query Format	Defines the query format. allowed values are **Exact** and **Regexp**. The default is **Exact**. This value is ignored unless the **Query** option was specified.	no

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



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

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.

16. Click **Save**.

SSH Integration

Required User Role: Standard, Scan Manager, or Administrator

To configure SSH integration:

1. Log in to Tenable Nessus Manager.
2. In the left navigation plane, click **Scans**.

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

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

   The selected scan template 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 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.

Option	Description	Required
CyberArk Elevate Privileges With	The privilege escalation method you want to use to increase users' privileges after initial	no

Option	Description	Required
	authentication. Your **CyberArk Elevate Privileges With** selection determines the specific options you must configure. For more information, see Privilege Escalation.	
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. **Note:** Customers self-hosting CyberArk CCP on a Windows Server 2022 and above should follow the guidance found in Tenable's Community post about CyberArk Client Certification Authentication Issue.	no
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	Yes, if the private key is applied.
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	Yes, if the private key is applied.
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes

Option	Description	Required
KDC Port	(Required if Kerberos Target Authentication is enabled.) The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	yes
KDC Transport	(Required if Kerberos Target Authentication is enabled.) The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	yes
Realm	(Required if Kerberos Target Authentication is enabled) The Realm is the authentication domain, usually noted as the domain name of the target (for example, example.com). By default, Tenable uses 443.	yes
Get credential by	The method with which your CyberArk API credentials are retrieved. Can be **Address**, **Identifier**, **Parameters**, or **Username**. **Note:** For more information about the **Parameters** option, refer to the **Parameters Options** table. **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.	yes
Username	(If **Get credential by** is set to **Username**) The username of the CyberArk user to request a password from.	no

Option	Description	Required
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
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows	no

Option	Description	Required
	the scan to access the target faster.	

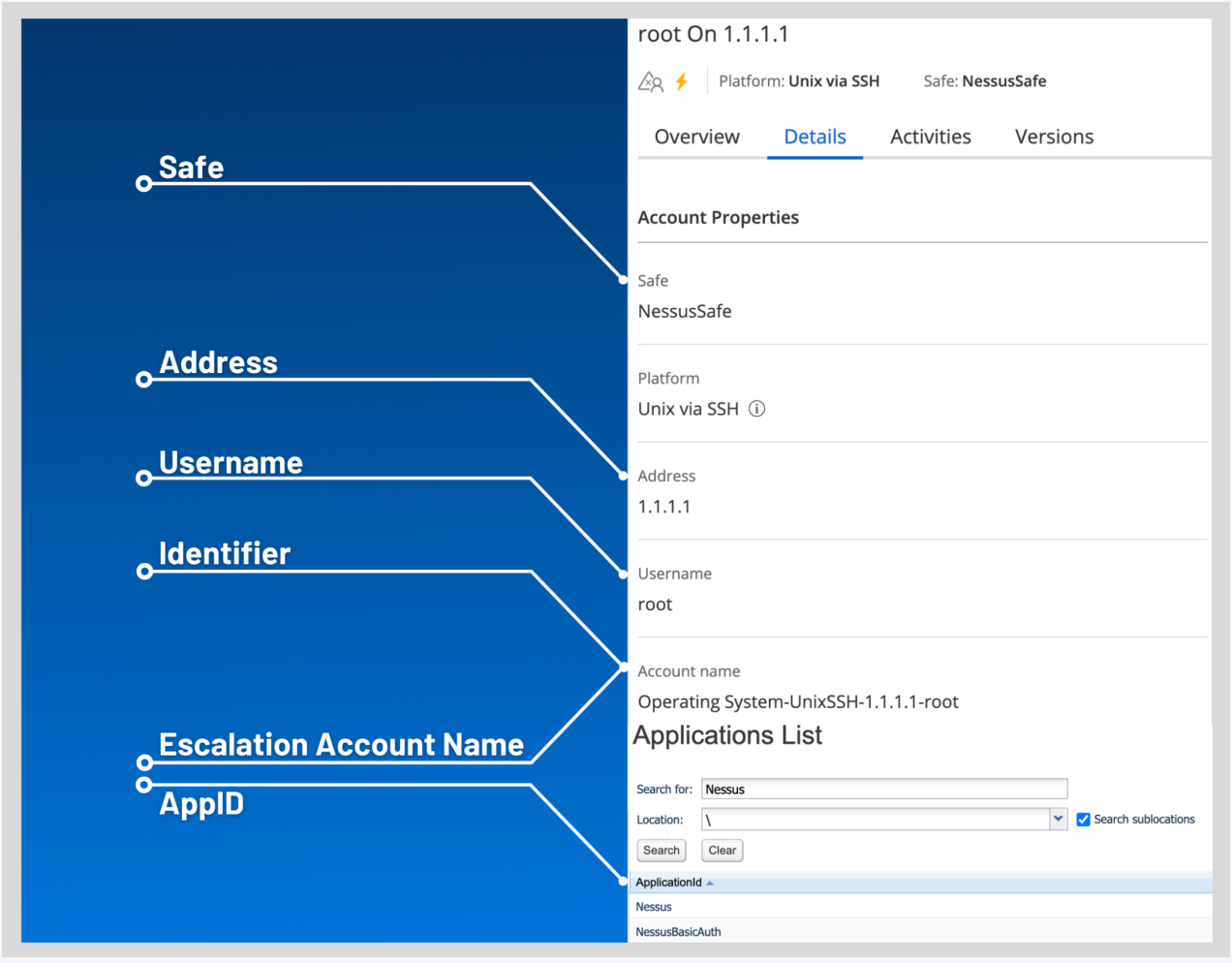
Parameters Options

The following options can be specified when **Get Credential By** is set to **Parameters**. These request parameters allow for advanced filtering of accounts based on their properties. The options correspond to the various options supported by the CyberArk REST API, as found in CyberArk documentation. These options can be specified in many different combinations to filter account results by their properties. For example, specifying **Root** as the **Folder** option results in a REST API query containing `&Folder=Root`.

Option	Description	Required
Safe	The safe containing the credential.	no
Address	Limit the query to accounts matching the specified address.	no
Use Target IP Address	(Optional) When enabled, the integration appends the target address to the credential query, which limits the query to accounts matching the scan target's address. This is ignored if **Address** is set.	no
Username	The username of the credential.	no
Account Name	The unique identifier assigned to the credential.	no
Folder	The folder of the credential.	no
Database	The database of the credential.	no
Query	Specify a custom "free query" using account properties. When this method is specified, all other search criteria are ignored.	no
Query Format	Defines the query format. allowed values are **Exact**	no

Option	Description	Required
	and **Regexp**. The default is **Exact**. This value is ignored unless the **Query** option was specified.	

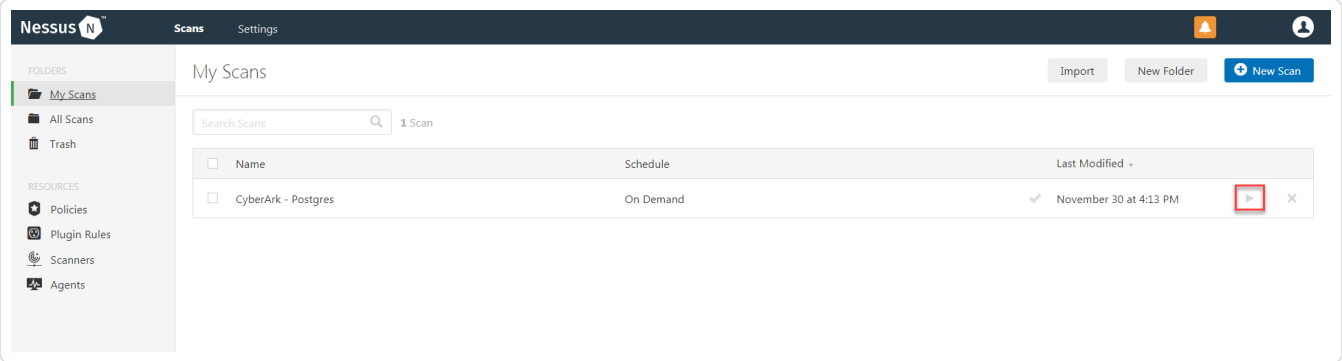
CyberArk credential field mapping to the CyberArk Accounts detail view in the CyberArk console:



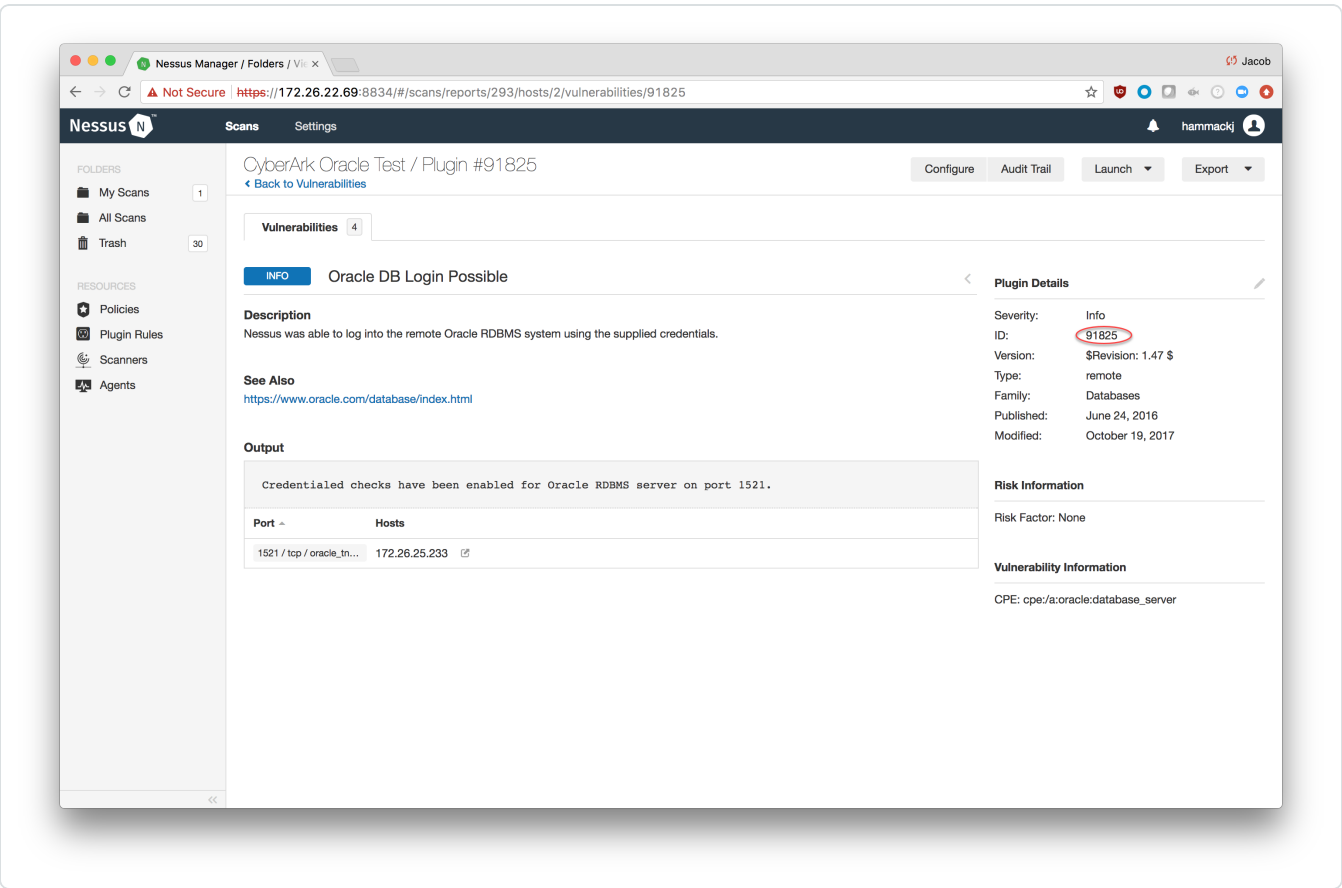
13. Click **Save**.

Verification

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



2. Once the scan has completed, select the completed scan. Look for the corresponding **ID** which validates that the authentication was successful. If the authentication is not successful, refer to the Debugging CyberArk Issues section of this document.



Privilege Escalation With CyberArk Credentials

Required User Role: Standard, Scan Manager, or Administrator

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

Before you begin:

- Ensure you have both a Tenable Nessus Manager and CyberArk account.

To configure SSH integration:

1. Log in to Tenable Nessus Manager.
2. In the left navigation plane, click **Scans**.

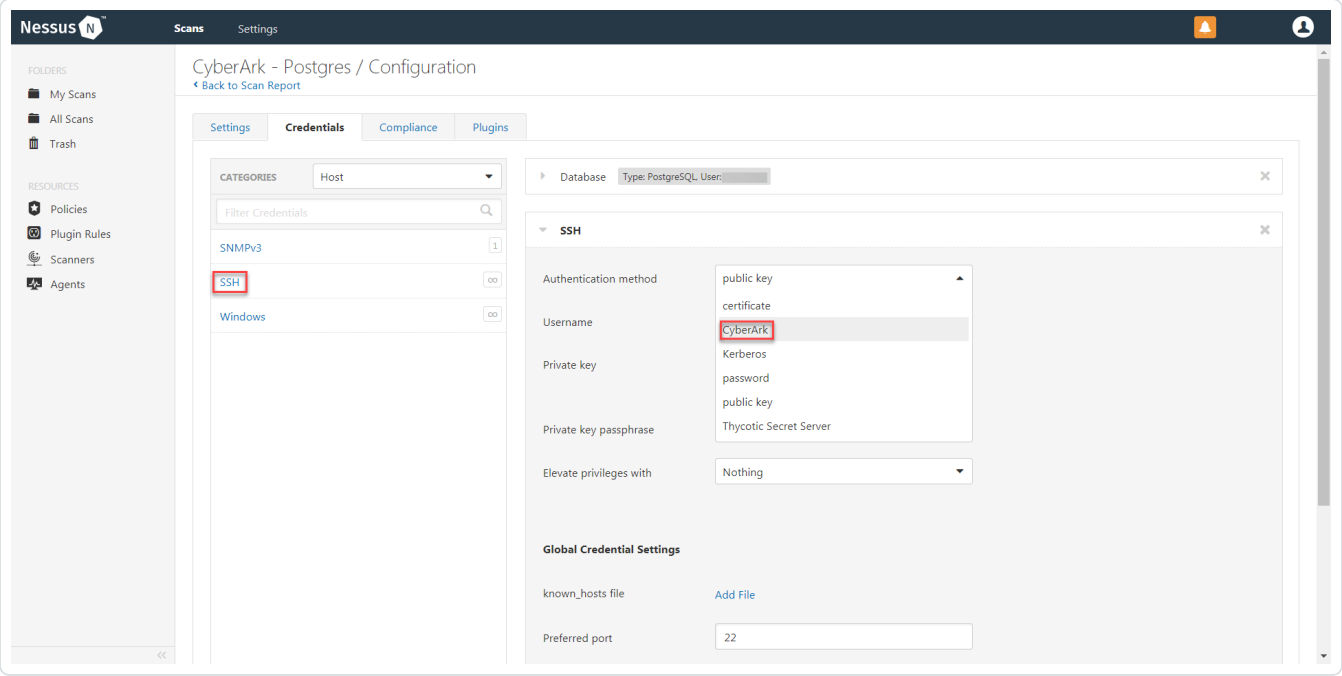
   The **Scans** page appears.
3. Click **+ New Scan**.

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

   The selected scan template 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 options appear.
9. In the left-hand menu, select **SSH**.
10. Click **Authentication method**.

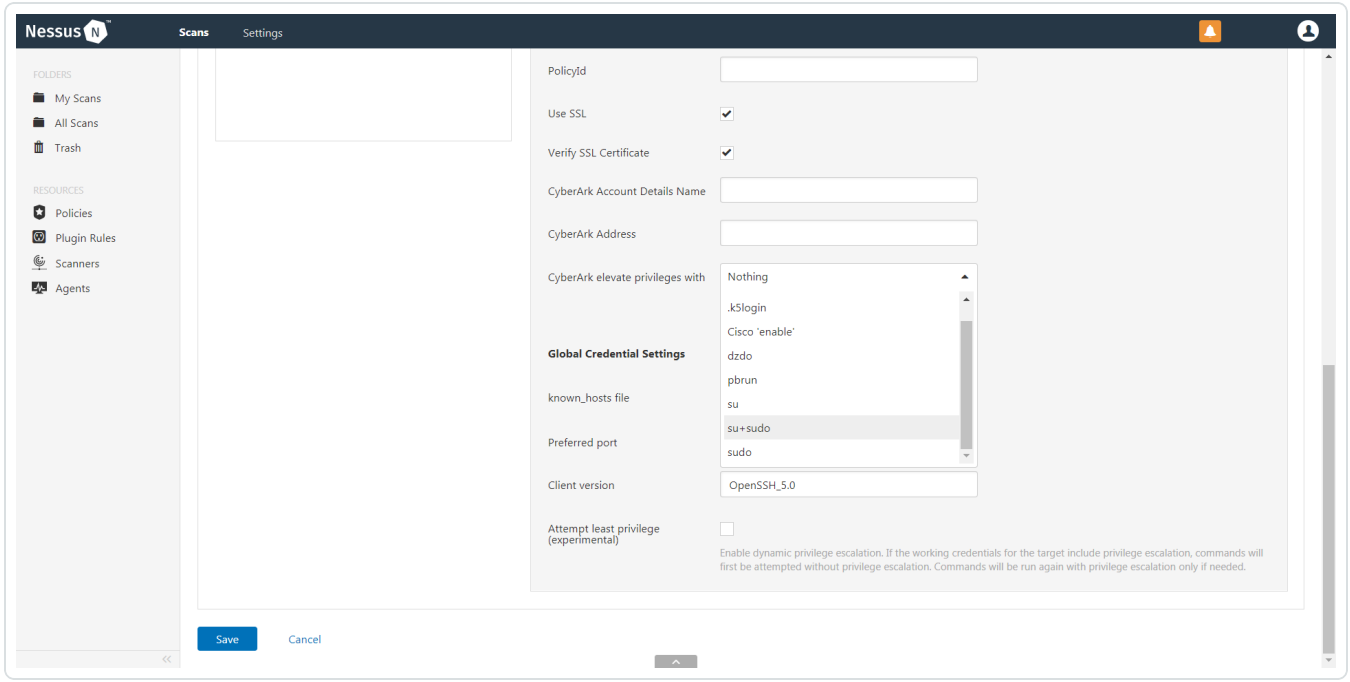
    A drop-down appears.
11. Select **CyberArk**.



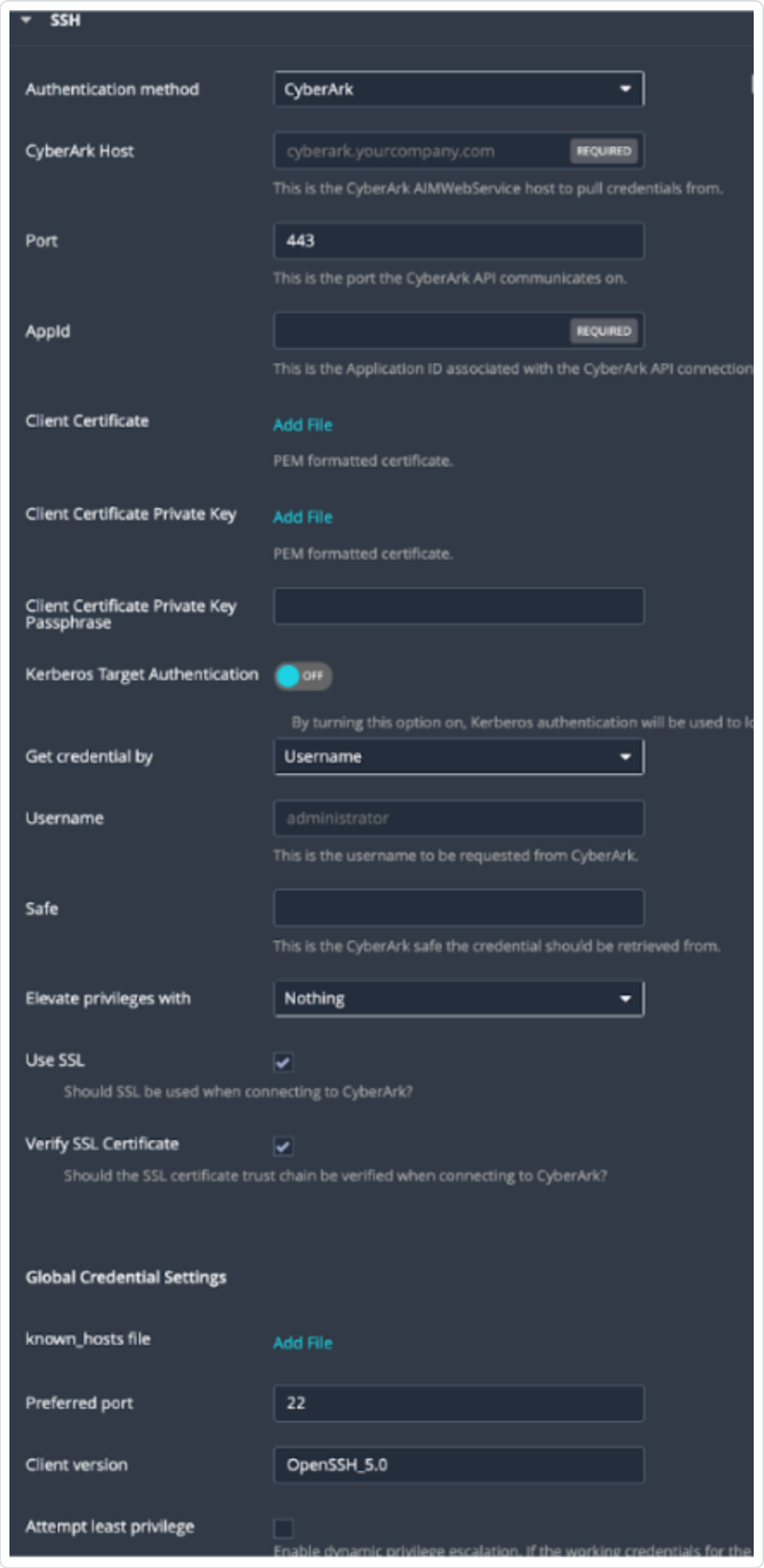
12. An option for **CyberArk elevate privileges with** appears near the bottom of the configuration page.

> **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**, **Get Escalation Credential By**, and **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 Nessus User Guide.



13. Configure each field for SSH authentication. Refer to the Nessus User Guide to get detailed descriptions for each option.


SSH
Authentication method
CyberArk
CyberArk Host
cyberark.yourcompany.com
REQUIRED
This is the CyberArk AIMWebService 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
Client Certificate
Add File
PEM formatted certificate.
Client Certificate Private Key
Add File
PEM formatted certificate.
Client Certificate Private Key Passphrase
Kerberos Target Authentication
OFF
By turning this option on, Kerberos authentication will be used to l
Get credential by
Username
Username
administrator
This is the username to be requested from CyberArk.
Safe
This is the CyberArk safe the credential should be retrieved from.
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?
Global Credential Settings
known_hosts file
Add File
Preferred port
22
Client version
OpenSSH_5.0
Attempt least privilege
Enable dynamic privilege escalation. If the working credentials for the

> **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.

14. Click **Save**.

Windows Integration

> **Required User Role:** Standard, Scan Manager, or Administrator

Tenable Nessus Manager provides an option for CyberArk Windows integration. Complete the following steps to configure Tenable Nessus Manager with CyberArk for Windows.

Before you begin:

- Ensure you have both a Tenable Nessus Manager and CyberArk account.

To configure Windows integration:

1. Log in to Tenable Nessus Manager.
2. In the left navigation plane, click **Scans**.

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

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

   The selected scan template 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** options appear.

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

10. Click **Authentication method**.

    A drop-down appears.

11. Select **CyberArk**.

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

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

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. **Note:** Customers self-hosting CyberArk CCP on a Windows Server 2022 and above should follow the guidance found in Tenable's Community post about CyberArk Client Certification Authentication Issue.	no
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	Yes, if the private key is applied.

Option	Description	Required
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	Yes, if the private key is applied.
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	(Required if Kerberos Target Authentication is enabled) The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	yes
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	yes
Domain	(Required if Kerberos Target Authentication is enabled) The domain to which Kerberos Target Authentication belongs, if applicable.	yes
Get credential by	The method with which your CyberArk API credentials are retrieved. Can be **Address**, **Identifier**, **Parameters**, or **Username**. **Note:** For more information about the **Parameters** option, refer to the **Parameters Options** table. **Note:** The frequency of queries for **Username** is one	yes

Option	Description	Required
	query per target. The frequency of queries for **Identifier** is one query per chunk. This feature requires all targets have the same identifier.	
Username	(If **Get credential by** is set to **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

Parameters Options

The following options can be specified when **Get Credential By** is set to **Parameters**. These request parameters allow for advanced filtering of accounts based on their properties. The options correspond to the various options supported by the CyberArk REST API, as found in CyberArk documentation. These options can be specified in many different combinations to filter account results by their properties. For example, specifying **Root** as the **Folder** option results in a REST API query containing `&Folder=Root`.

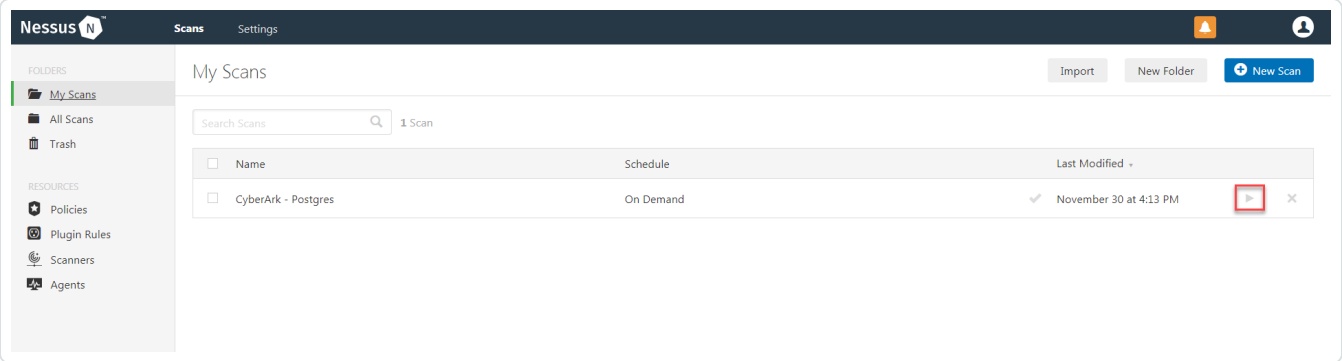
Option	Description	Required
Safe	The safe containing the credential.	no
Address	Limit the query to accounts matching the specified address.	no
Use Target IP Address	(Optional) When enabled, the integration appends the target address to the credential query, which limits the query to accounts matching the scan target's address. This is ignored if **Address** is set.	no
Username	The username of the credential.	no
Account Name	The unique identifier assigned to the credential.	no
Folder	The folder of the credential.	no
Database	The database of the credential.	no
Query	Specify a custom "free query" using account properties. When this method is specified, all other search criteria are ignored.	no
Query Format	Defines the query format. allowed values are **Exact** and **Regexp**. The default is **Exact**. This value is ignored unless the **Query** option was specified.	no

(missing or bad snippet)

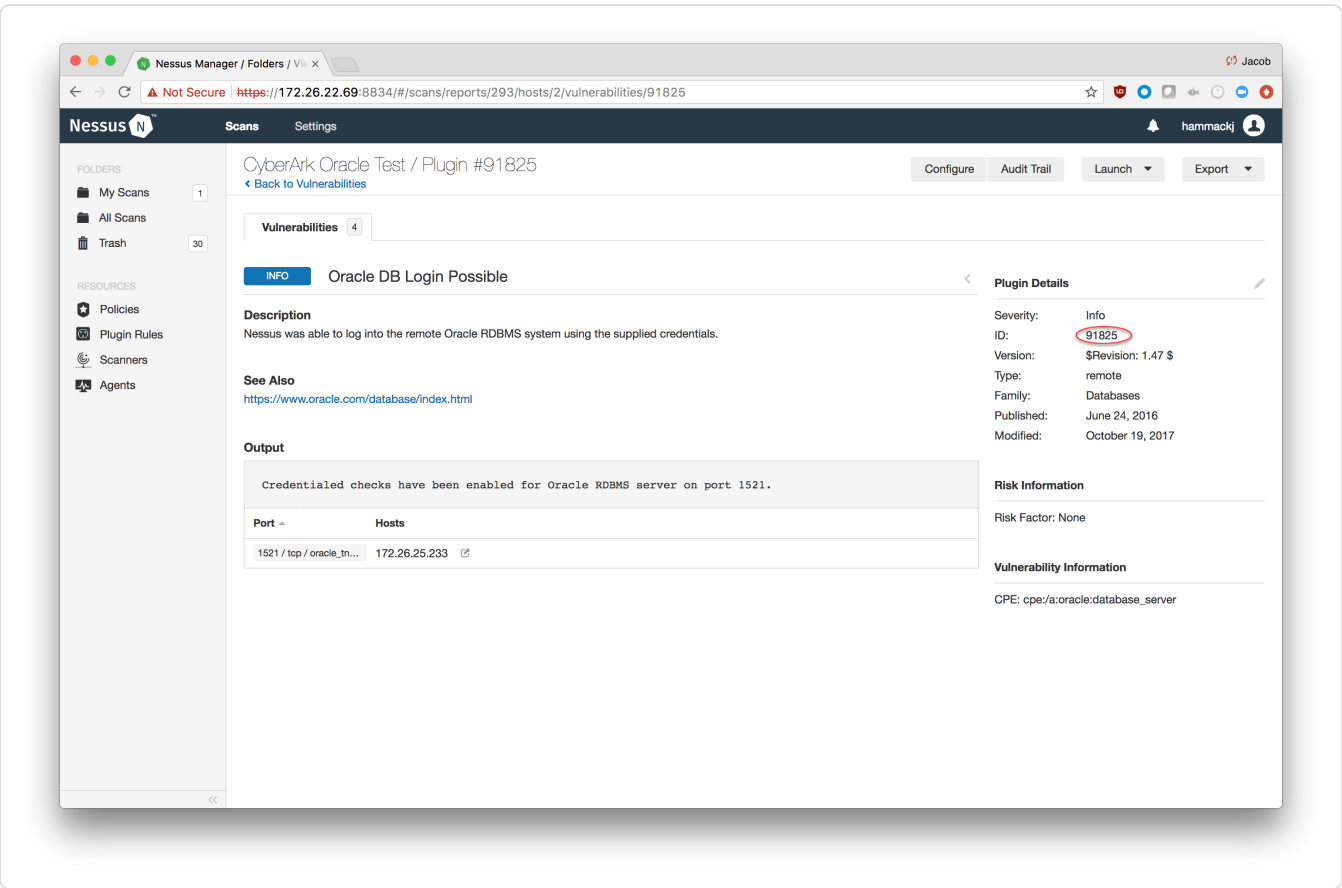
13. Click **Save**.

Verification

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



2. Once the scan has completed, select the completed scan. Look for the corresponding **ID** which validates that the authentication was successful. If the authentication is not successful, refer to the Debugging CyberArk Issues section of this document.

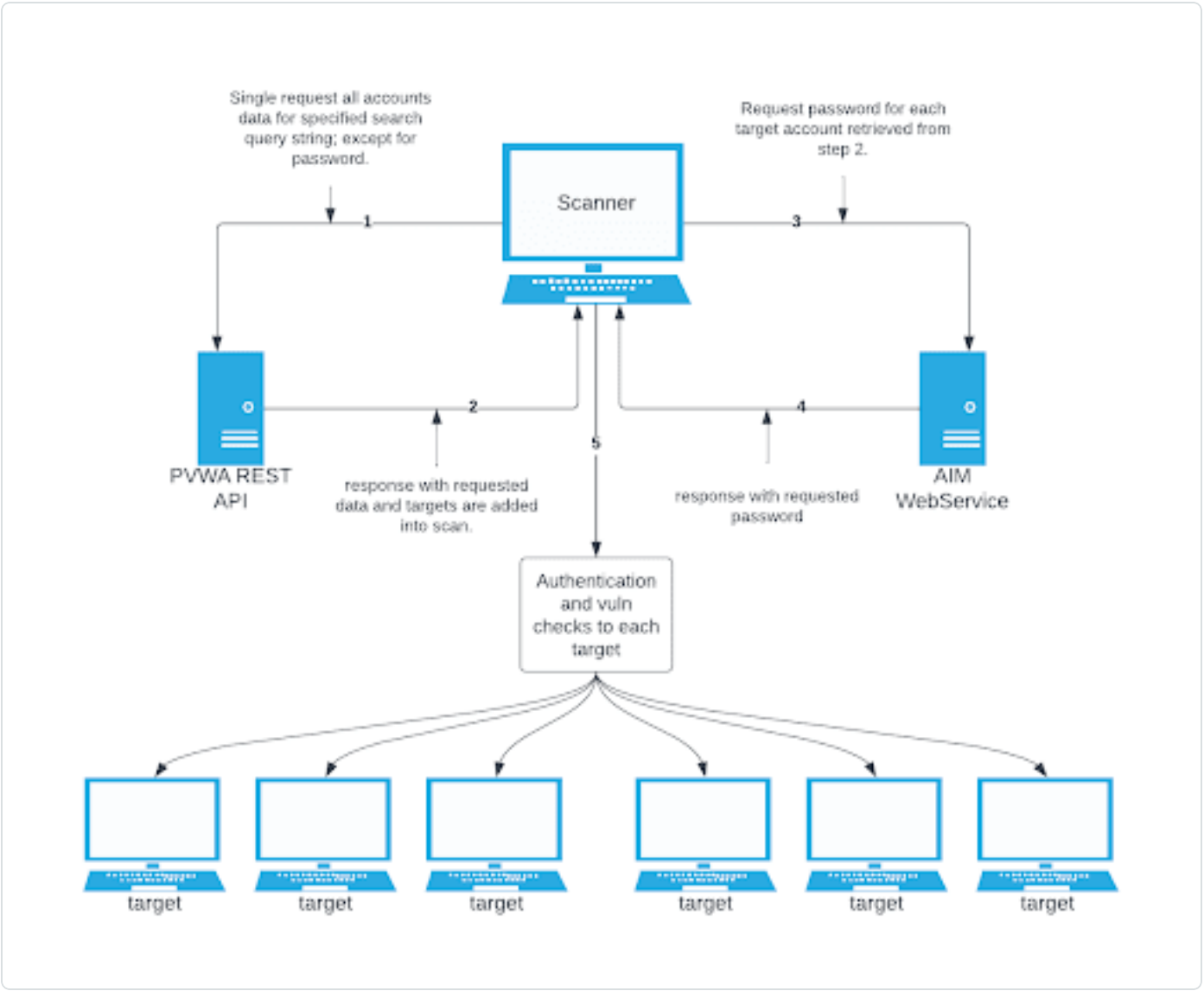


CyberArk Dynamic Scanning

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.

Caution: Tenable recommends utilizing scanner groups with one scanner when using Auto-Discovery credentials and users should only enter only a single initial host in the scan. If multiple scanners are used in an Auto-Discovery scan, targets retrieved from the integration may be scanned multiple times.



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

> **Required User Role:** Standard, Scan Manager, or Administrator

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 are not 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

Field name	Description	Field value
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

Before you begin:

- Ensure you have both a Tenable Nessus Manager and CyberArk account.

To configure database auto-discovery:

1. Log in to Tenable Nessus Manager.
2. In the left navigation plane, click **Scans**.

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

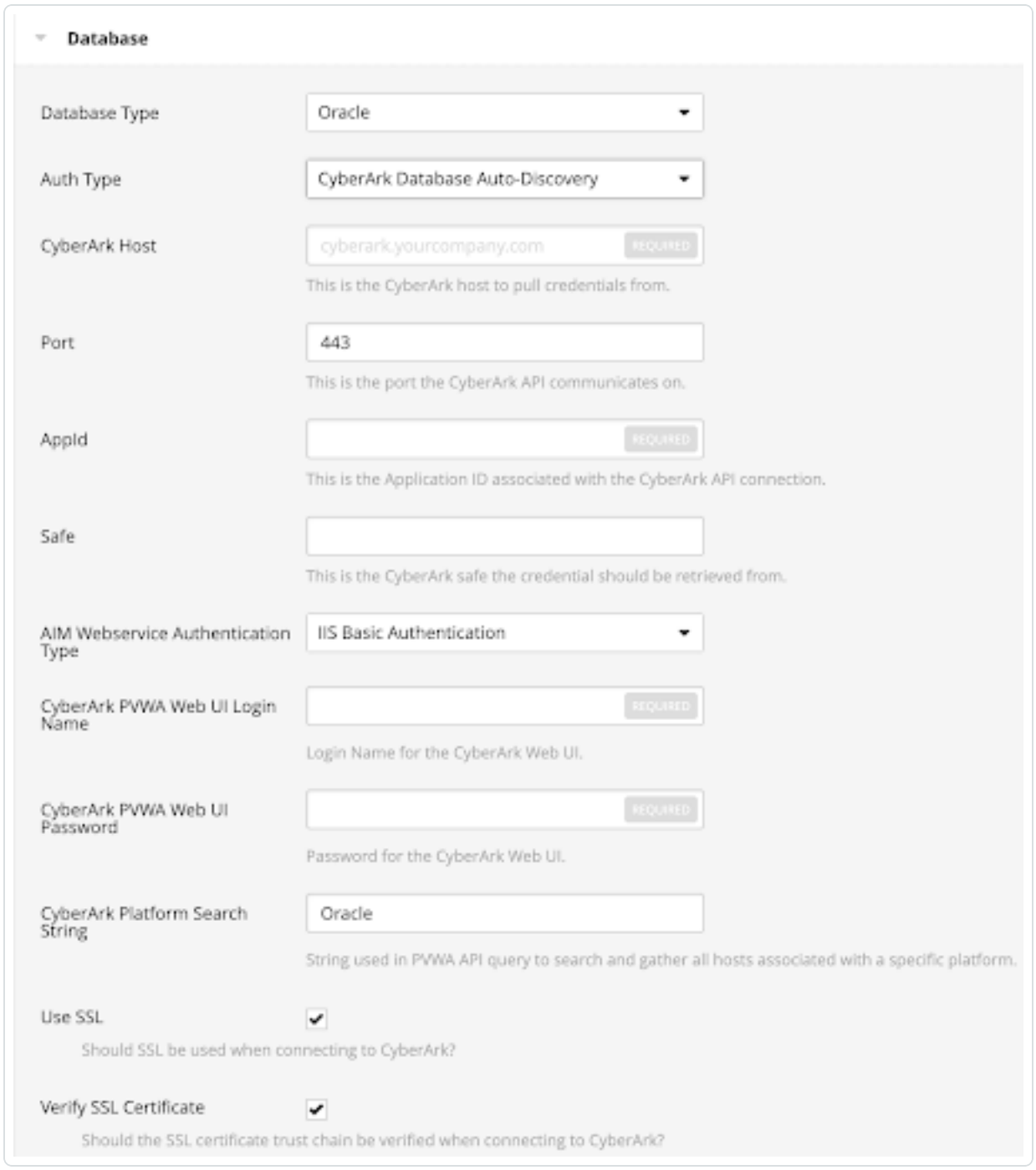
   The **Scan Templates** page appears.
4. Select a **Scan Template**. For demonstration, the **Advanced Network Scan** template is used.

   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:



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
	Note: Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	yes
CCP Host	The IP address or FQDN name for the user's CyberArk CCP component. (Not available with Tenable Security Center.) **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the CCP host.	no
CCP Port	The port on which the CyberArk CCP (AIM Web Service) API communicates. By default, Tenable uses 443. (Not available with Tenable Security Center.) **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the CCP host.	no
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

Option	Description	Required
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
PVWA REST API Authentication Method	Choose whether to authenticate to the PVWA by entering username and password or to gather credentials from the Central Credential Provider (CCP). (**Not available with Tenable Security Center.**)	yes
PVWA REST API Credential ID	The unique identifier ("Account name") of the CyberArk account containing CCP credentials. (**Not available with Tenable Security Center.**)	Yes, if the PVWA REST API Authentication Method is set to **Gather from CCP**.
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	yes

Option	Description	Required
	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.	
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 Vulnerability Management User Guide and the **Central Credential Provider Implementation Guide** located at cyberark.com (login required).

13. Click **Save**.

SSH Auto-Discovery

Required User Role: Standard, Scan Manager, or Administrator

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.

Note: Privilege Escalation is available, but only using the SUDO method at this time. More research is needed to explore other escalation methods.

Note: SSH Key authentication is supported, but escalated privileges after SSH Key authentication is not available at this time.

To configure SSH auto-discovery:

1. Log in to Tenable Nessus Manager.
2. In the left navigation plane, click **Scans**.

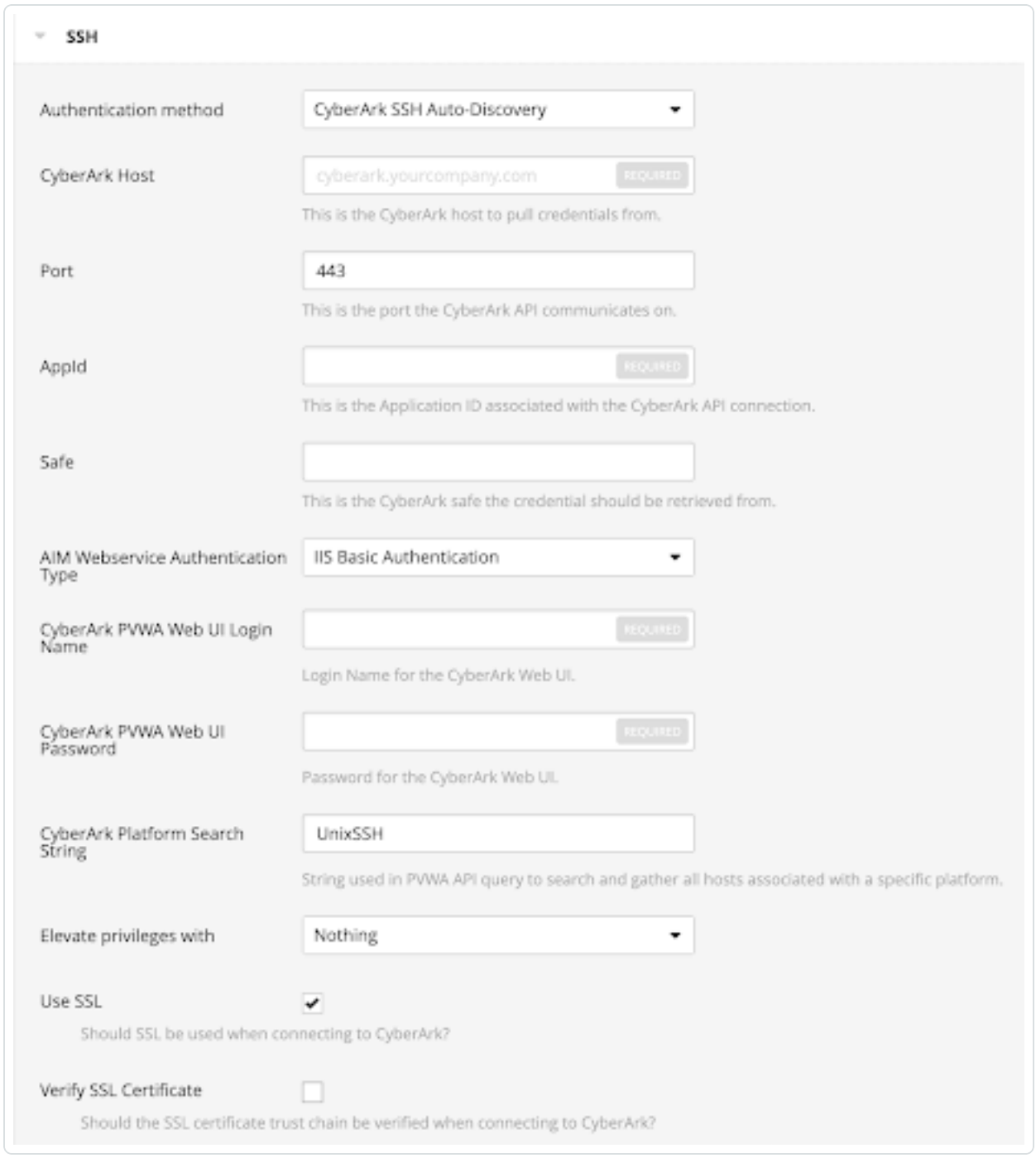
   The **Scans** page appears.
3. Click **+ New Scan**.

   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:



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
	Note: Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	yes
CCP Host	The IP address or FQDN name for the user's CyberArk CCP component. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	no
CCP Port	The port on which the CyberArk CCP (AIM Web Service) API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	no
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**	yes

Option	Description	Required
	Authentication and **Certificate Authentication**. Certificate Authentication can be either encrypted or unencrypted.	
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
PVWA REST API Authentication Method	Choose whether to authenticate to the PVWA by entering username and password or to gather credentials from the Central Credential Provider (CCP). (**Not available with Tenable Security Center.**)	yes
PVWA REST API Credential ID	The unique identifier ("Account name") of the CyberArk account containing CCP credentials. (**Not available with Tenable**	Yes, if the PVWA REST API Authentication

Option	Description	Required
	Security Center.)	Method is set to **Gather from CCP**.
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
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	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 Vulnerability Management User Guide and the **Central Credential Provider Implementation Guide** located at cyberark.com (login required).

13. Click **Save**.

Windows Auto-Discovery

Required User Role: Standard, Scan Manager, or Administrator

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.

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 left navigation plane, 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 left navigation plane, click **Settings**.

   The **Settings** page appears.

10. Click the **Credentials** widget.

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

11. Click the ⊕ button next to the **Credentials** title.

    The credential form plane appears.

12. Click the **Host** option.

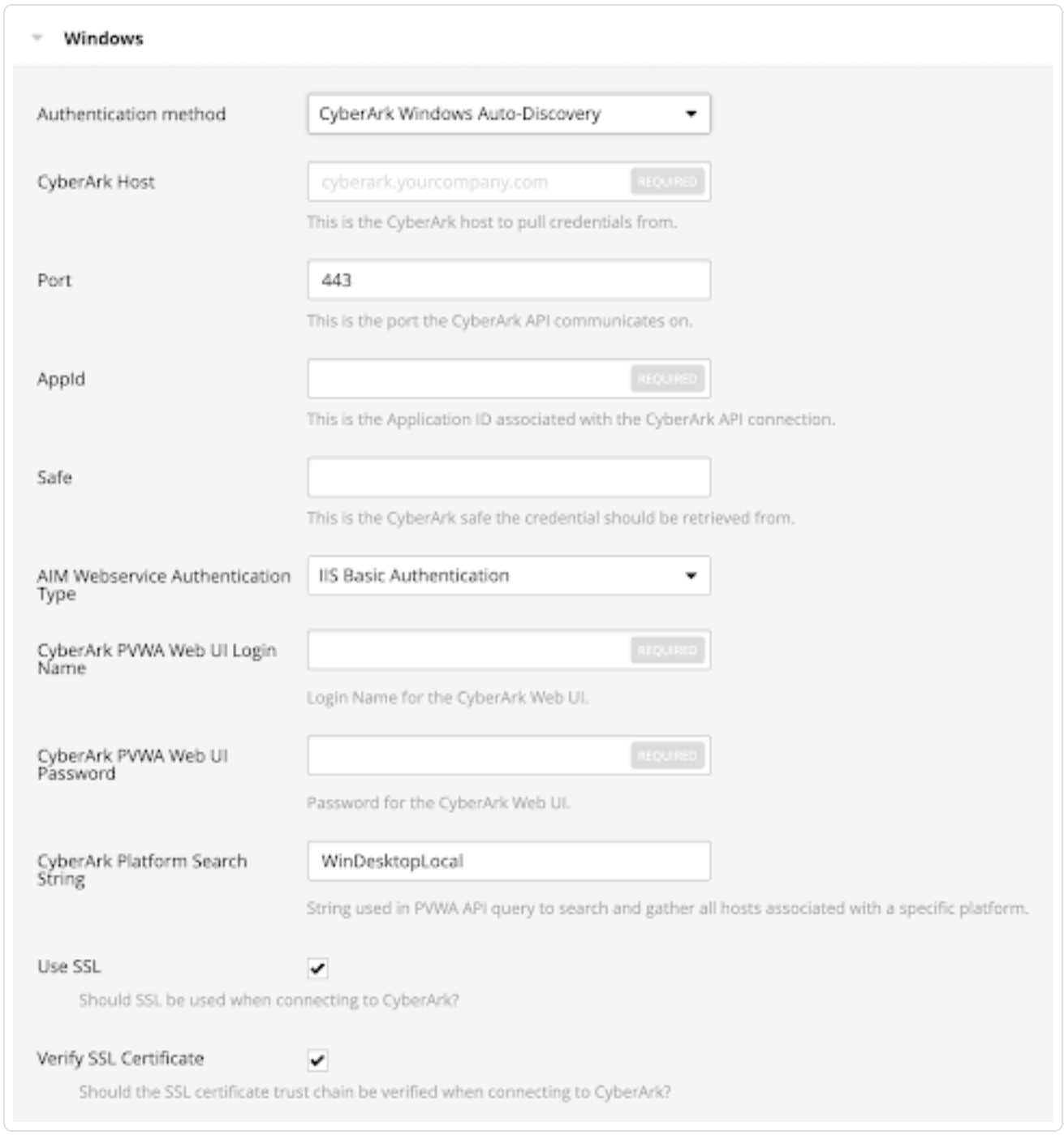
    The **Host** options appear.

13. In the **Host** section, click **Windows**.

    The selected credential options appear.

14. From the **Authentication Method** drop-down, select **CyberArk Windows Auto-Discovery**.

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



15. 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

Option	Description	Required
	Note: Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	yes
CCP Host	The IP address or FQDN name for the user's CyberArk CCP component. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	no
CCP Port	The port on which the CyberArk CCP (AIM Web Service) API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	no
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**	yes

Option	Description	Required
	Authentication and **Certificate Authentication**. Certificate Authentication can be either encrypted or unencrypted.	
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 practice would be to create a custom platform name in CyberArk and enter that value in this field to improve accuracy.	yes
PVWA REST API Authentication Method	Choose whether to authenticate to the PVWA by entering username and password or to gather credentials from the Central Credential Provider (CCP). (**Not available with Tenable Security Center.**)	yes
PVWA REST API Credential ID	The unique identifier ("Account name") of the CyberArk account containing CCP credentials. (**Not available with Tenable**	Yes, if the PVWA REST API Authentication

Option	Description	Required
	Security Center.)	Method is set to **Gather from CCP**.
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 Vulnerability Management User Guide and the **Central Credential Provider Implementation Guide** located at cyberark.com (login required).

16. Click **Save**.

CyberArk (Legacy) Integration

Caution: Support for SOAP requests are no longer be supported by CyberArk as of December 31, 2024. If you are using the CyberArk Legacy Integration which utilizes SOAP for API requests, Tenable recommends using our non-Legacy CyberArk Integration which supports REST API requests.

View one of the following options for CyberArk legacy integration steps.

Database (Legacy) Integration

SSH (Legacy) Integration

Privilege Escalation (Legacy)

Windows (Legacy) Integration

Database (Legacy) Integration

Caution: Support for SOAP requests are no longer be supported by CyberArk as of December 31, 2024. If you are using the CyberArk Legacy Integration which utilizes SOAP for API requests, Tenable recommends using our non-Legacy CyberArk Integration which supports REST API requests.

Tenable Nessus Manager provides full database support for CyberArk. Complete the following steps to configure Tenable Nessus Manager with CyberArk Vault

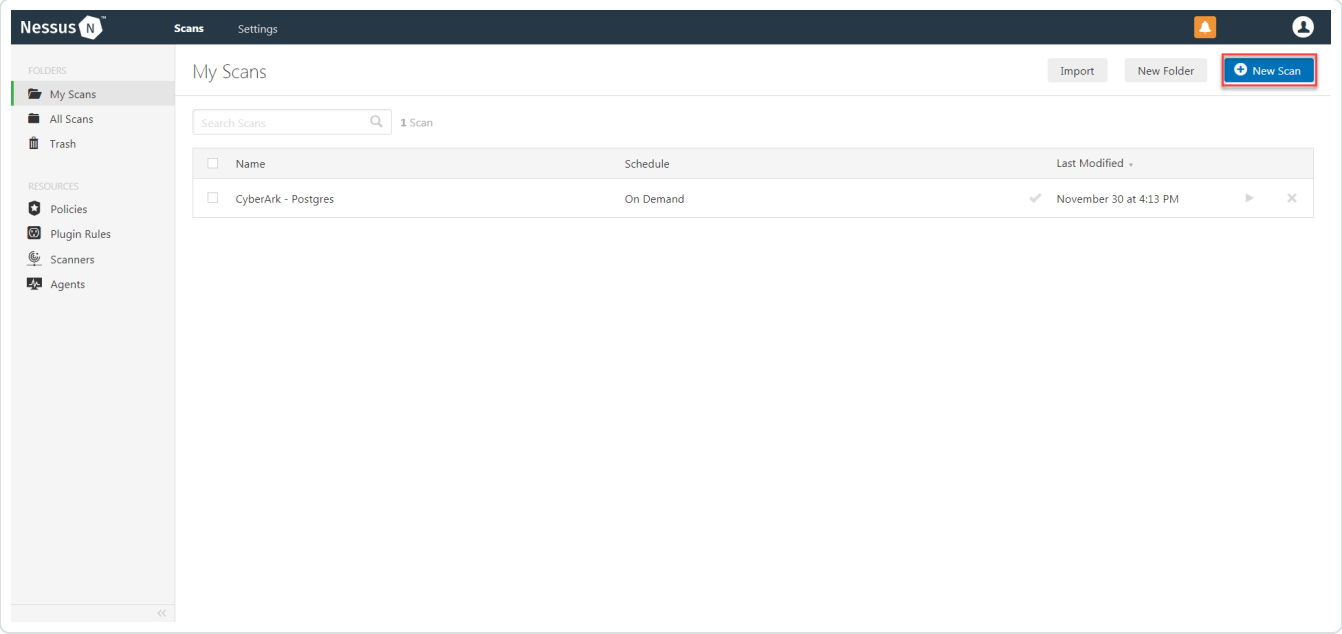
Requirements:

- CyberArk account
- Nessus Manager account

To configure Database integration:

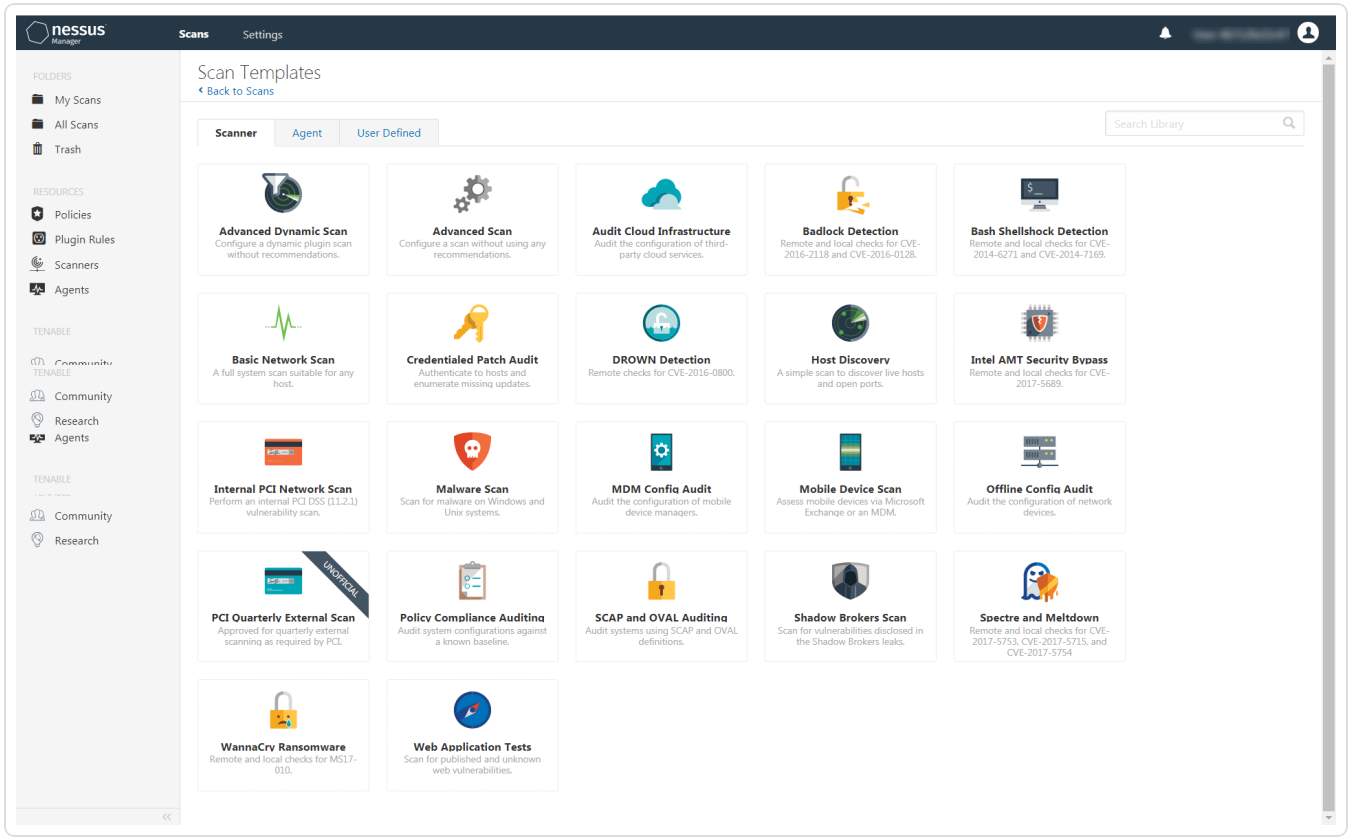
1. Log in to Tenable Nessus Manager-.
2. Click **Scans**.

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



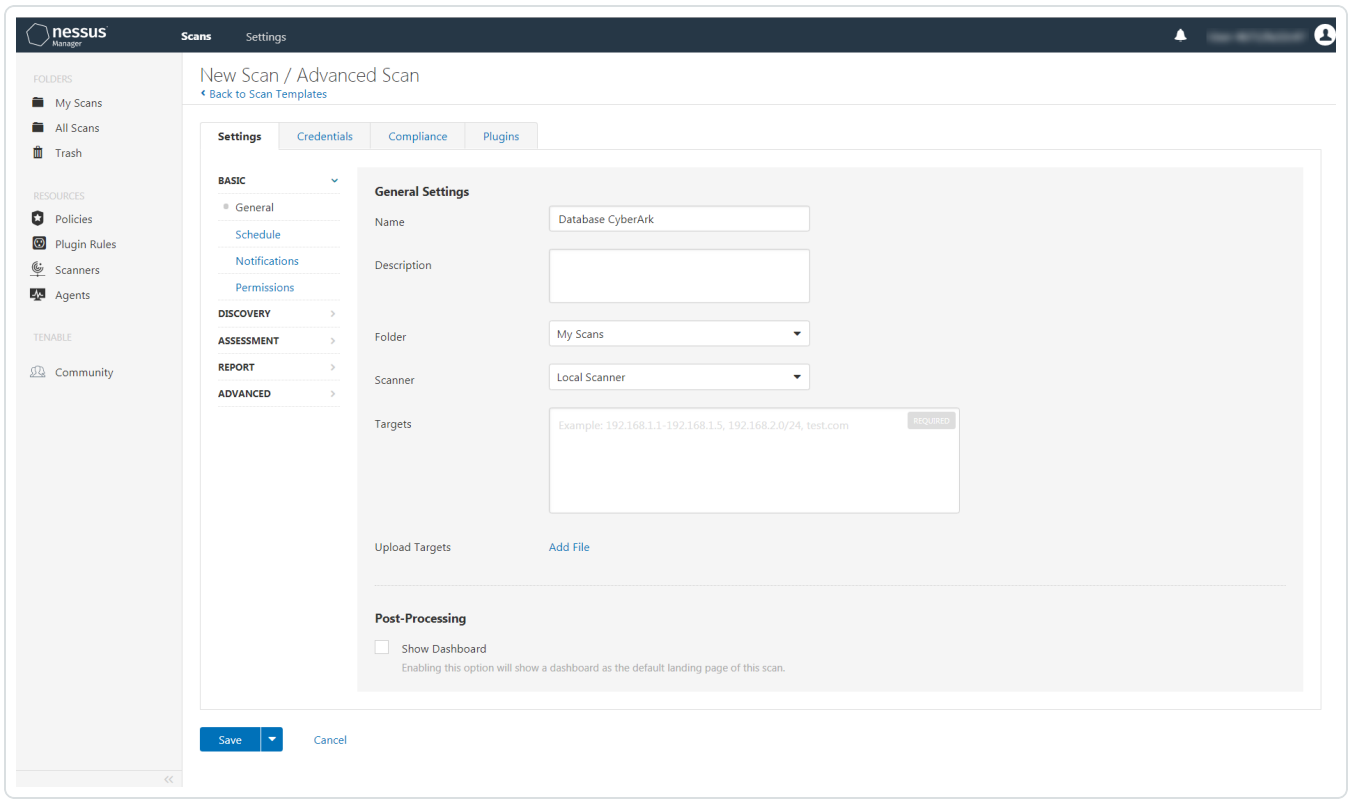
   The **Scan Templates** page appears.

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 **Categories** drop-down, select **Database**.

   The **Database** options appear.

10. Click **Database**.

    The **Database** options appear.

11. Click the **Database Type** drop-down.

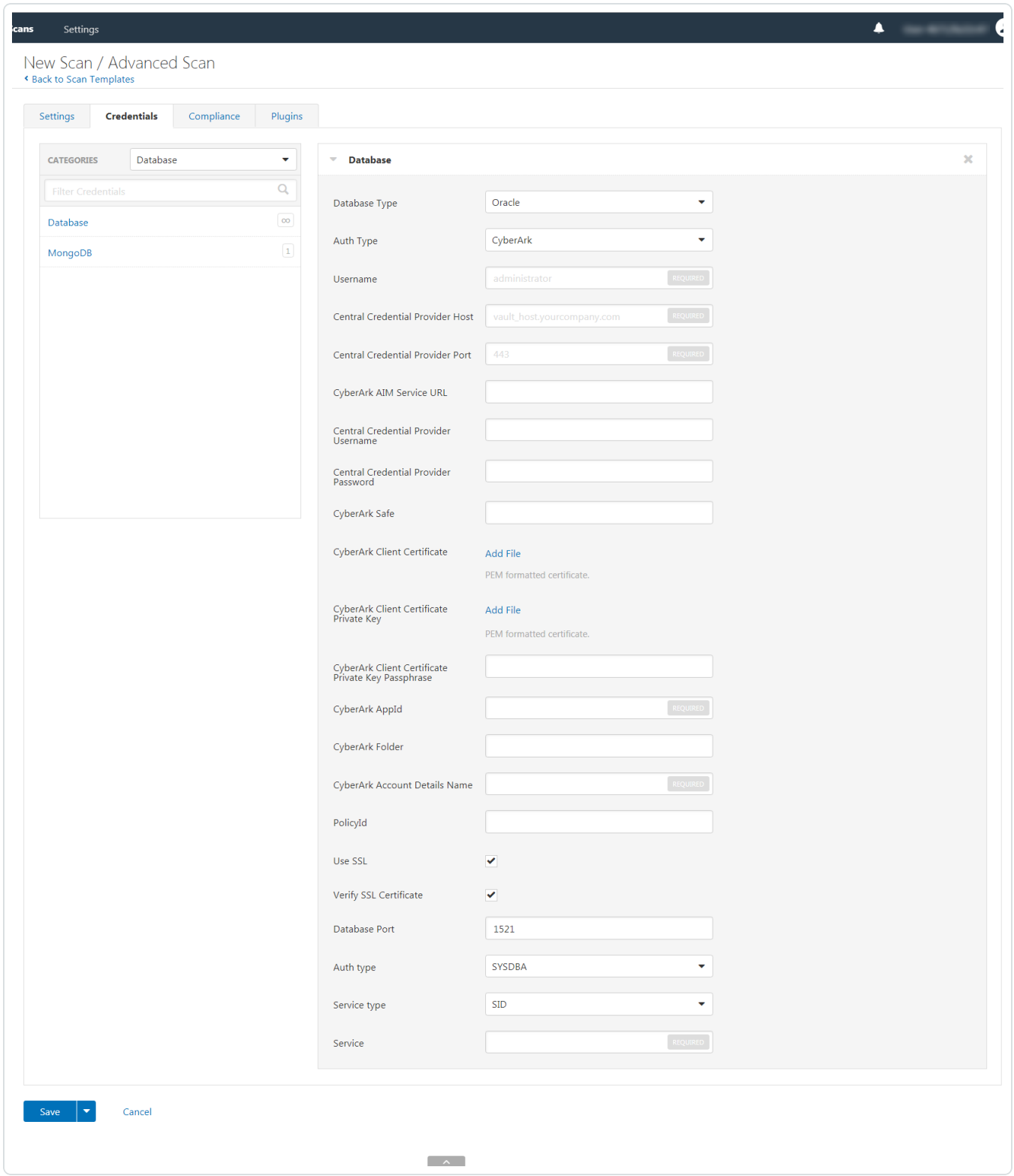
12. The **Database** field options appear.

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

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

    The **CyberArk** field options appear.

15. Configure each field for the **Database** authentication. See the Nessus User Guide to view detailed descriptions for each option.



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

16. Click **Save**.

SSH (Legacy) Integration

Caution: Support for SOAP requests are no longer be supported by CyberArk as of December 31, 2024. If you are using the CyberArk Legacy Integration which utilizes SOAP for API requests, Tenable recommends using our non-Legacy CyberArk Integration which supports REST API requests.

To configure SSH integration:

1. Log in to Nessus.
2. Click **Scans**.
3. Click **+ New Scan**.

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

   The selected scan template 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 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.

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 uses `/AIMWebservice/v1.1/AIM.asmx`. **Note:** When the customer is using the default path, they can leave this blank.	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	If the CyberArk Central Credential Provider (CCP) is configured to use basic authentication, you can fill in this field for authentication. **Note:** This field should be the Username to Authenticate to the AIM Web Service API.	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

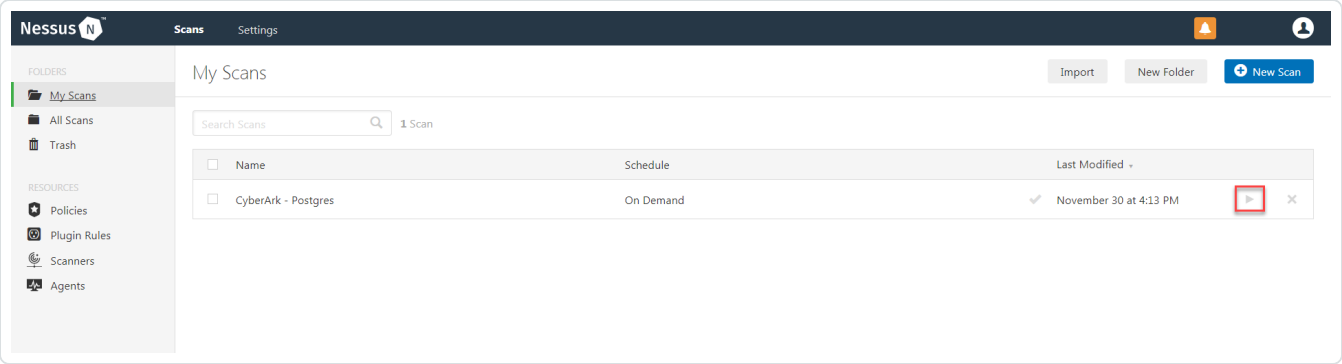
Option	Description	Required
CyberArk Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host.	no
CyberArk Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	no
CyberArk Client Certificate Private Key Passphrase	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
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

Option	Description	Required
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 CyberArk receiving an unrecognized password prompt on the target host's interactive SSH shell.	no

13. Click **Save**.

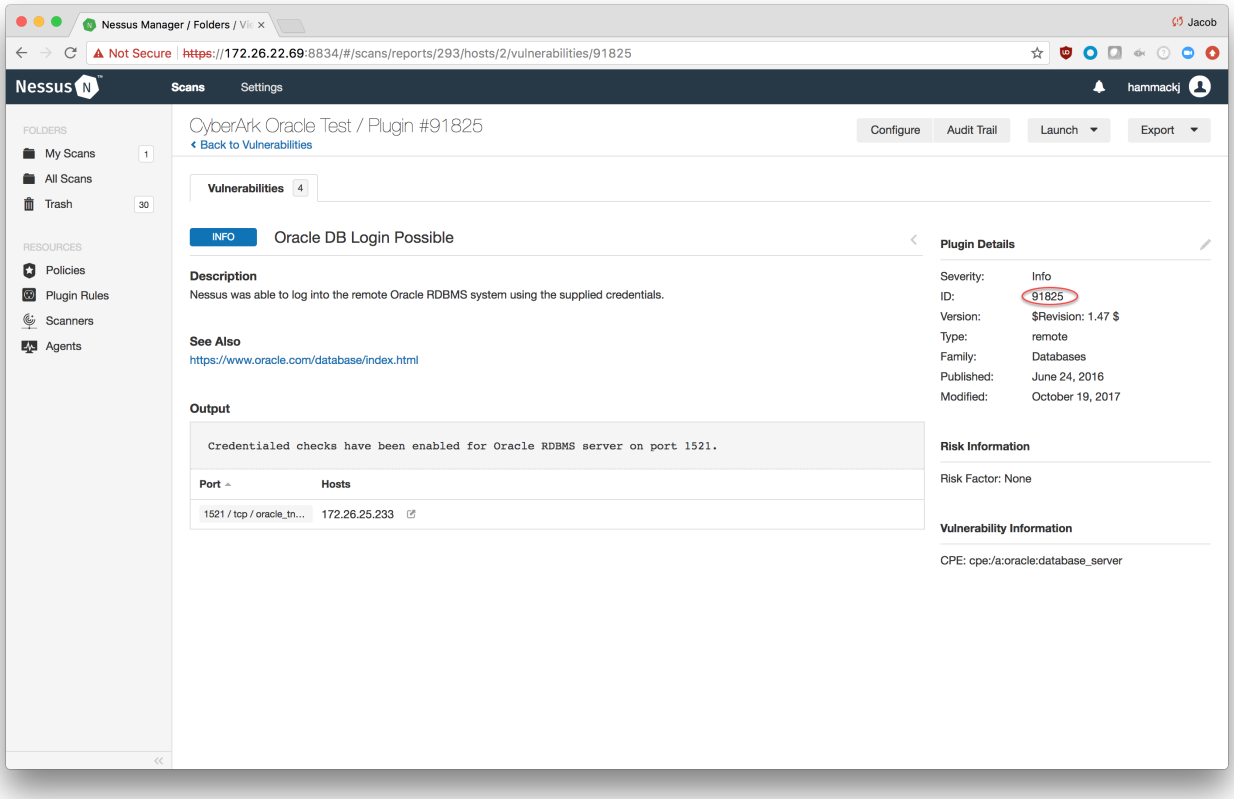
Verification

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



2. Once the scan has completed, select the completed scan. Look for the corresponding **ID** (see chart below), 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 (Legacy) Credentials

Caution: Support for SOAP requests are no longer be supported by CyberArk as of December 31, 2024. If you are using the CyberArk Legacy Integration which utilizes SOAP for API requests, Tenable recommends using our non-Legacy CyberArk Integration which supports REST API requests.

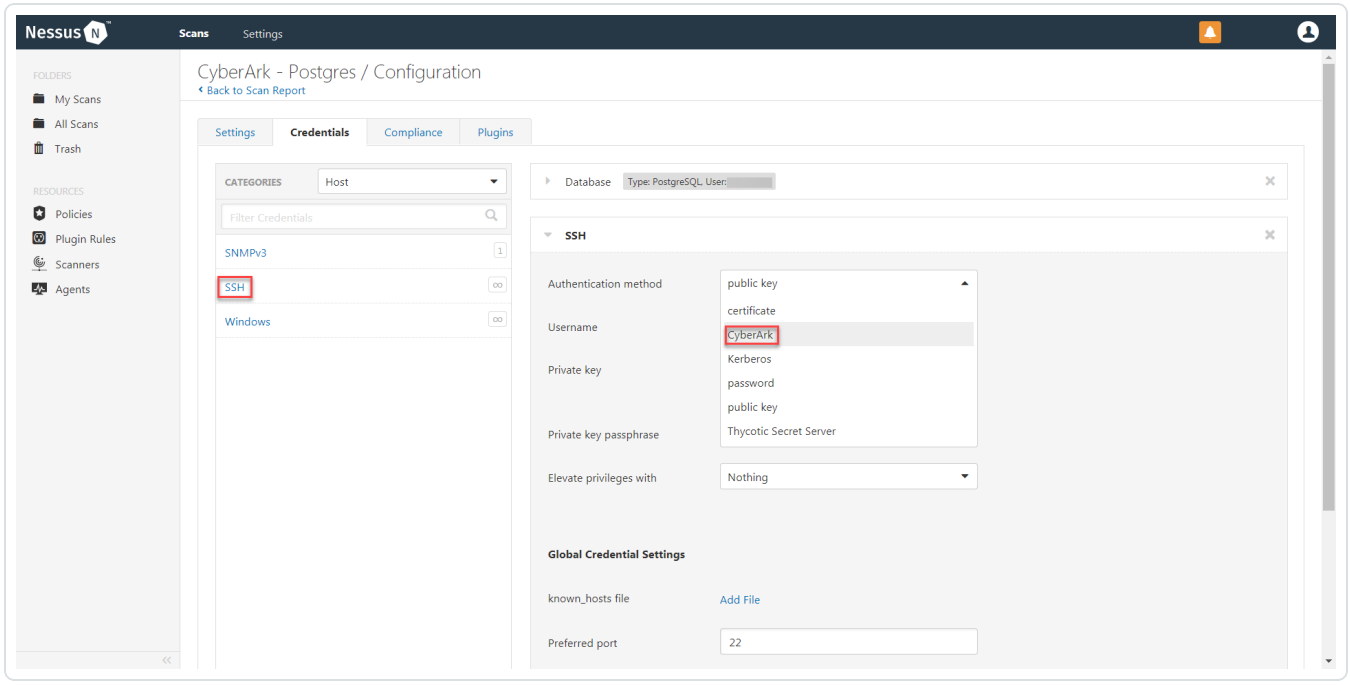
Tenable Nessus Manager supports the use of privilege escalation, such as *su* and *sudo*, when using SSH through the CyberArk authentication method.

Requirements:

- CyberArk account
- Nessus Manager account

To configure SSH integration:

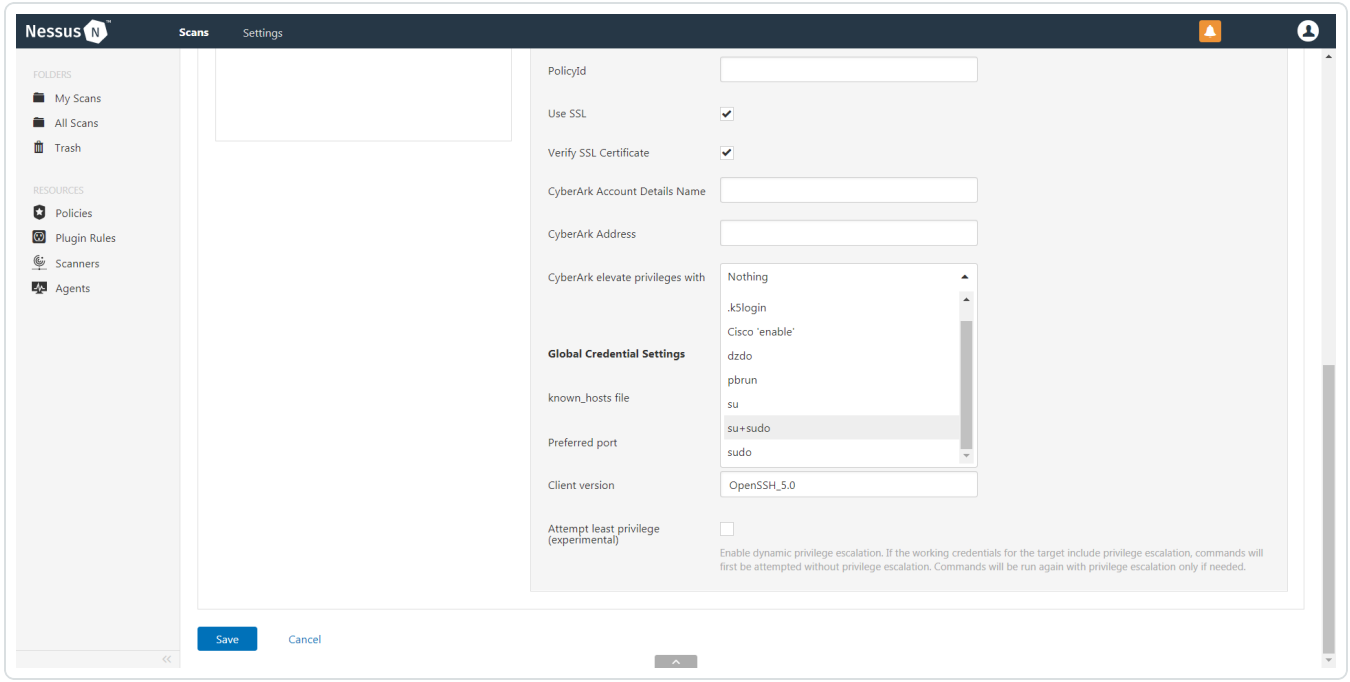
1. Select **SSH** as the **Type** and CyberArk as the **Authentication Method.**



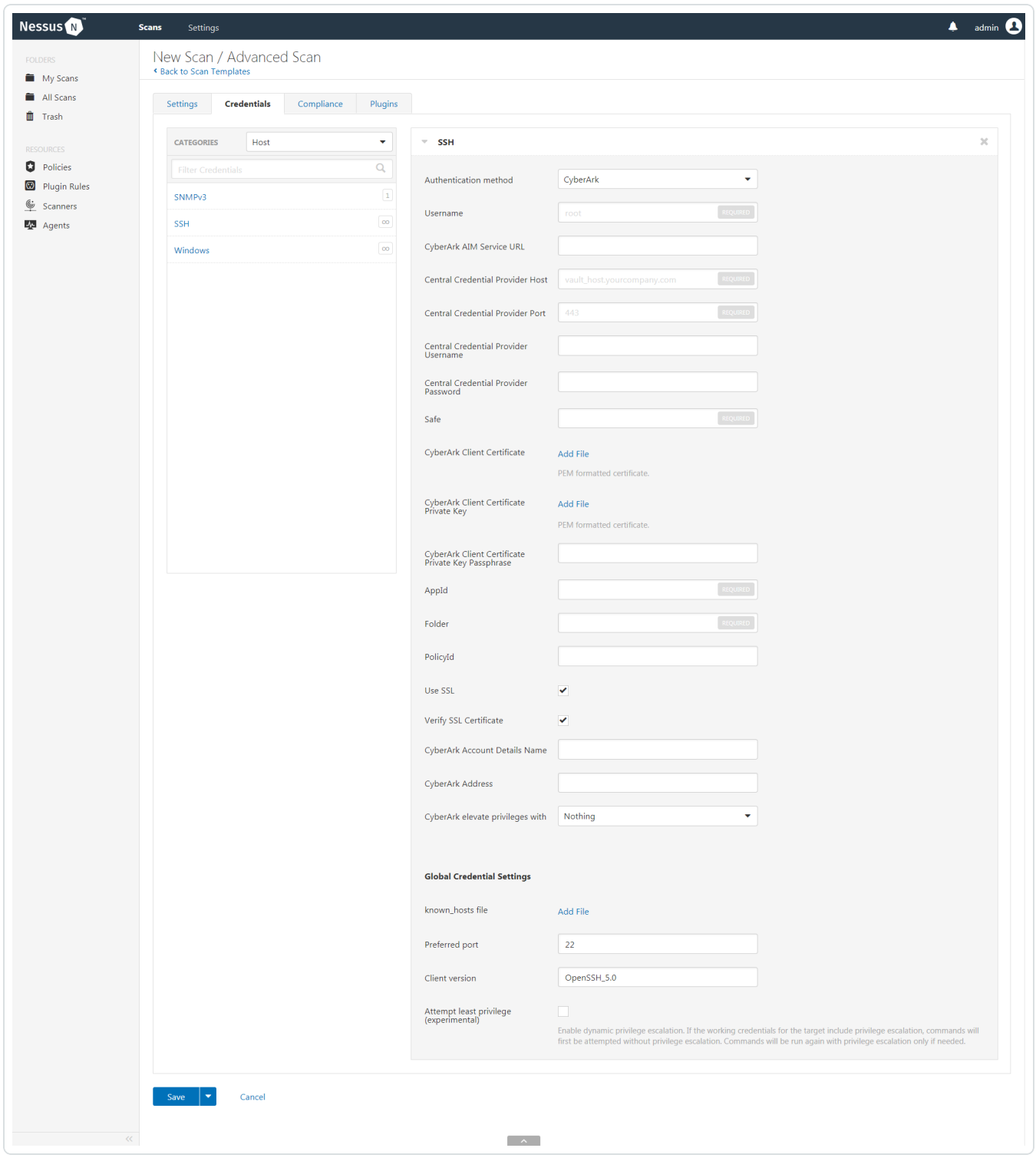
2. An option for **CyberArk elevate privileges with** appears near the bottom of the configuration page.

> **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 **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 Nessus User Guide.



3. Configure each field for SSH authentication. See the Nessus User Guide to get detailed descriptions for each option.



4. Click **Save**.

Windows (Legacy) Integration

Caution: Support for SOAP requests are no longer be supported by CyberArk as of December 31, 2024. If you are using the CyberArk Legacy Integration which utilizes SOAP for API requests, Tenable recommends using our non-Legacy CyberArk Integration which supports REST API requests.

Tenable Nessus Manager provides an option for CyberArk Windows integration. Complete the following steps to configure Tenable Nessus Manager with CyberArk for Windows.

Requirements:

- CyberArk account
- Nessus Manager account

To configure Windows integration:

1. Log in to Nessus.
2. Click **Scans**.
3. Click **+ New Scans**.

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

   The selected scan template 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** options appear.
9. In the left-hand menu, select **Windows**.
10. Click **Authentication method**.

    A drop-down appears.
11. Select **CyberArk**.

    Configure each field for **Windows** authentication.
12. (missing or bad snippet)

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

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. Look for the corresponding **ID** (see chart below), which validates that authentication was successful. If the authentication is not successful, refer to the Debugging CyberArk Issues section of this document.

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.

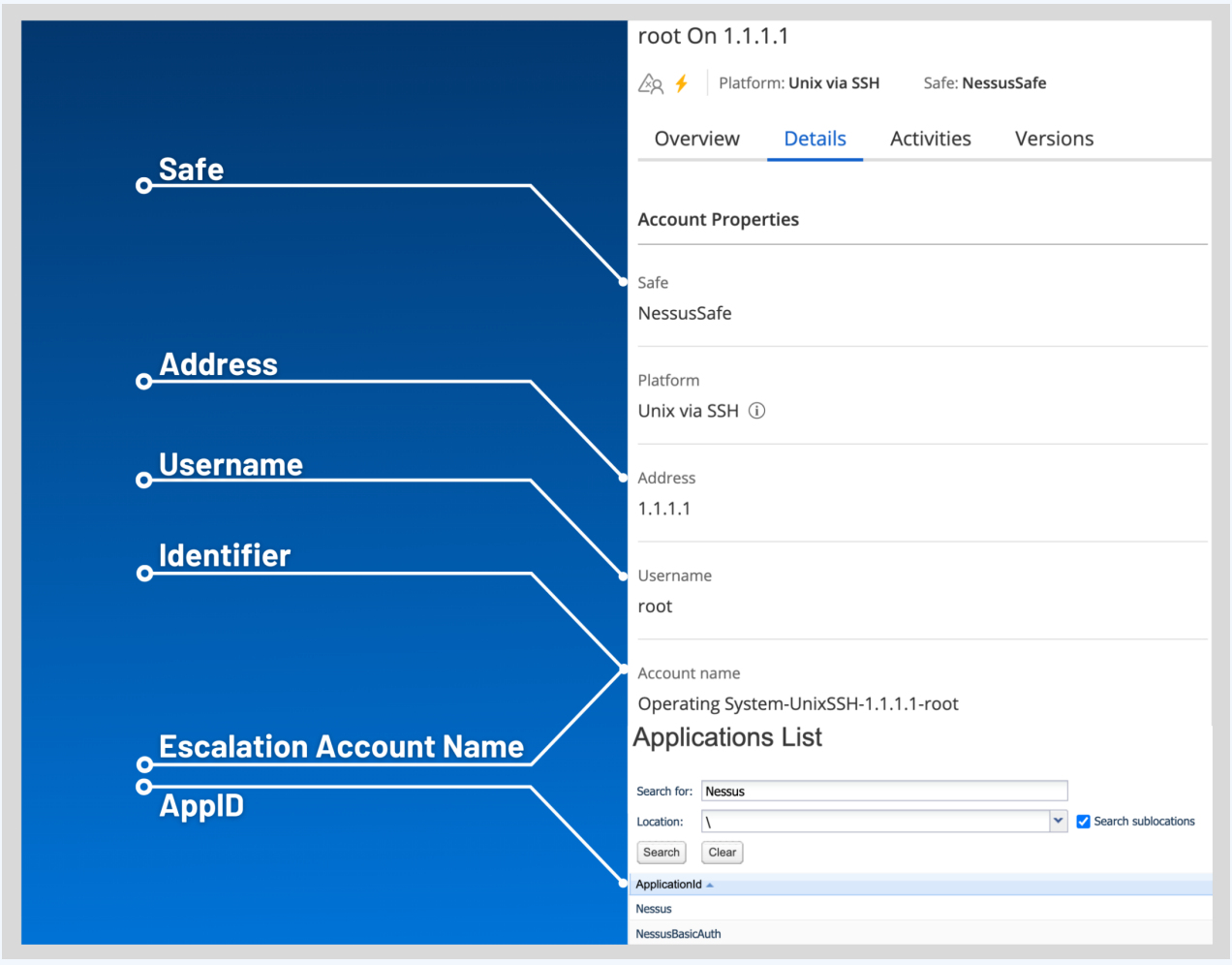
9. Configure each field for the **Oracle Database** authentication.

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	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. **Note:** Customers self-hosting CyberArk CCP on a Windows Server 2022 and above should follow the guidance found in Tenable's Community post about CyberArk Client Certification Authentication Issue.	no
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	Yes, if the private key is applied.
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	Yes, if the private key is applied.
Get credential by	The method with which your CyberArk API credentials are retrieved. Can be **Username**, **Identifier**, or **Address**. The method with which your CyberArk API credentials are retrieved. Can be **Username**,	yes

Option	Description	Required
	Identifier, **Address**, or **Parameters**. **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.	
Account Name	(If **Get credential by** is **Identifier**) The unique account name or identifier assigned to the CyberArk API credential.	no
Address	(If **Get credential by** is **Address** or **Parameters**) The address unique to the CyberArk API credential.	no
Username	(If **Get credential by** is **Username** or **Parameters**) The username of the CyberArk user to request a password from.	no
Safe	The CyberArk safe the credential should be retrieved from.	no
Use Target IP Address	(If **Get credential by** is **Parameters**) When enabled, the integration appends the target address to the credential query, which limits the query to accounts matching the scan target's address. This is ignored if **Address** is set.	no
Folder	(If **Get credential by** is **Parameters**) The folder of the credential.	no
Database	(If **Get credential by** is **Parameters**) The database of the credential.	no
Query	(If **Get credential by** is **Parameters**) Specify a custom "free query" using account properties. When this method is specified, all other search criteria are	no

Option	Description	Required
	ignored.	
Query Format	(If **Get credential by** is **Parameters**) Defines the query format. Allowed values are **Exact** and **Regexp**. The default is **Exact**. This value is ignored unless the **Query** option was specified.	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:



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.

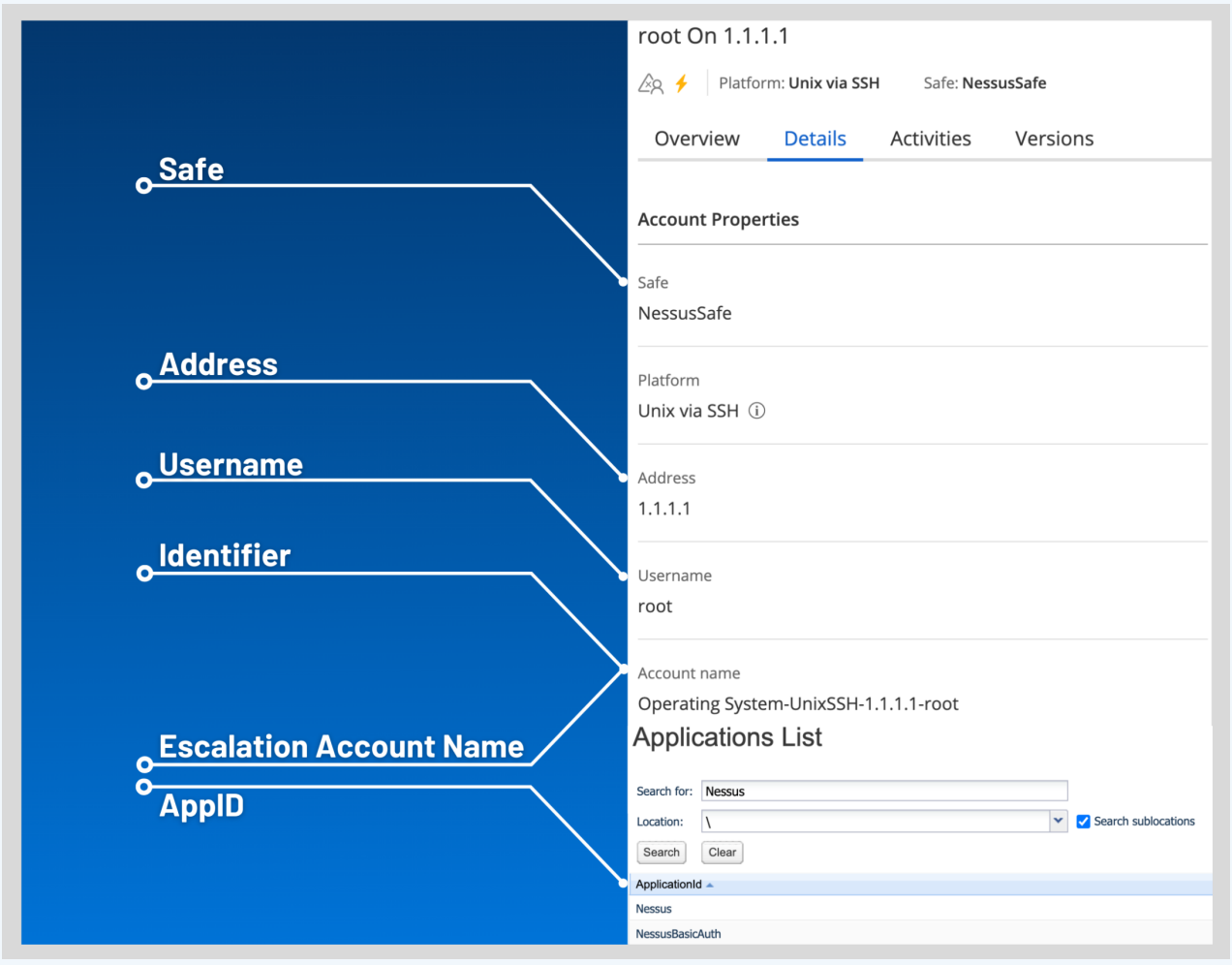
Option	Description	Required
CyberArk Elevate Privileges With	The privilege escalation method you want to use to increase users' privileges after initial authentication. Your **CyberArk Elevate Privileges With** selection determines the specific options you must configure. For more information, see Privilege Escalation.	no
Get credential by	The method with which your CyberArk API credentials are retrieved. Can be **Username**, **Identifier**, or **Address**. The method with which your CyberArk API credentials are retrieved. Can be **Username**, **Identifier**, **Address**, or **Parameters**. **Note:** The frequency of queries for **Username** is one query per target. The frequency of	yes

Option	Description	Required
	queries for **Identifier** is one query per chunk. This feature requires all targets have the same identifier.	
Account Name	(If **Get credential by** is **Identifier**) The unique account name or identifier assigned to the CyberArk API credential.	no
Address	(If **Get credential by** is **Address** or **Parameters**) The address unique to the CyberArk API credential.	no
Username	(If **Get credential by** is **Username** or **Parameters**) The username of the CyberArk user to request a password from.	no
Safe	The CyberArk safe the credential should be retrieved from.	no
Use Target IP Address	(If **Get credential by** is **Parameters**) When enabled, the integration appends the target address to the credential query, which limits the query to accounts matching the scan target's address. This is ignored if **Address** is set.	no
Folder	(If **Get credential by** is **Parameters**) The folder of the credential.	no
Database	(If **Get credential by** is **Parameters**) The database of the credential.	no
Query	(If **Get credential by** is **Parameters**) Specify a custom "free query" using account properties. When this method is specified, all other search criteria are ignored.	no

Option	Description	Required
Query Format	(If **Get credential by** is **Parameters**) Defines the query format. Allowed values are **Exact** and **Regexp**. The default is **Exact**. This value is ignored unless the **Query** option was specified.	no
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. **Note:** Customers self-hosting CyberArk CCP on a Windows Server 2022 and above should follow the guidance found in Tenable's Community post about CyberArk Client Certification Authentication Issue.	no
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	Yes, if the private key is applied.
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	Yes, if private key is applied.
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for	yes

Option	Description	Required
	the user.	
KDC Port	(Required if Kerberos Target Authentication is enabled.) The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	yes
KDC Transport	(Required if Kerberos Target Authentication is enabled.) The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	yes
Realm	(Required if Kerberos Target Authentication is enabled) The Realm is the authentication domain, usually noted as the domain name of the target (for example, example.com). By default, CyberArkTenable Security Center uses 443.	yes
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:



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.

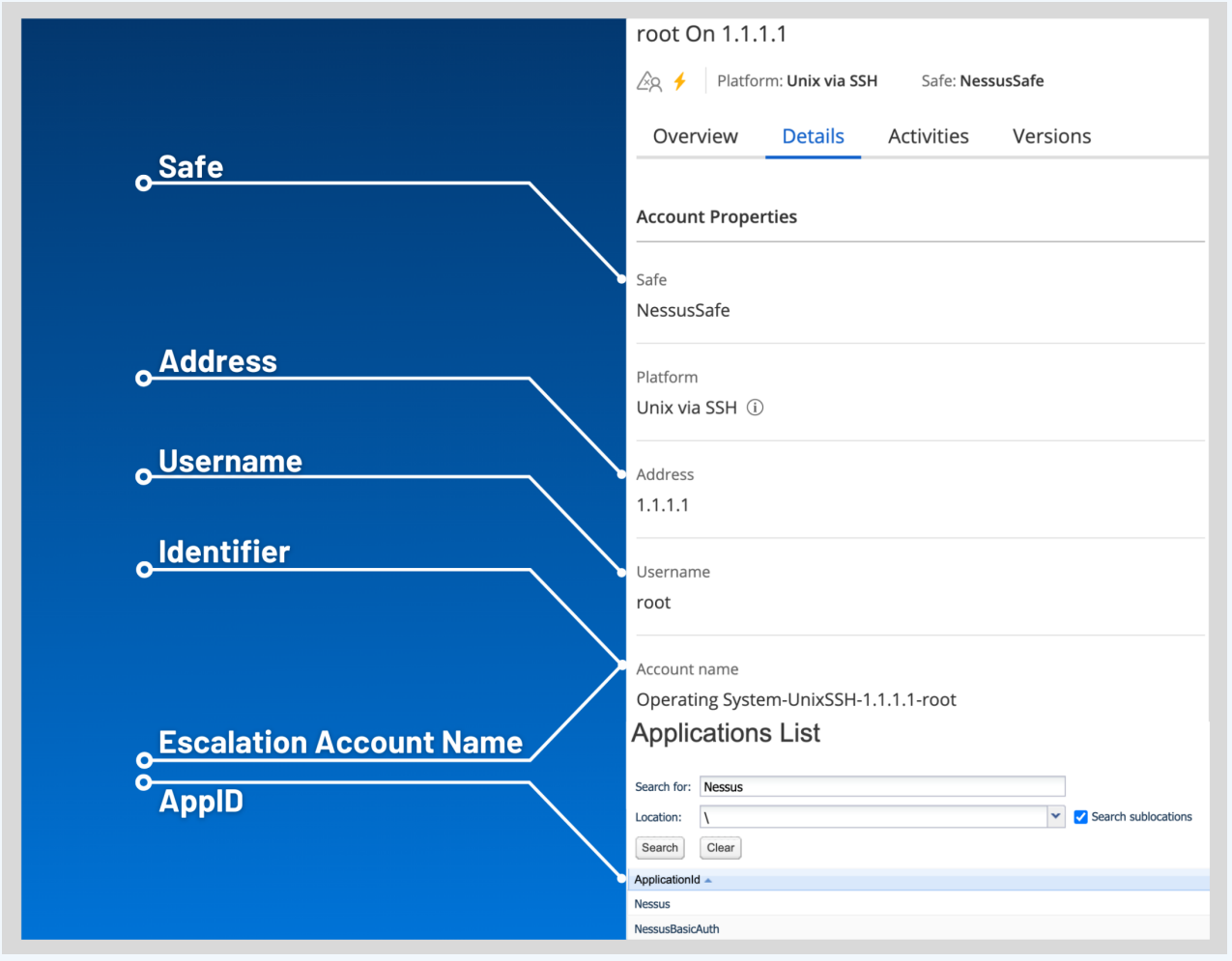
Option	Description	Required
CyberArk Host	The IP address or FQDN name for the CyberArk AIM Web Service.	yes
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443.	yes
AppID	The Application ID associated with the CyberArk API connection.	yes
Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host. **Note:** Customers self-hosting CyberArk CCP on a Windows Server 2022 and above should follow the guidance found in Tenable's Community post about CyberArk Client Certification Authentication Issue.	no
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	Yes, if the private key is applied.
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	Yes, if the private key is applied.
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	(Required if Kerberos Target Authentication is	yes

Option	Description	Required
	enabled.) The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	
KDC Transport	(Required if Kerberos Target Authentication is enabled.) The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	yes
Domain	(Required if Kerberos Target Authentication is enabled) The domain to which Kerberos Target Authentication belongs, if applicable.	yes
Get credential by	The method with which your CyberArk API credentials are retrieved. Can be **Username**, **Identifier**, or **Address**. The method with which your CyberArk API credentials are retrieved. Can be **Username**, **Identifier**, **Address**, or **Parameters**. **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.	yes
Account Name	(If **Get credential by** is **Identifier**) The unique account name or identifier assigned to the CyberArk API credential.	no
Address	(If **Get credential by** is **Address** or **Parameters**)	no

Option	Description	Required
	The address unique to the CyberArk API credential.	
Username	(If **Get credential by** is **Username** or **Parameters**) The username of the CyberArk user to request a password from.	no
Safe	The CyberArk safe the credential should be retrieved from.	no
Use Target IP Address	(If **Get credential by** is **Parameters**) When enabled, the integration appends the target address to the credential query, which limits the query to accounts matching the scan target's address. This is ignored if **Address** is set.	no
Folder	(If **Get credential by** is **Parameters**) The folder of the credential.	no
Database	(If **Get credential by** is **Parameters**) The database of the credential.	no
Query	(If **Get credential by** is **Parameters**) Specify a custom "free query" using account properties. When this method is specified, all other search criteria are ignored.	no
Query Format	(If **Get credential by** is **Parameters**) Defines the query format. Allowed values are **Exact** and **Regexp**. The default is **Exact**. This value is ignored unless the **Query** option was specified.	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	no

Option	Description	Required
	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

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



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**.

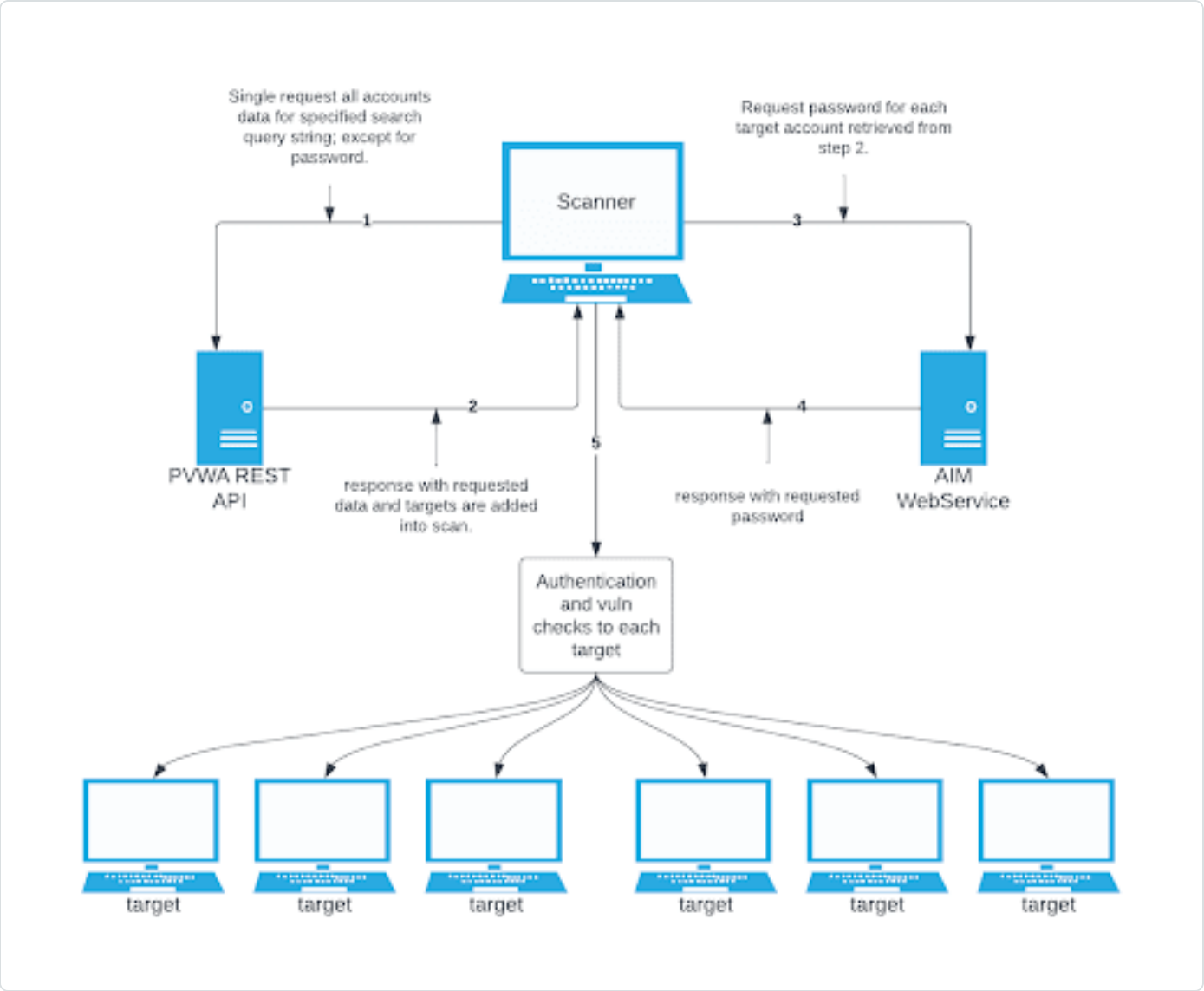
8. Next, follow the steps for Add the Credential to the Scan.

CyberArk 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.

Caution: Tenable recommends utilizing scanner groups with one scanner when using Auto-Discovery credentials and users should only enter only a single initial host in the scan. If multiple scanners are used in an Auto-Discovery scan, targets retrieved from the integration may be scanned multiple times.



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.

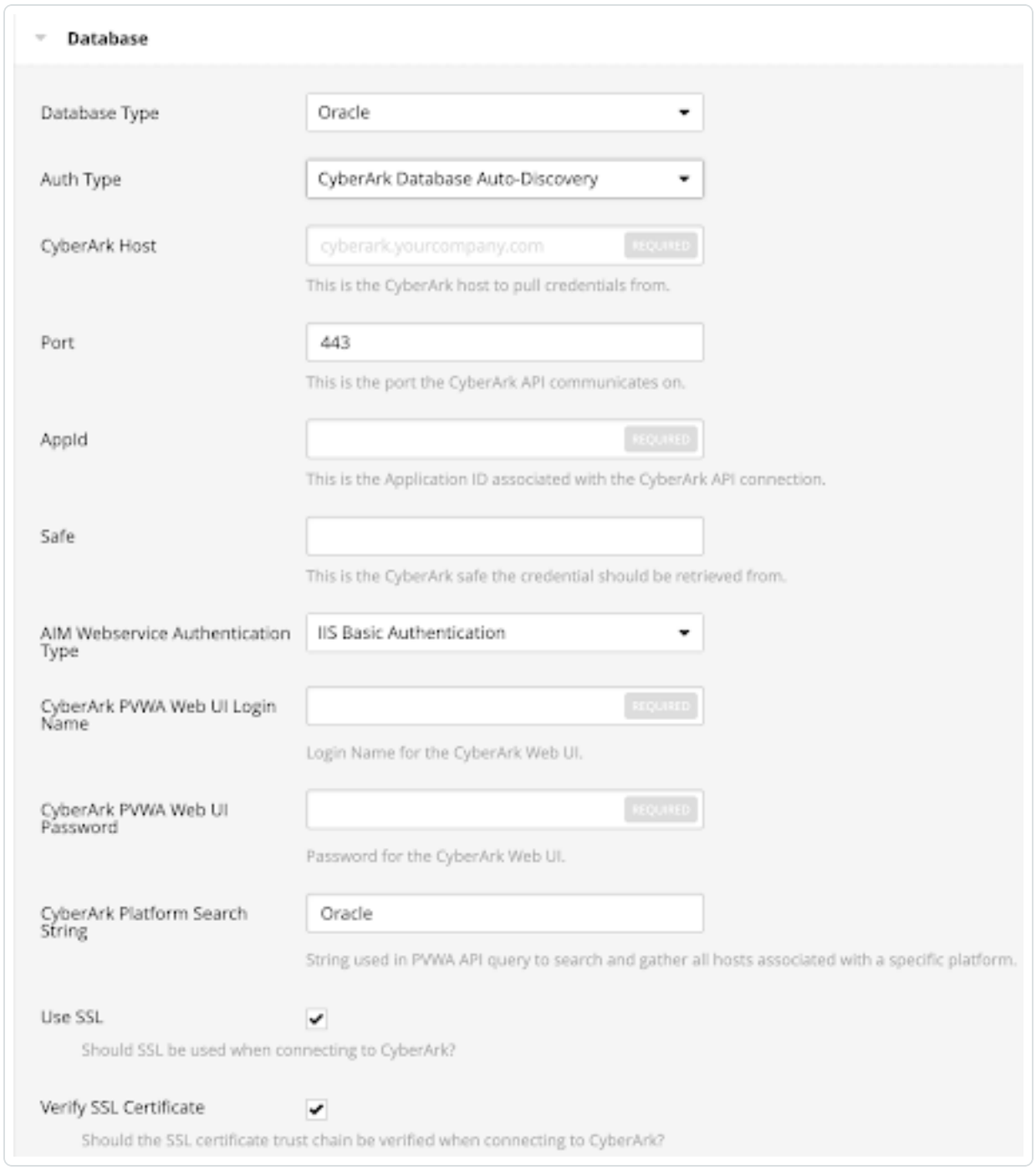
9. Click the **Database** option.

   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:



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
	Note: Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	yes
CCP Host	The IP address or FQDN name for the user's CyberArk CCP component. (Not available with Tenable Security Center.) **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the CCP host.	no
CCP Port	The port on which the CyberArk CCP (AIM Web Service) API communicates. By default, Tenable uses 443. (Not available with Tenable Security Center.) **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the CCP host.	no
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

Option	Description	Required
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
PVWA REST API Authentication Method	Choose whether to authenticate to the PVWA by entering username and password or to gather credentials from the Central Credential Provider (CCP). (**Not available with Tenable Security Center.**)	yes
PVWA REST API Credential ID	The unique identifier ("Account name") of the CyberArk account containing CCP credentials. (**Not available with Tenable Security Center.**)	Yes, if the PVWA REST API Authentication Method is set to **Gather from CCP**.
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	yes

Option	Description	Required
	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.	
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.

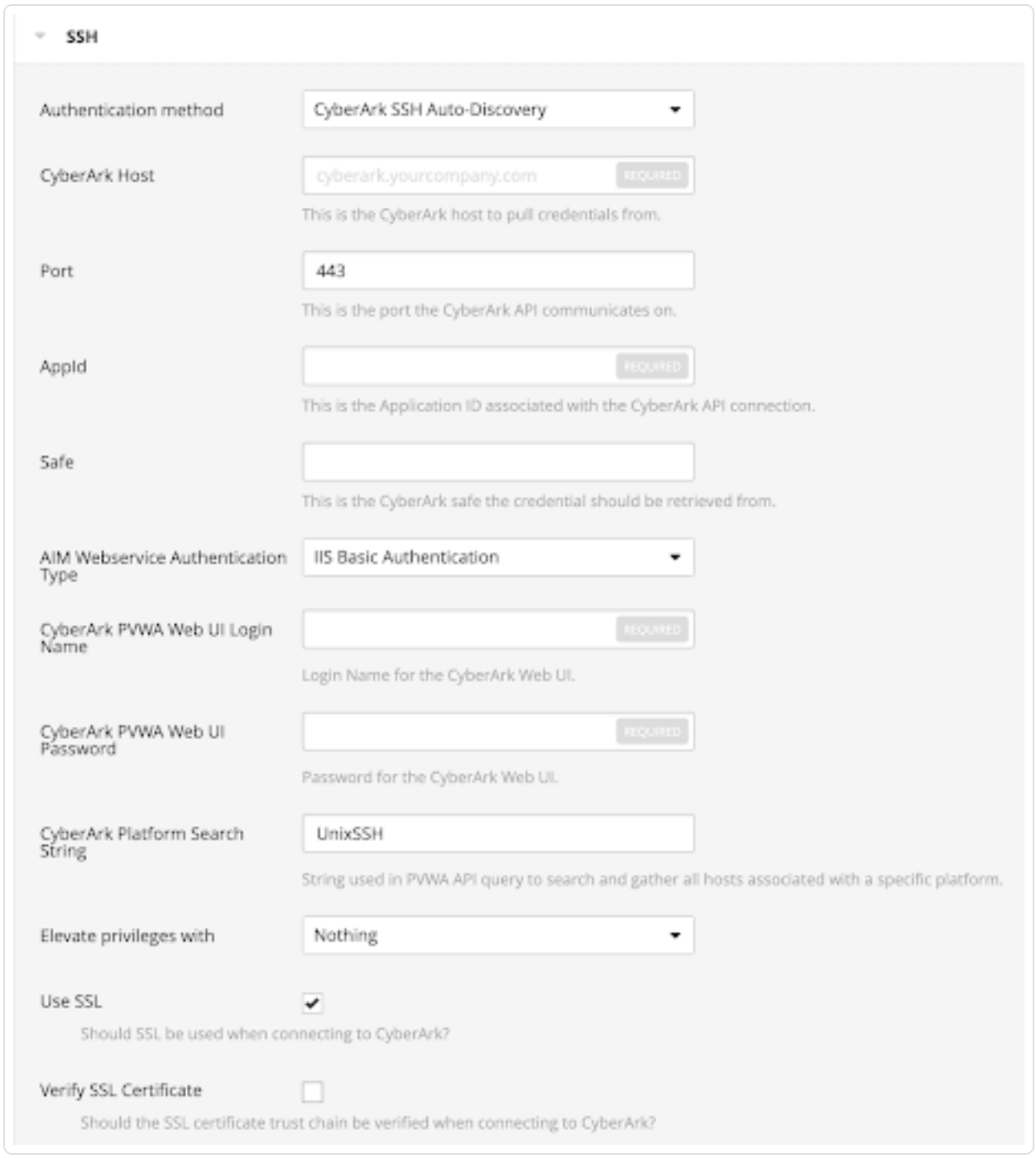
   The **Credentials** pane appears.

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:



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
	Note: Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	yes
CCP Host	The IP address or FQDN name for the user's CyberArk CCP component. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	no
CCP Port	The port on which the CyberArk CCP (AIM Web Service) API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	no
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**	yes

Option	Description	Required
	Authentication and **Certificate Authentication**. Certificate Authentication can be either encrypted or unencrypted.	
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
PVWA REST API Authentication Method	Choose whether to authenticate to the PVWA by entering username and password or to gather credentials from the Central Credential Provider (CCP). (**Not available with Tenable Security Center.**)	yes
PVWA REST API Credential ID	The unique identifier ("Account name") of the CyberArk account containing CCP credentials. (**Not available with Tenable**	Yes, if the PVWA REST API Authentication

Option	Description	Required
	Security Center.)	Method is set to **Gather from CCP**.
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
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	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.

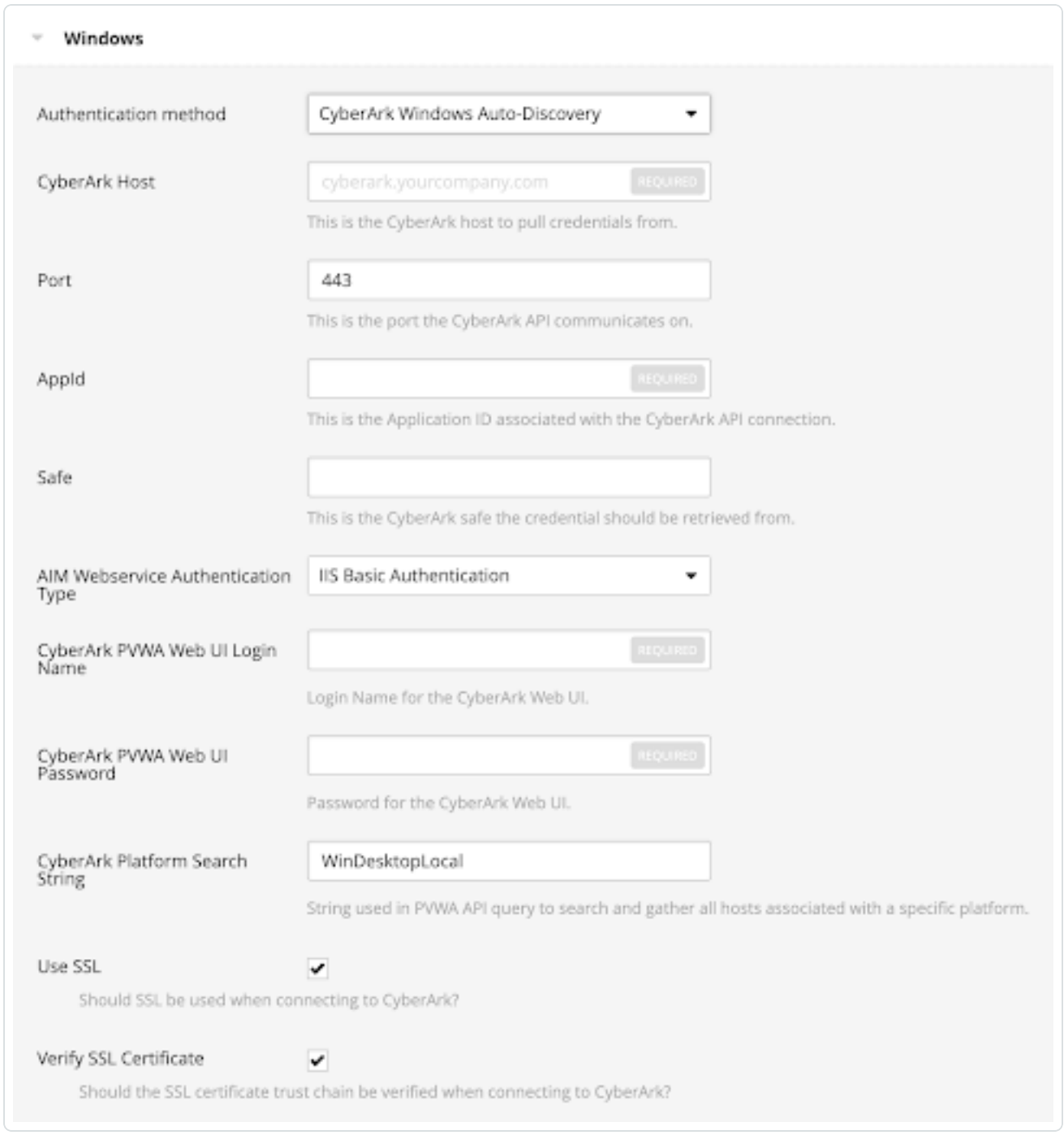
The **Host** options appear.

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:



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

Option	Description	Required
	Note: Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	yes
CCP Host	The IP address or FQDN name for the user's CyberArk CCP component. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	no
CCP Port	The port on which the CyberArk CCP (AIM Web Service) API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	no
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**	yes

Option	Description	Required
	Authentication and **Certificate Authentication**. Certificate Authentication can be either encrypted or unencrypted.	
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 practice would be to create a custom platform name in CyberArk and enter that value in this field to improve accuracy.	yes
PVWA REST API Authentication Method	Choose whether to authenticate to the PVWA by entering username and password or to gather credentials from the Central Credential Provider (CCP). (**Not available with Tenable Security Center.**)	yes
PVWA REST API Credential ID	The unique identifier ("Account name") of the CyberArk account containing CCP credentials. (**Not available with Tenable**	Yes, if the PVWA REST API Authentication

Option	Description	Required
	Security Center.)	Method is set to **Gather from CCP**.
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 (Legacy) Integration

Caution: Support for SOAP requests are no longer be supported by CyberArk as of December 31, 2024. If you are using the CyberArk Legacy Integration which utilizes SOAP for API requests, Tenable recommends using our non-Legacy CyberArk Integration which supports REST API requests.

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

Caution: Support for SOAP requests are no longer be supported by CyberArk as of December 31, 2024. If you are using the CyberArk Legacy Integration which utilizes SOAP for API requests, Tenable recommends using our non-Legacy CyberArk Integration which supports REST API requests.

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, Tenable uses `/AIMWebservice/v1.1/AIM.asmx`. **Note:** When the customer is using the default path, they can leave this blank.	no
Central Credential Provider Username	All	If the CyberArk Central Credential Provider (CCP) is configured to use basic authentication, you can fill in this field for authentication. **Note:** This field should be the Username to Authenticate to the AIM Web Service API.	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

Option	Database Types	Description	Required
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
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	All	The unique name of the credential	yes

Option	Database Types	Description	Required
Account Details Name		you want to retrieve from CyberArk.	
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
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	yes

Option	Database Types	Description	Required
		Oracle values include: Sybase ASE values include: • RSA • Plain Text	
Instance Name	SQL Server	The name for your database instance.	no
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

Caution: Support for SOAP requests are no longer be supported by CyberArk as of December 31, 2024. If you are using the CyberArk Legacy Integration which utilizes SOAP for API requests, Tenable recommends using our non-Legacy CyberArk Integration which supports REST API requests.

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, Tenable uses `/AIMWebservice/v1.1/AIM.asmx`. **Note:** When the customer is using the default path, they can leave this blank.	no
Central Credential Provider Host	The CyberArk Central Credential Provider IP/DNS address.	yes
Central Credential	The port on which the CyberArk Central Credential Provider is listening.	yes

Option	Description	Required
Provider Port		
Central Credential Provider Username	If the CyberArk Central Credential Provider (CCP) is configured to use basic authentication, you can fill in this field for authentication. **Note:** This field should be the Username to Authenticate to the AIM Web Service API.	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	yes

Option	Description	Required
	the target password.	
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
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 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

Caution: Support for SOAP requests are no longer be supported by CyberArk as of December 31, 2024. If you are using the CyberArk Legacy Integration which utilizes SOAP for API requests, Tenable recommends using our non-Legacy CyberArk Integration which supports REST API requests.

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 uses `/AIMWebservice/v1.1/AIM.asmx`. **Note:** When the customer is using the default path, they can leave this blank.	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
Central Credential Provider Username	If the CyberArk Central Credential Provider (CCP) is configured to use basic authentication, you can fill in this field for authentication. **Note:** This field should be the Username to Authenticate to the AIM Web Service API.	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

Option	Description	Required
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
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

Option	Description	Required
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 a Credential to a Scan

To add a credential to a 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**.

Database Integration

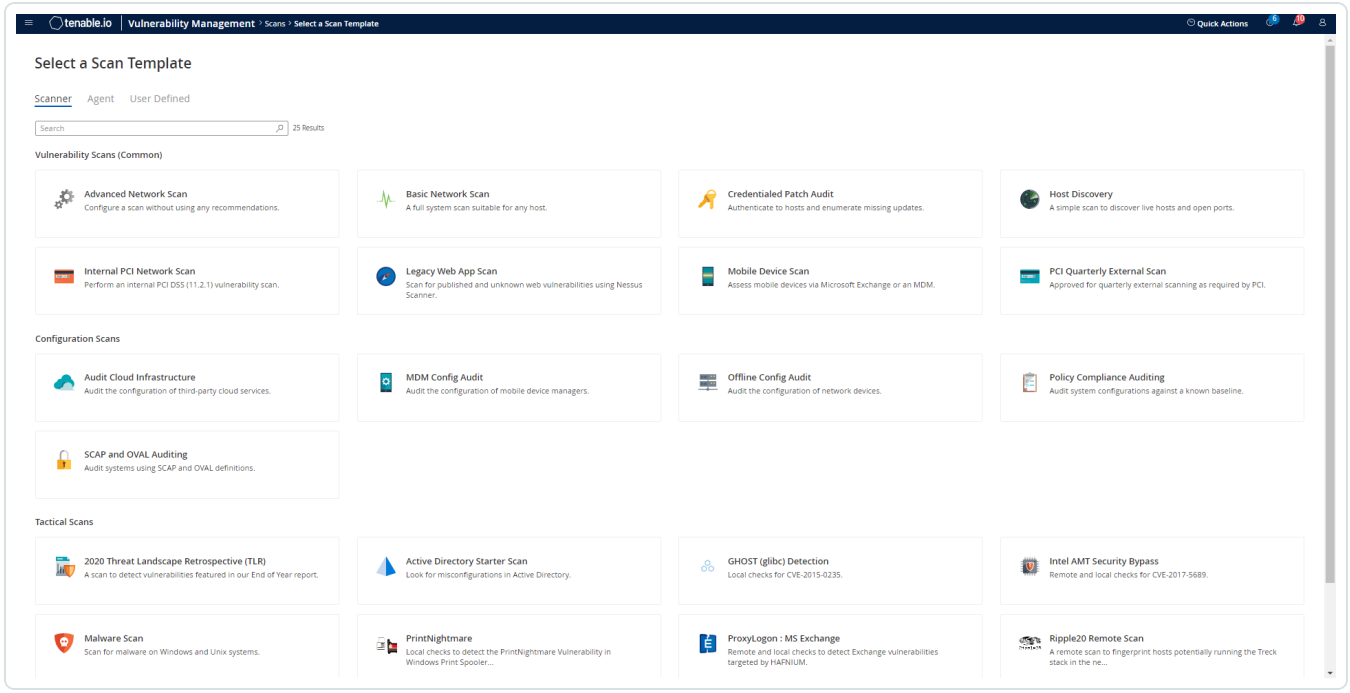
Required User Role: Standard, Scan Manager, or Administrator

To configure the database integration:

1. Log in to Tenable Vulnerability Management.
2. In the left navigation plane, click **Scans**.

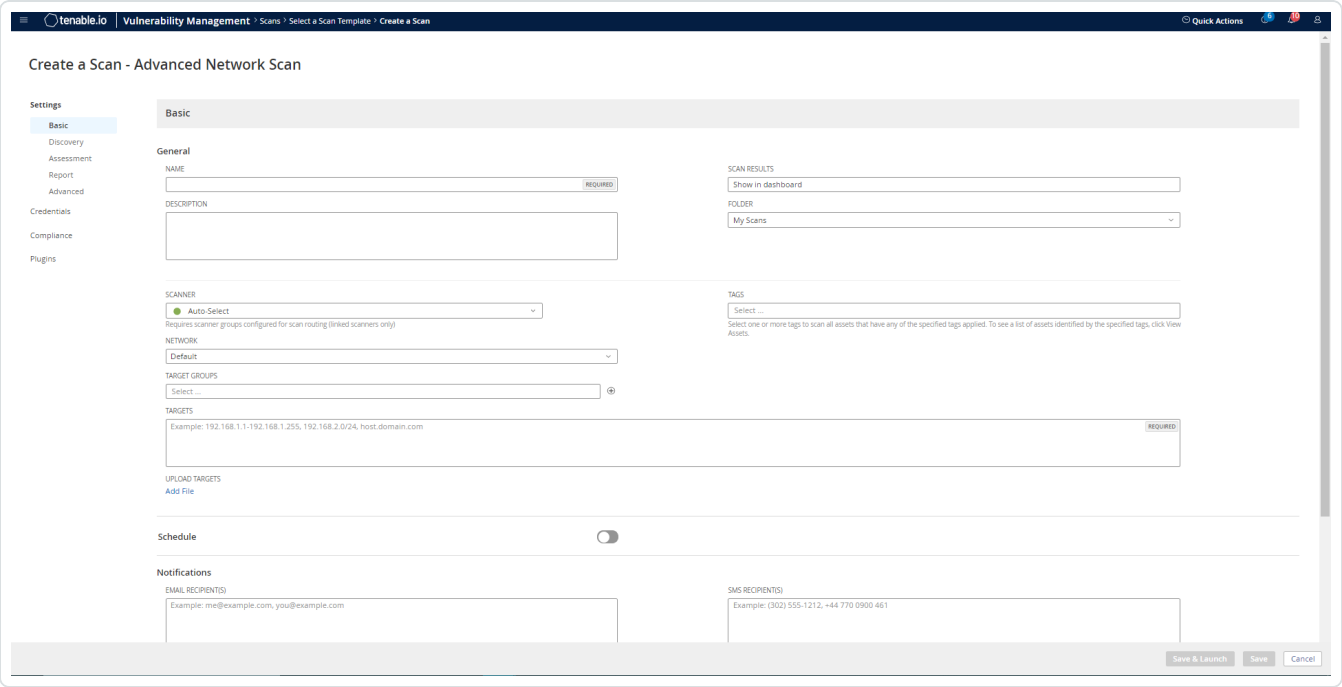
   The **Scans** page appears.
3. Click **+ New Scan.**

   The **Scan Templates** page appears.

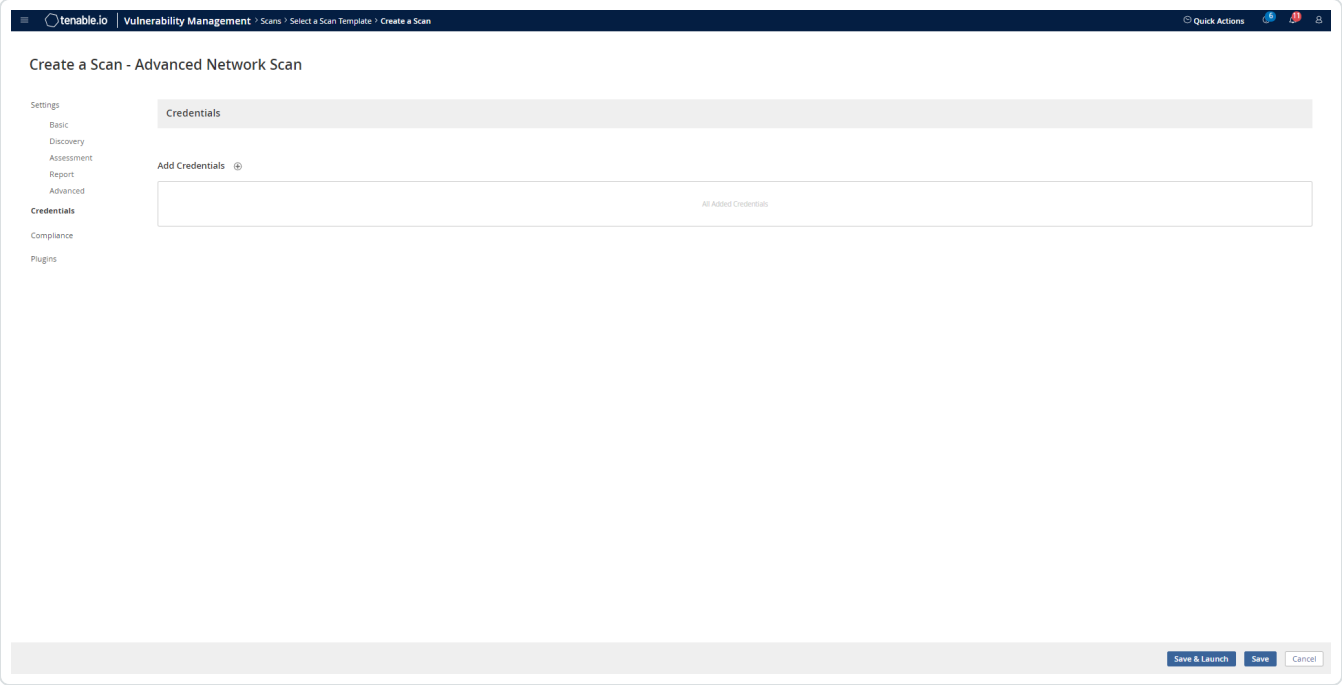


4. Select a **Scan Template**. For demonstration, the **Advanced Network Scan** template is used.

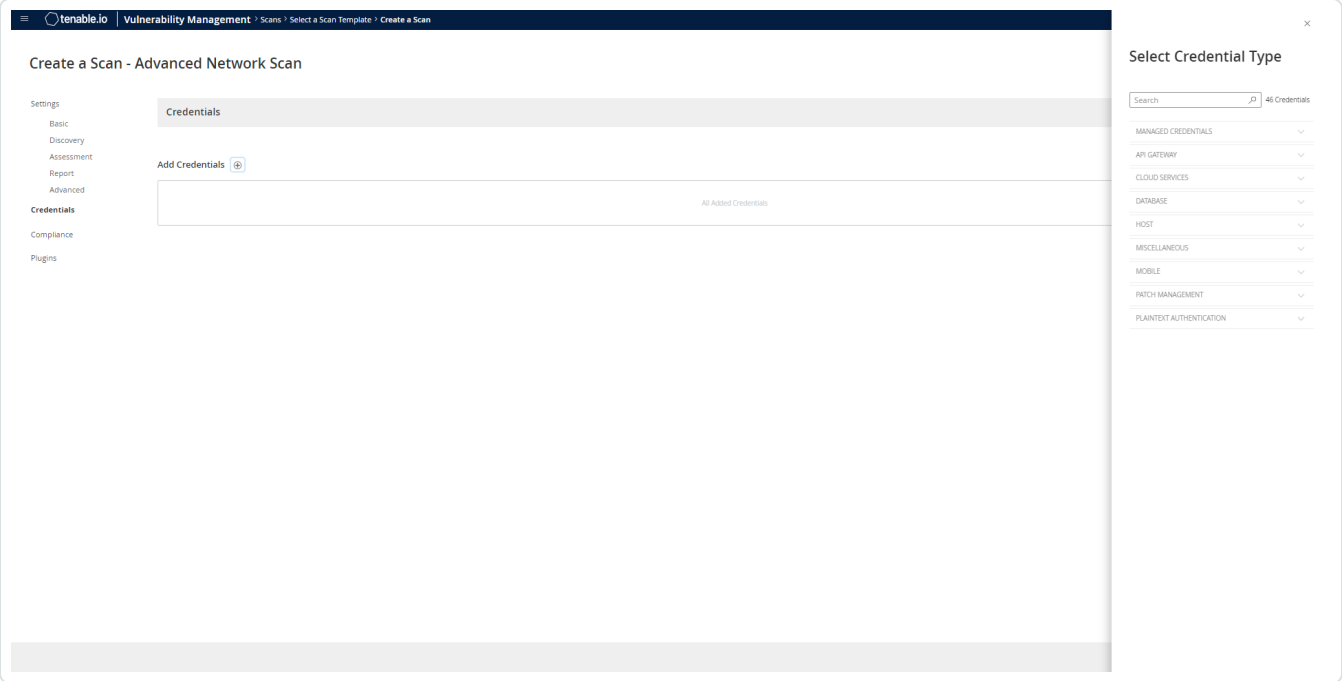
   The scan configuration page appears.



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.

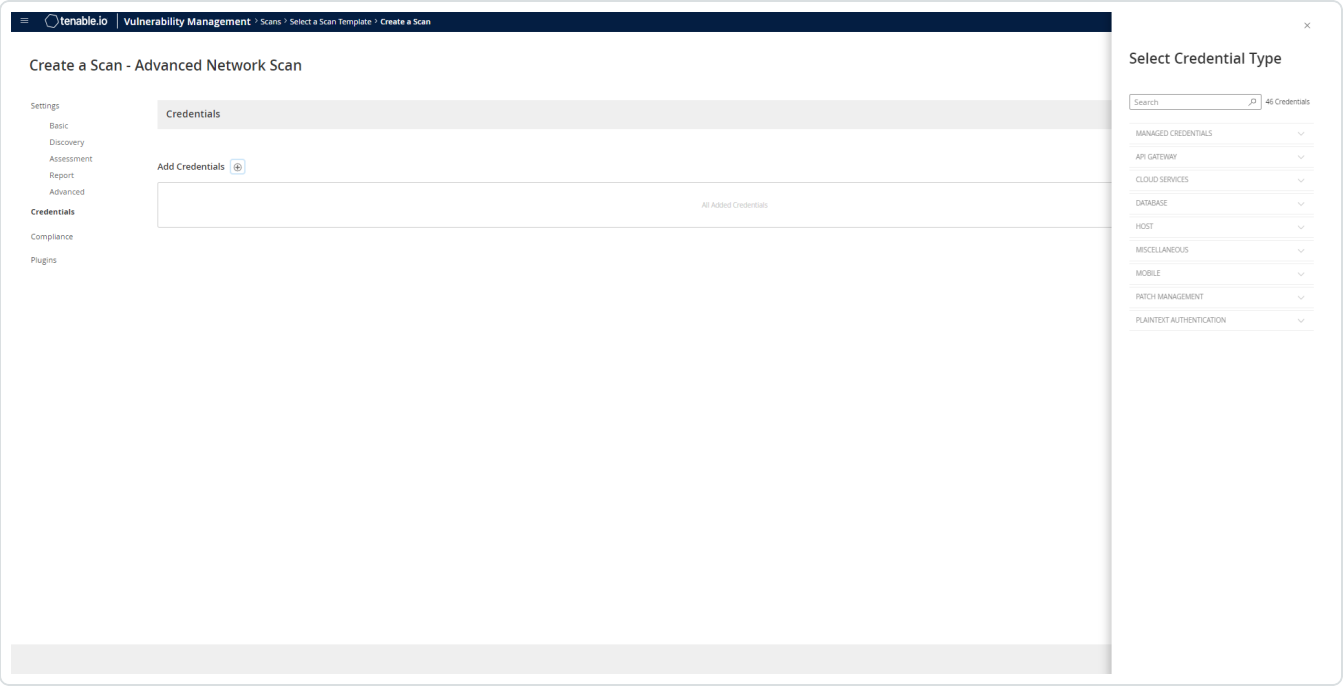


The **Credentials** pane appears.

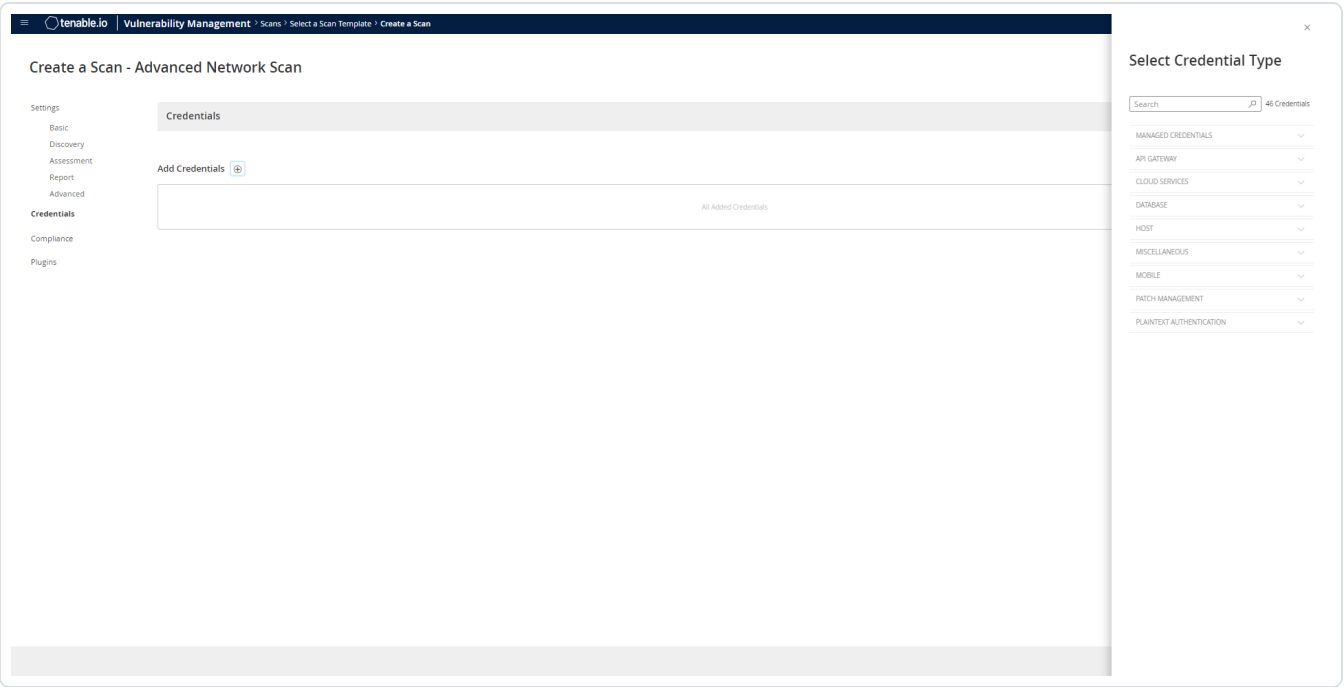


9. Click the **Database** option.

   The **Database** options appear.

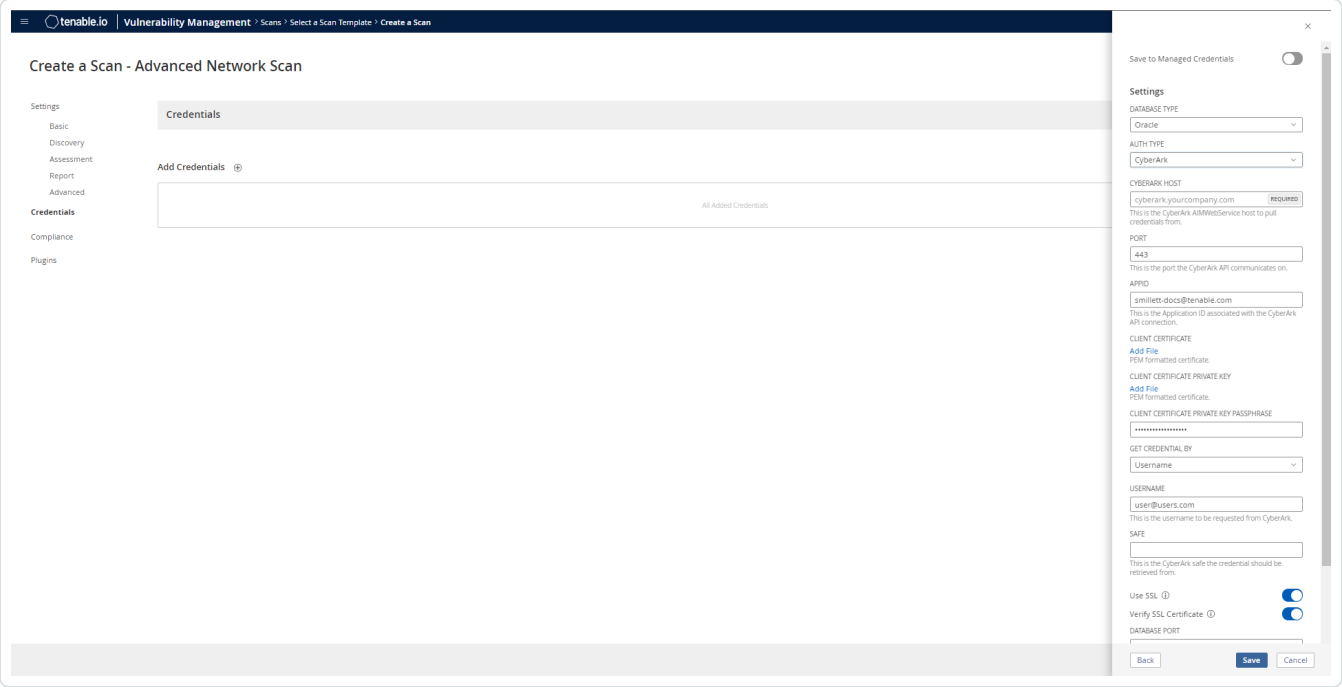


10. From the **Database Type** drop-down, select **Oracle**.



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

    The **CyberArk** field options appear.



12. Configure each field for the **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	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. **Note:** Customers self-hosting CyberArk CCP on a Windows Server 2022 and above should follow the guidance found in Tenable's Community post about CyberArk Client Certification Authentication Issue.	no

Option	Description	Required
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	Yes, if the 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 **Address**, **Identifier**, **Parameters**, or **Username**. **Note:** For more information about the **Parameters** option, refer to the **Parameters Options** table. **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.	yes
Username	(If **Get credential by** is set to **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

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

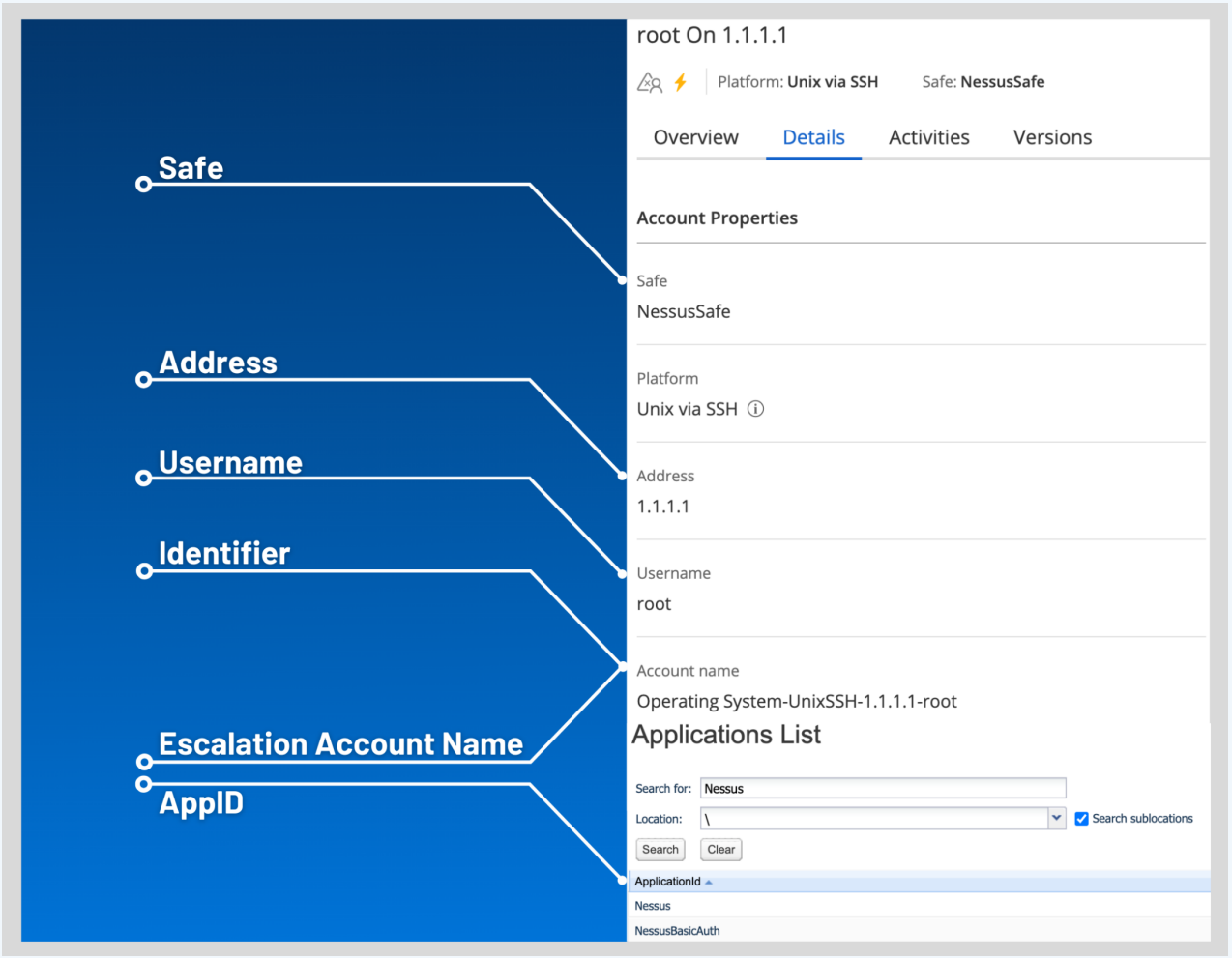
Parameters Options

The following options can be specified when **Get Credential By** is set to **Parameters**. These request parameters allow for advanced filtering of accounts based on their properties. The options correspond to the various options supported by the CyberArk REST API, as found in CyberArk documentation. These options can be specified in many different combinations to filter account results by their properties. For example, specifying **Root** as the **Folder** option results in a REST API query containing `&Folder=Root`.

Option	Description	Required
Safe	The safe containing the credential.	no
Address	Limit the query to accounts matching the specified address.	no
Use Target IP Address	(Optional) When enabled, the integration appends the target address to the credential query, which limits the query to accounts matching the scan target's address. This is ignored if **Address** is set.	no
Username	The username of the credential.	no
Account Name	The unique identifier assigned to the credential.	no
Folder	The folder of the credential.	no
Database	The database of the credential.	no
Query	Specify a custom "free query" using account properties. When this method is specified, all other	no

Option	Description	Required
	search criteria are ignored.	
Query Format	Defines the query format. allowed values are **Exact** and **Regexp**. The default is **Exact**. This value is ignored unless the **Query** option was specified.	no

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



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

13. Click **Save**.

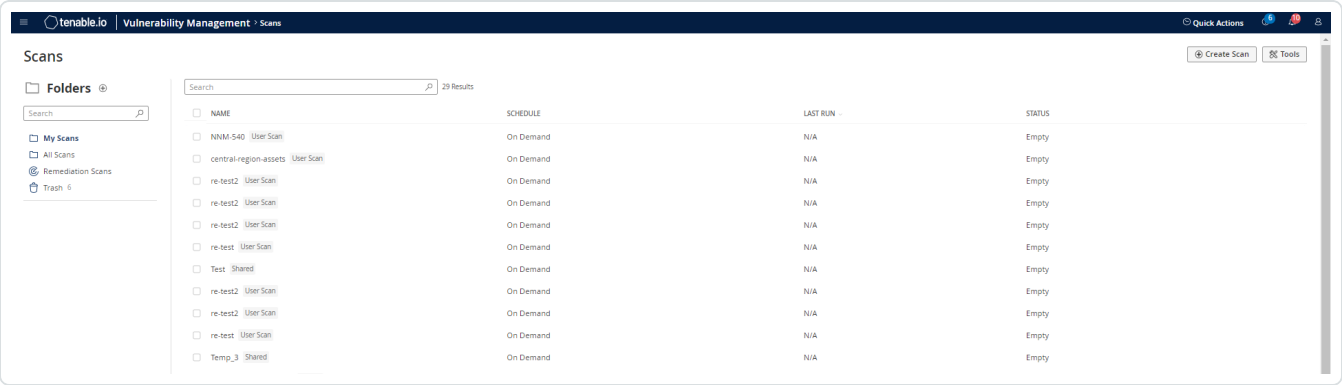
SSH Integration

Required User Role: Standard, Scan Manager, or Administrator

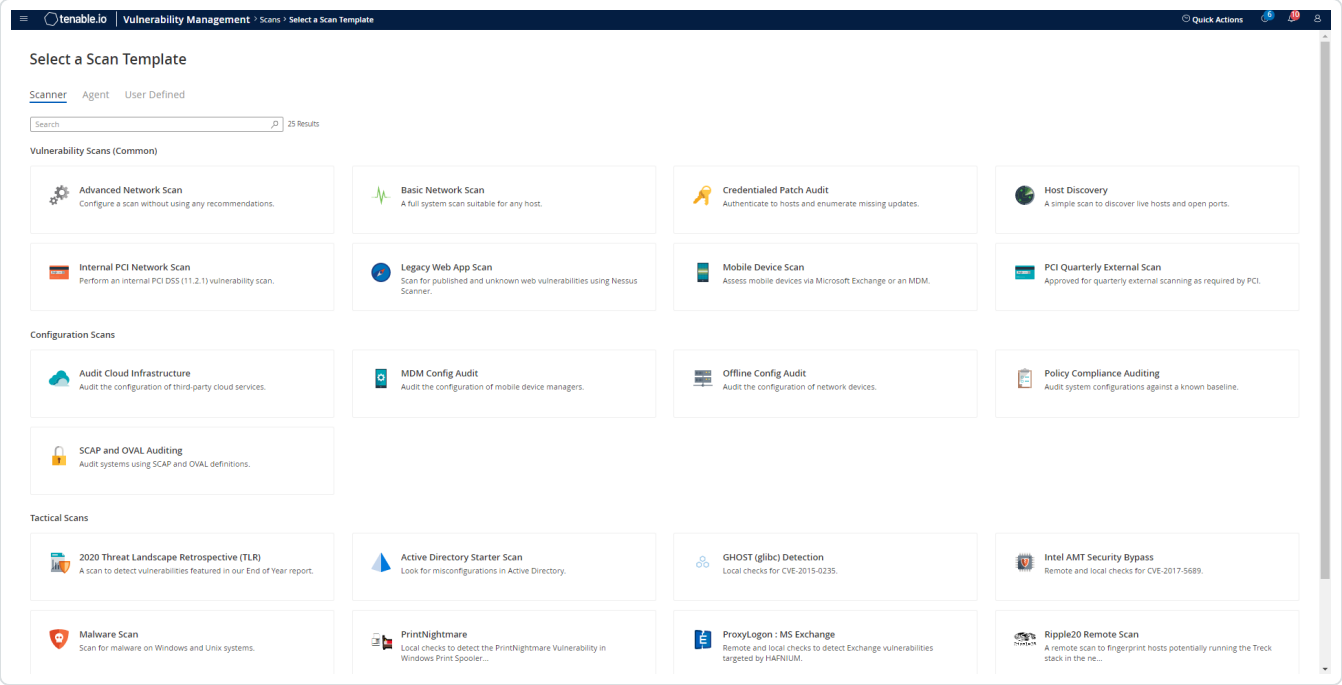
To configure SSH integration:

1. Log in to Tenable Vulnerability Management.
2. In the left navigation plane, click **Scans**.

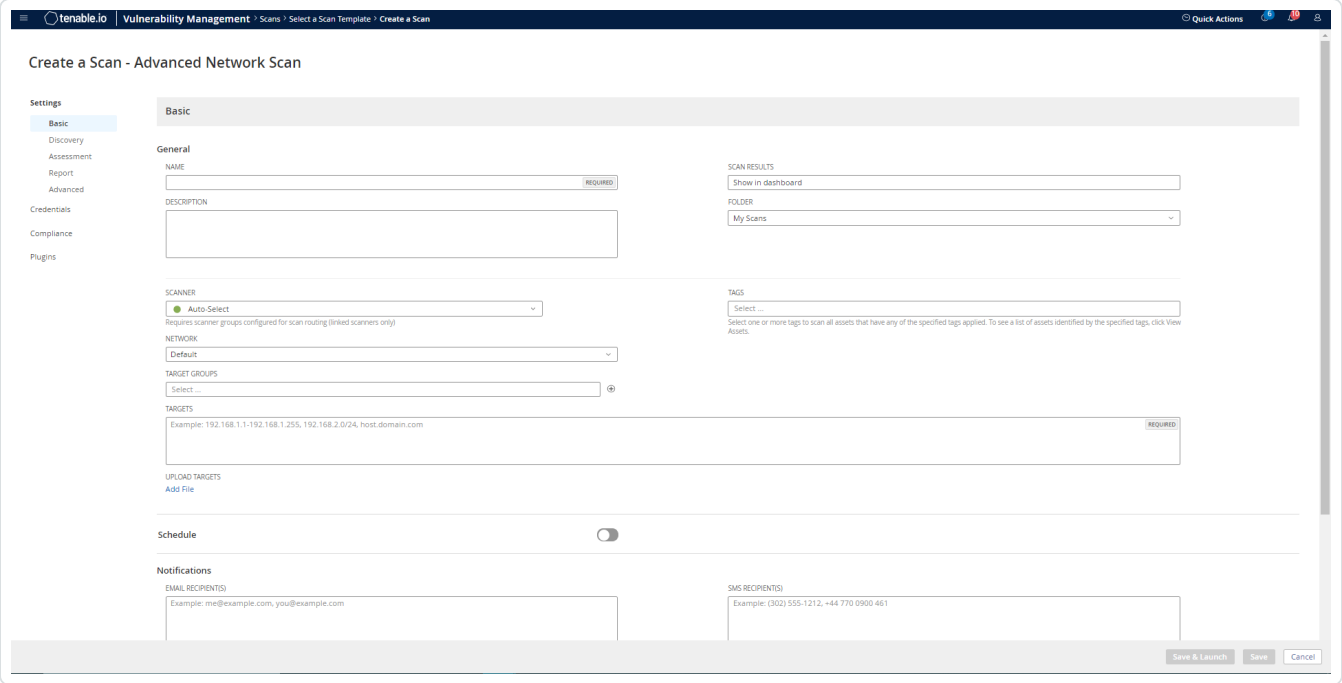
   The **Scans** page appears.
3. Click **+ New Scan**.



4. Select a **Scan Template**.



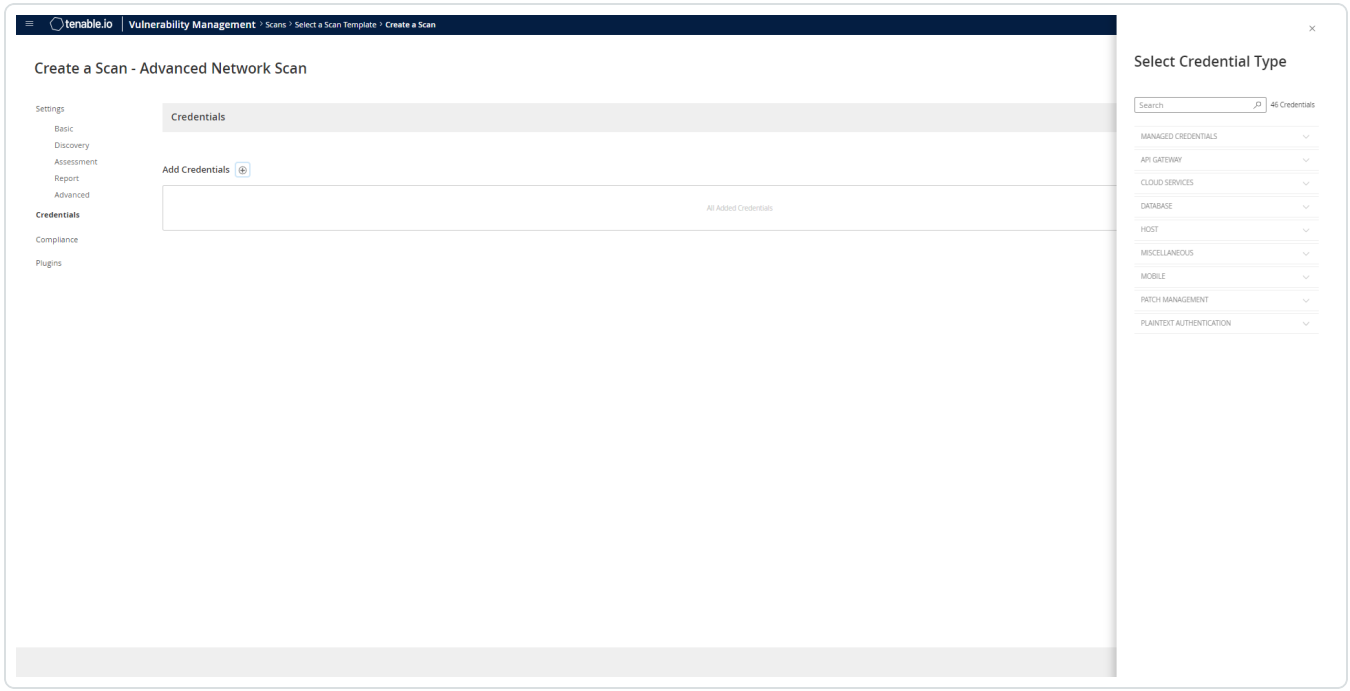
The scan configuration page appears.



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.

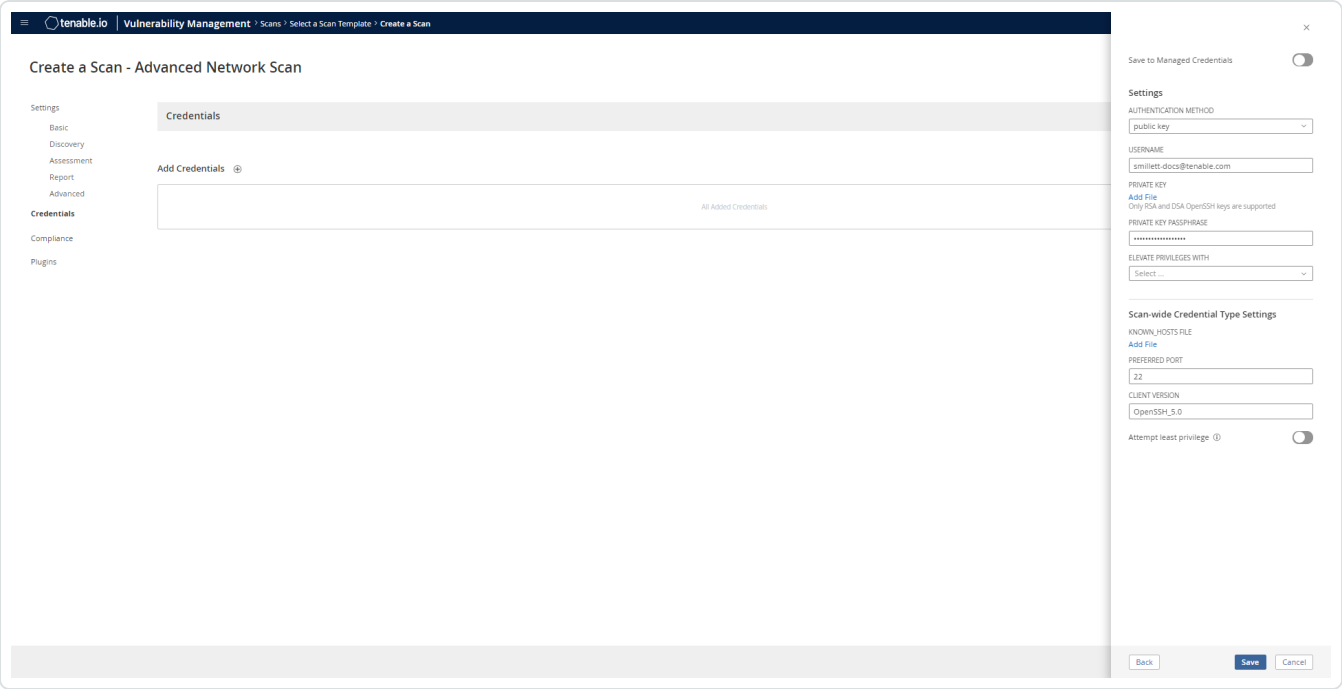
8. Click the **Credentials** tab.

   The Credentials options appear.



9. In the **Select a Credential** menu, select the **Host** drop-down.
10. Select **SSH**.

    The **CyberArk** field options appear.



11. Configure each field for **SSH** authentication.

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. **Note:** Customers self-hosting CyberArk CCP on a Windows Server 2022 and above should follow the guidance found in Tenable's Community post about CyberArk Client Certification Authentication Issue.	no
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	Yes, if the private key is

Option	Description	Required
		applied.
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	Yes, if the private key is applied.
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	(Required if Kerberos Target Authentication is enabled.) The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	yes
KDC Transport	(Required if Kerberos Target Authentication is enabled.) The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	yes
Realm	(Required if Kerberos Target Authentication is enabled) The Realm is the authentication domain, usually noted as the domain name of the target (for example, example.com). By default, Tenable uses 443.	yes
Get credential by	The method with which your CyberArk API credentials are retrieved. Can be **Address**, **Identifier**, **Parameters**, or **Username**.	yes

Option	Description	Required
	Note: For more information about the **Parameters** option, refer to the **Parameters Options** table. **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.	
Username	(If **Get credential by** is set to **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
Targets to Prioritize	Specify IPs or CIDR blocks on which this credential is attempted before any other	no

Option	Description	Required
Credentials	credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	

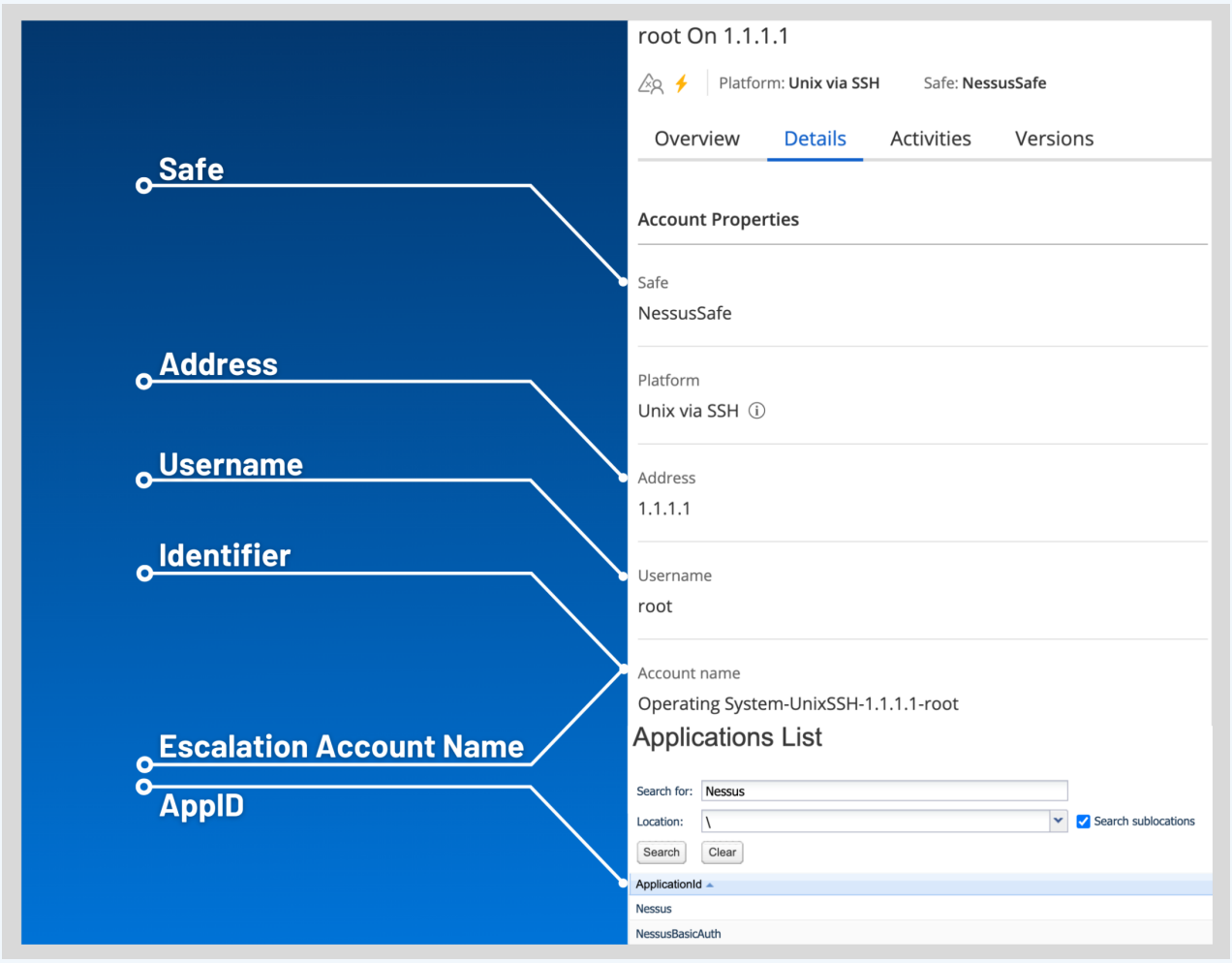
Parameters Options

The following options can be specified when **Get Credential By** is set to **Parameters**. These request parameters allow for advanced filtering of accounts based on their properties. The options correspond to the various options supported by the CyberArk REST API, as found in CyberArk documentation. These options can be specified in many different combinations to filter account results by their properties. For example, specifying **Root** as the **Folder** option results in a REST API query containing `&Folder=Root`.

Option	Description	Required
Safe	The safe containing the credential.	no
Address	Limit the query to accounts matching the specified address.	no
Use Target IP Address	(Optional) When enabled, the integration appends the target address to the credential query, which limits the query to accounts matching the scan target's address. This is ignored if **Address** is set.	no

Option	Description	Required
Username	The username of the credential.	no
Account Name	The unique identifier assigned to the credential.	no
Folder	The folder of the credential.	no
Database	The database of the credential.	no
Query	Specify a custom “free query” using account properties. When this method is specified, all other search criteria are ignored.	no
Query Format	Defines the query format. allowed values are **Exact** and **Regexp**. The default is **Exact**. This value is ignored unless the **Query** option was specified.	no

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



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

12. 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

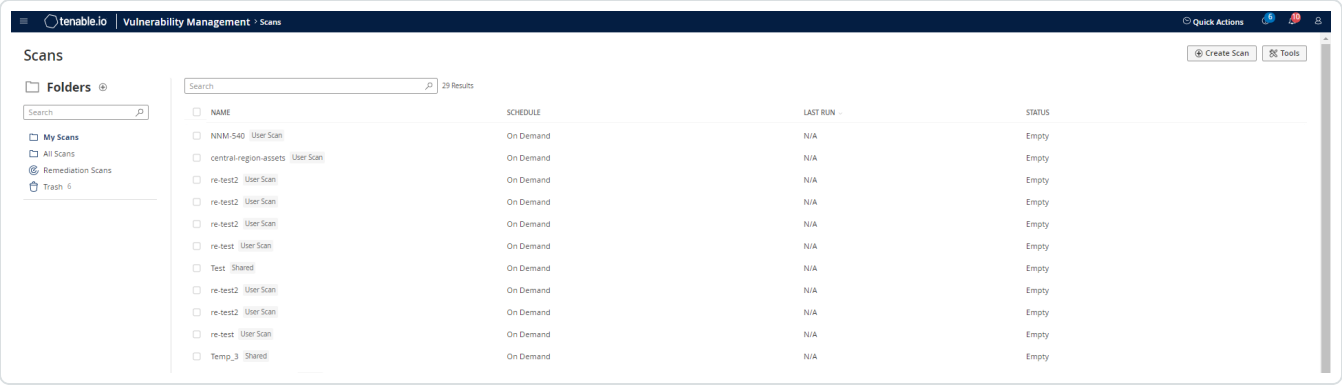
> **Required User Role:** Standard, Scan Manager, or Administrator

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

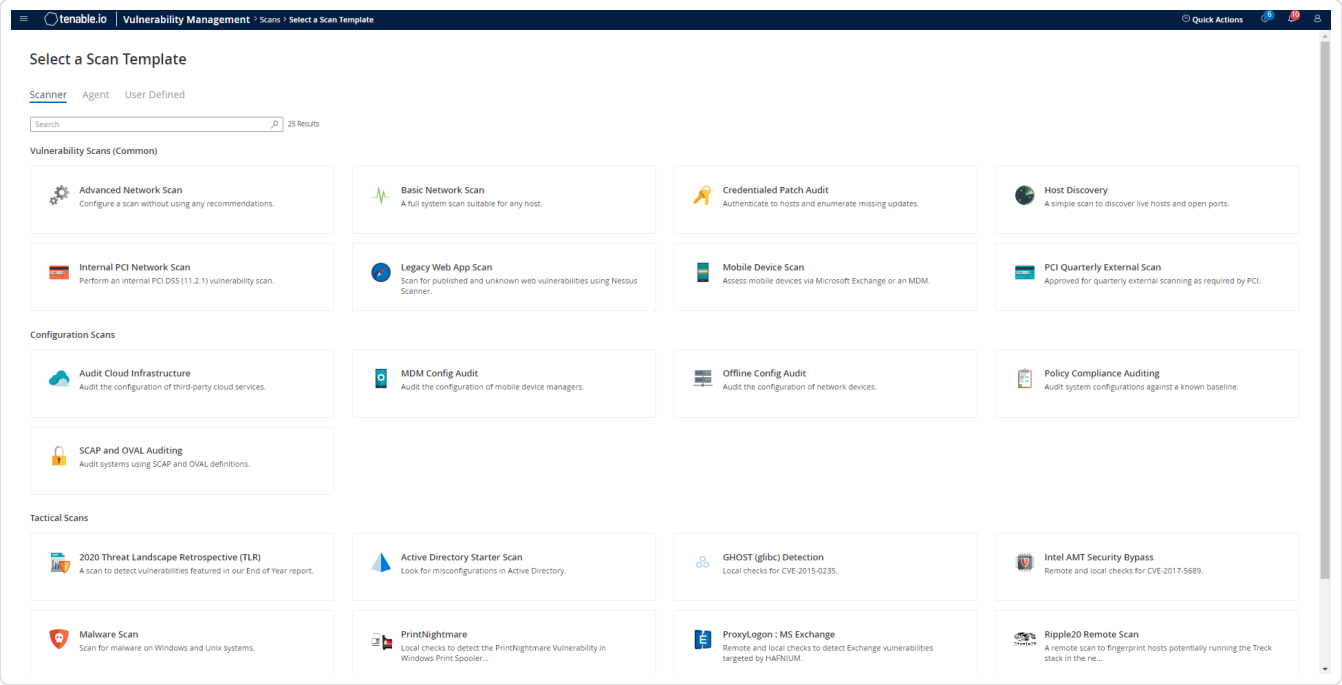
To configure SSH integration:

1. Log in to Tenable Vulnerability Management.
2. In the left navigation plane, click **Scans**.

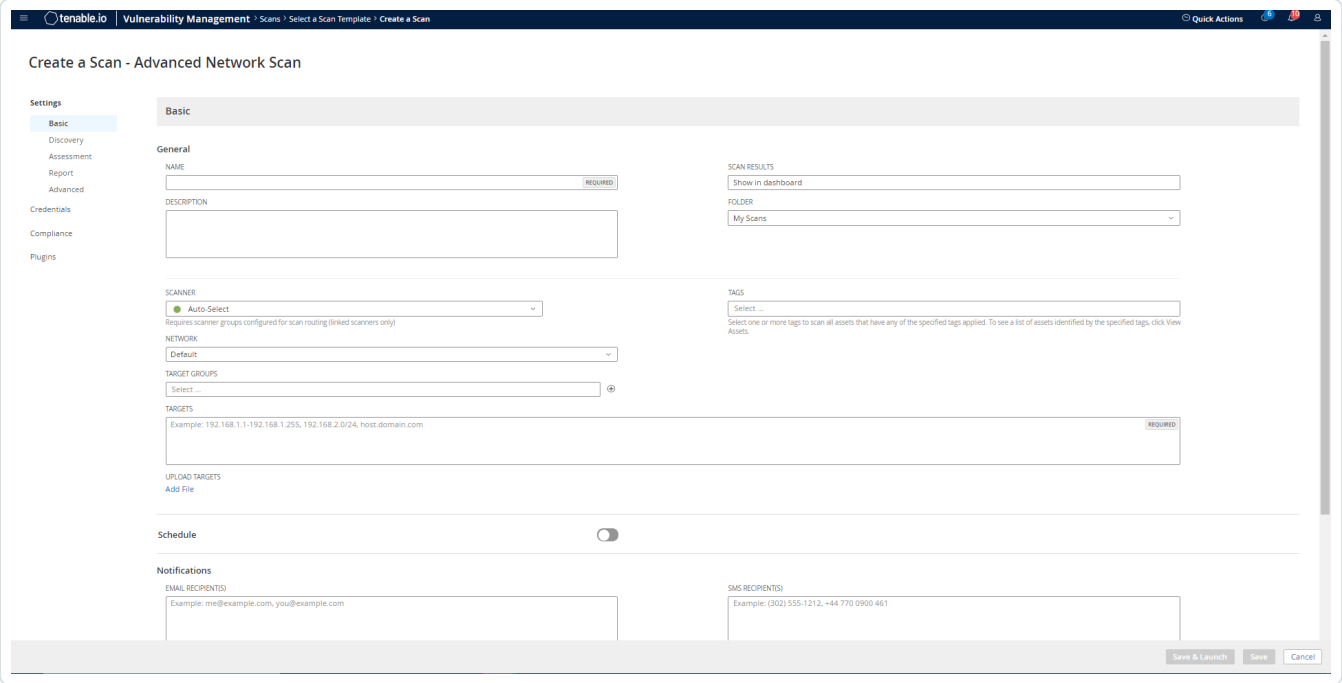
   The **Scans** page appears.
3. Click **+ New Scan**.



4. Select a **Scan Template**.



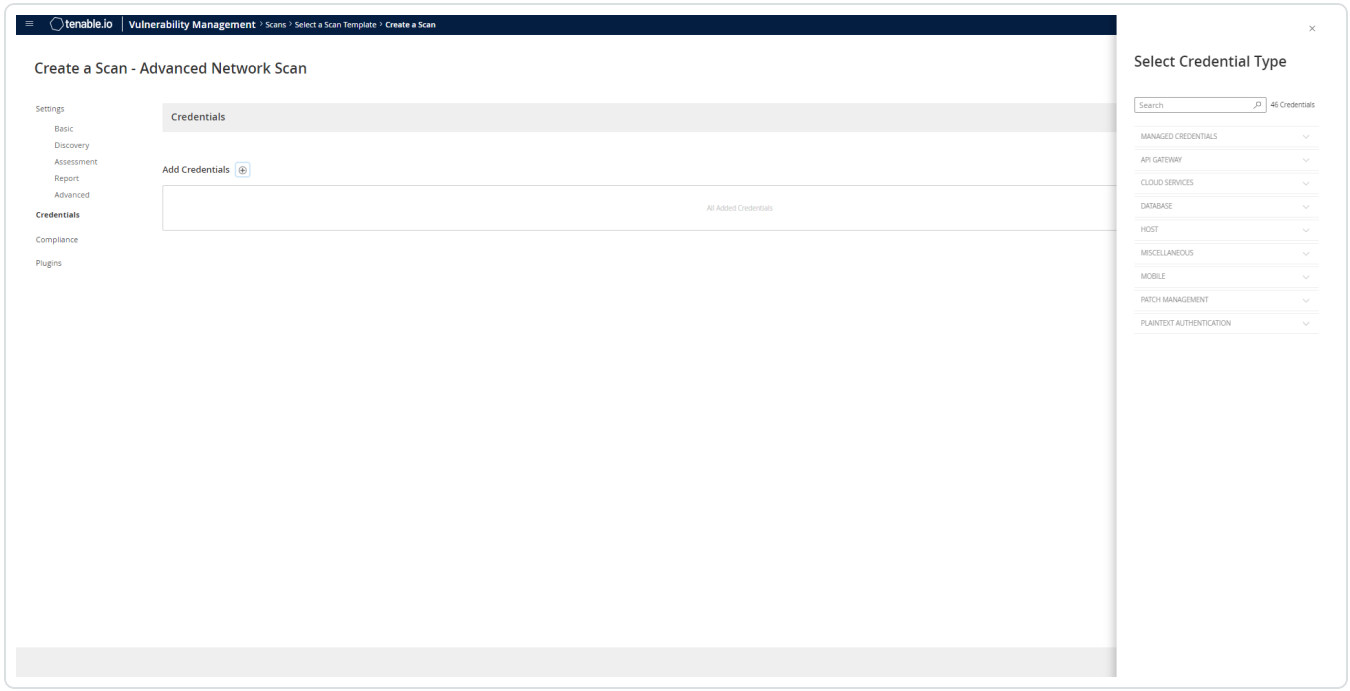
The scan configuration page appears.



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.

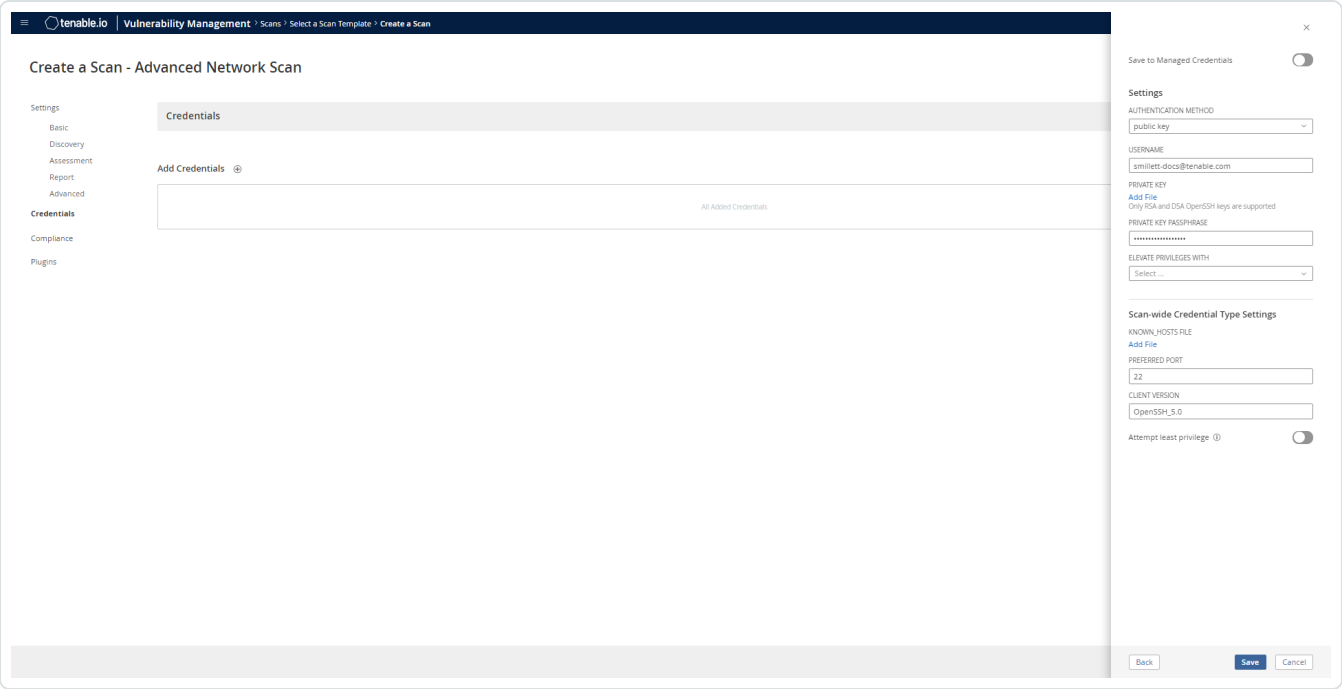
8. Click the **Credentials** tab.

   The Credentials options appear.



9. In the **Select a Credential** menu, select the **Host** drop-down.

10. Select **SSH** as the **Type** and CyberArk as the **Authentication Method.**



11. Select an option for the **Elevate Privileges With** field.

> **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**, **Get Escalation Credential By**, and **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 Vulnerability Management User Guide.

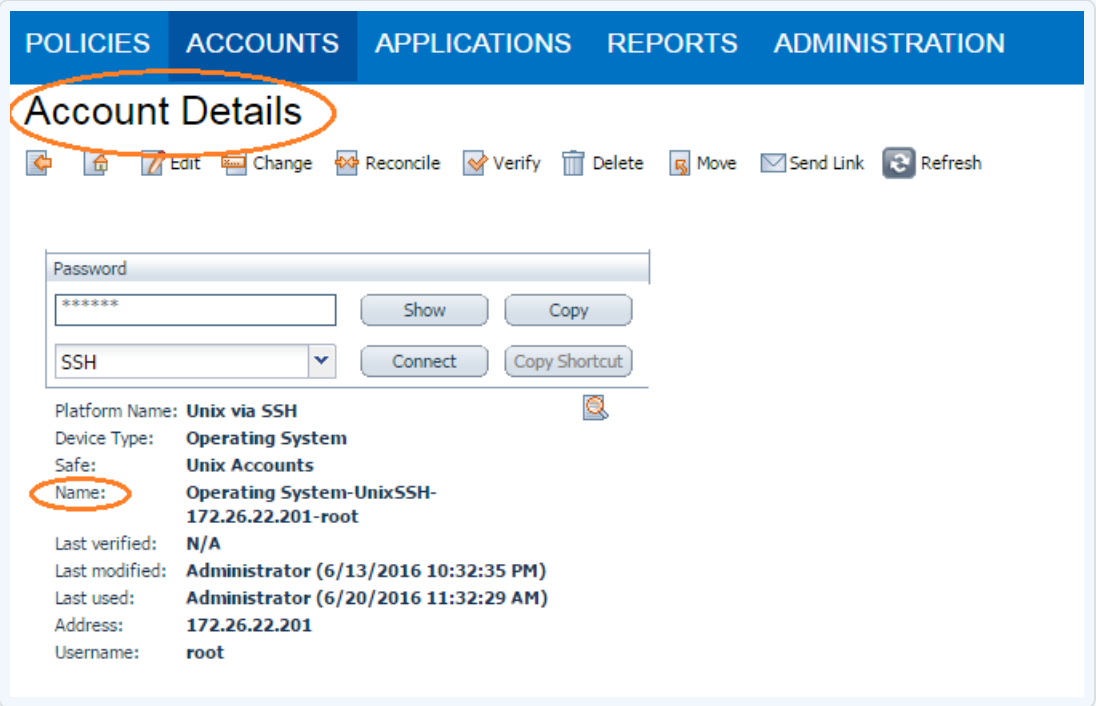
12. Select an option for the **Get Escalation Credential By** field.

> **Note:** The **Escalation Credential** may be obtained using the same query parameters as the login credential. Specifying an escalation credential identifier is optional. When no escalation credential is specified, the login credential is used for both login and escalation. If using a different password for login and escalation (for example, using su to “switch user”), it is required to enter both the login and escalation users.

13. Complete the privilege escalation options and click **Save**.

> **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.



Windows Integration

Required User Role: Standard, Scan Manager, or Administrator

To configure Tenable Vulnerability Management with CyberArk using Windows integration:

1. Log in to your Tenable user interface.
2. In the left navigation plane, click **Scans**.

   The **Scans** page appears.
3. In the upper-right corner of the page, click the **Create a Scan** button.

   The **Select a Scan Template** 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 **Host** section, click **Windows**.

   The selected credential options appear.
10. In the **Authentication Method** drop-down, select **CyberArk**.

    The **CyberArk** options appear.
11. Configure the **CyberArk** credentials.

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. **Note:** Customers self-hosting CyberArk CCP on a Windows Server 2022 and above should follow the guidance found in Tenable's Community post about CyberArk Client Certification Authentication Issue.	no
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	Yes, if the private key is

Option	Description	Required
		applied.
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	Yes, if the private key is applied.
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified Linux or Unix target.	no
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled) This host supplies the session tickets for the user.	yes
KDC Port	(Required if Kerberos Target Authentication is enabled) The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	yes
KDC Transport	The KDC uses TCP by default in Linux implementations. For UDP, change this option. If you need to change the KDC Transport value, you may also need to change the port as the KDC UDP uses either port 88 or 750 by default, depending on the implementation.	yes
Domain	(Required if Kerberos Target Authentication is enabled) The domain to which Kerberos Target Authentication belongs, if applicable.	yes
Get credential by	The method with which your CyberArk API credentials are retrieved. Can be **Address**, **Identifier**, **Parameters**, or **Username**. **Note:** For more information about the **Parameters** option, refer to the **Parameters Options** table.	yes

Option	Description	Required
	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.	
Username	(If **Get credential by** is set to **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

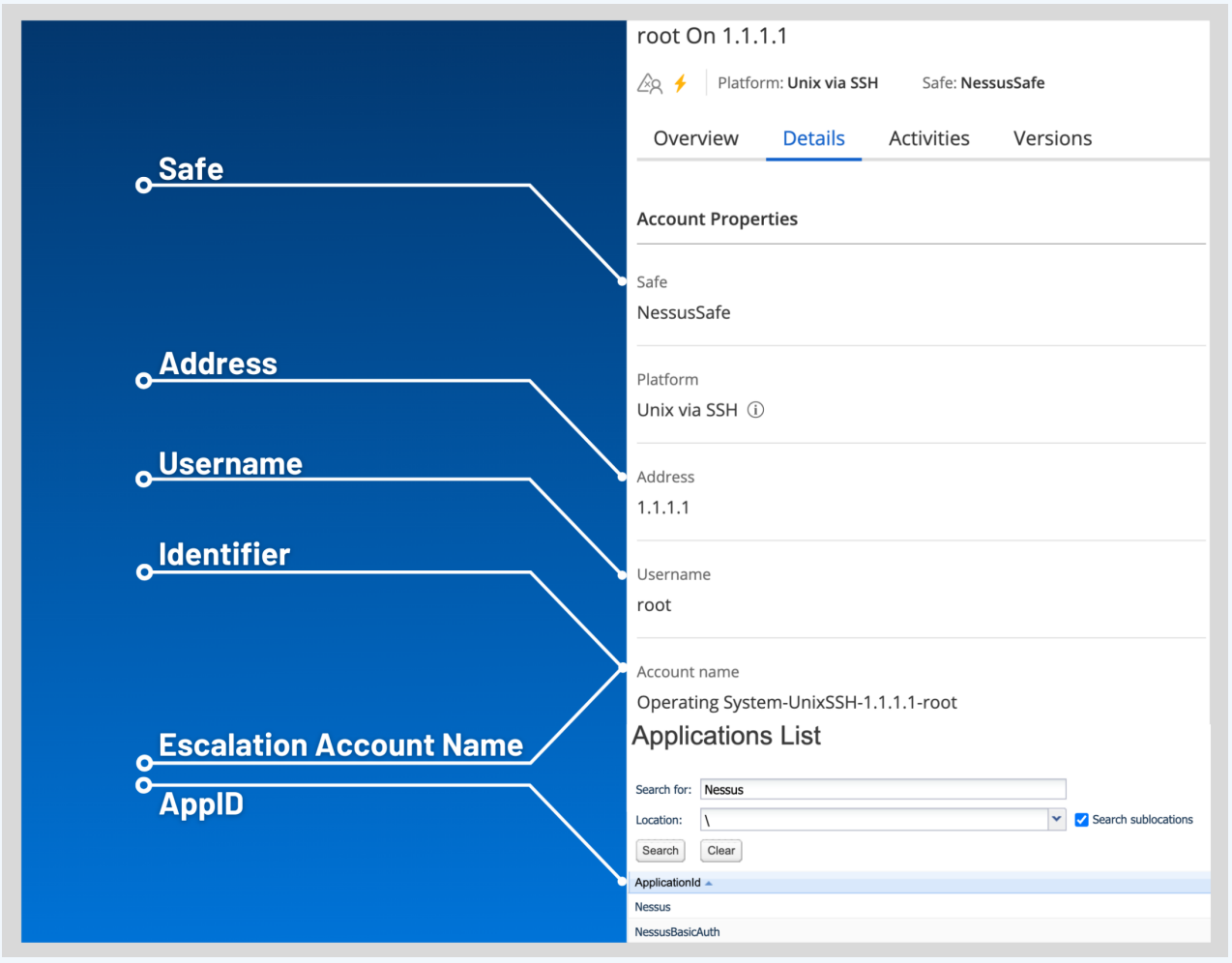
Parameters Options

The following options can be specified when **Get Credential By** is set to **Parameters**. These request parameters allow for advanced filtering of accounts based on their properties. The options correspond to the various options supported by the CyberArk REST API, as found in CyberArk documentation. These options can be specified in many different combinations to

filter account results by their properties. For example, specifying **Root** as the **Folder** option results in a REST API query containing `&Folder=Root`.

Option	Description	Required
Safe	The safe containing the credential.	no
Address	Limit the query to accounts matching the specified address.	no
Use Target IP Address	(Optional) When enabled, the integration appends the target address to the credential query, which limits the query to accounts matching the scan target's address. This is ignored if **Address** is set.	no
Username	The username of the credential.	no
Account Name	The unique identifier assigned to the credential.	no
Folder	The folder of the credential.	no
Database	The database of the credential.	no
Query	Specify a custom "free query" using account properties. When this method is specified, all other search criteria are ignored.	no
Query Format	Defines the query format. allowed values are **Exact** and **Regexp**. The default is **Exact**. This value is ignored unless the **Query** option was specified.	no

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



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

12. 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 authentication is not successful, refer to the Debugging CyberArk Issues section of this document.

SNMPv3 Integration

> **Required User Role:** Standard, Scan Manager, or Administrator

Tenable Vulnerability Management provides an option for CyberArk SNMPv3 integration. Complete the following steps to configure Tenable Vulnerability Management with CyberArk for SNMPv3.

Before you begin:

- Ensure you have both a Tenable Vulnerability Management and CyberArk account.

To integrate Tenable Vulnerability Management with CyberArk using SNMPv3 credentials:

1. Log in to Tenable Vulnerability Management.
2. In the left navigation plane, click **Scans**.

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

   The **Select a Scan Template** 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 **SNMPv3**.

The **Settings** pane appears.

11. In the SNMPv3 Authentication Method drop-down, select CyberArk.

    The CyberArk options appear.

12. Configure each option for SNMPv3 authentication.

> **Note:** The SNMPv3 credential with the CyberArk authentication type will always use the same account for all the targets. Unlike SSH, Windows, and Database, there is no way to separate accounts by target IP/FQDN. This is because the SNMPv3 CyberArk integration does not include target IP/FQDN in its queries for credentials. The SNMPv3 CyberArk credential does not collect an Account Name or Identifier, because the credential issues two separate queries for authentication and privacy passwords, which can not be specified via a single account identifier. Tenable recommends that the same username and address be assigned to a single pairing of SNMPv3 and SNMPv3PrivacyKey within CyberArk.

Option	Description	Required
Username	(Required) The username for the SNMPv3 account that Tenable Vulnerability Management uses to perform checks on the target system.	yes
Port	The TCP port that SNMPv3 listens on for communications from Tenable Vulnerability Management. By default, Tenable uses 161.	yes
SNMPv3 Authentication Method	The authentication method to SNMPv3. Available options: • Password Entry • CyberArk **Note:** Select **CyberArk** from the options.	yes
Security Level	The security level for SNMP (set to **Authentication and privacy** by default): • No authentication and no privacy	yes

Option	Description	Required
	• Authentication without privacy • Authentication and privacy	
Authentication Algorithm	The algorithm the remove service supports the following: SHA1, SHA224, SHA-256, SHA-384, SHA-512, or MD5.	yes
Privacy Algorithm	The encryption algorithm to use for SNMP traffic: AES, AES-192, AES-192C, AES-256, AES-256C, or DES.	yes
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
CyberArk 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	The CyberArk safe, the credential should be retrieved from.	no
Username	(If **Get credential by** is set to **Username**) The username of the CyberArk user to request a password from.	no
Account Name	(If **Get credential by** is **Identifier**) The unique account name or identifier assigned to the CyberArk API credential.	no
CyberArk Address	The option should only be used if the Address value is unique to a single CyberArk account credential.	no

Option	Description	Required
Folder	The folder of the credential.	no
Database	The database of the credential.	no
Query	Specify a custom “free query” using account properties. When this method is specified, all other search criteria are ignored.	no
Query Format	Defines the query format. Allowed values are **Exact** and **Regexp**. The default is **Exact**. This value is ignored unless the **Query** option was specified.	no
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 the private key is applied.
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	Yes, if private key is applied.
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

13. Do one of the following:

    - If you want to save without launching the scan, click **Save**.

- If you want to save and launch the scan immediately, click **Save & Launch**.

> **Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

What to do next

Verify the integration is working:

1. On the **My Scans** page, click the **Launch** button to initiate an on-demand scan.
2. Once the scan completes, select the completed scan and look for the following message:

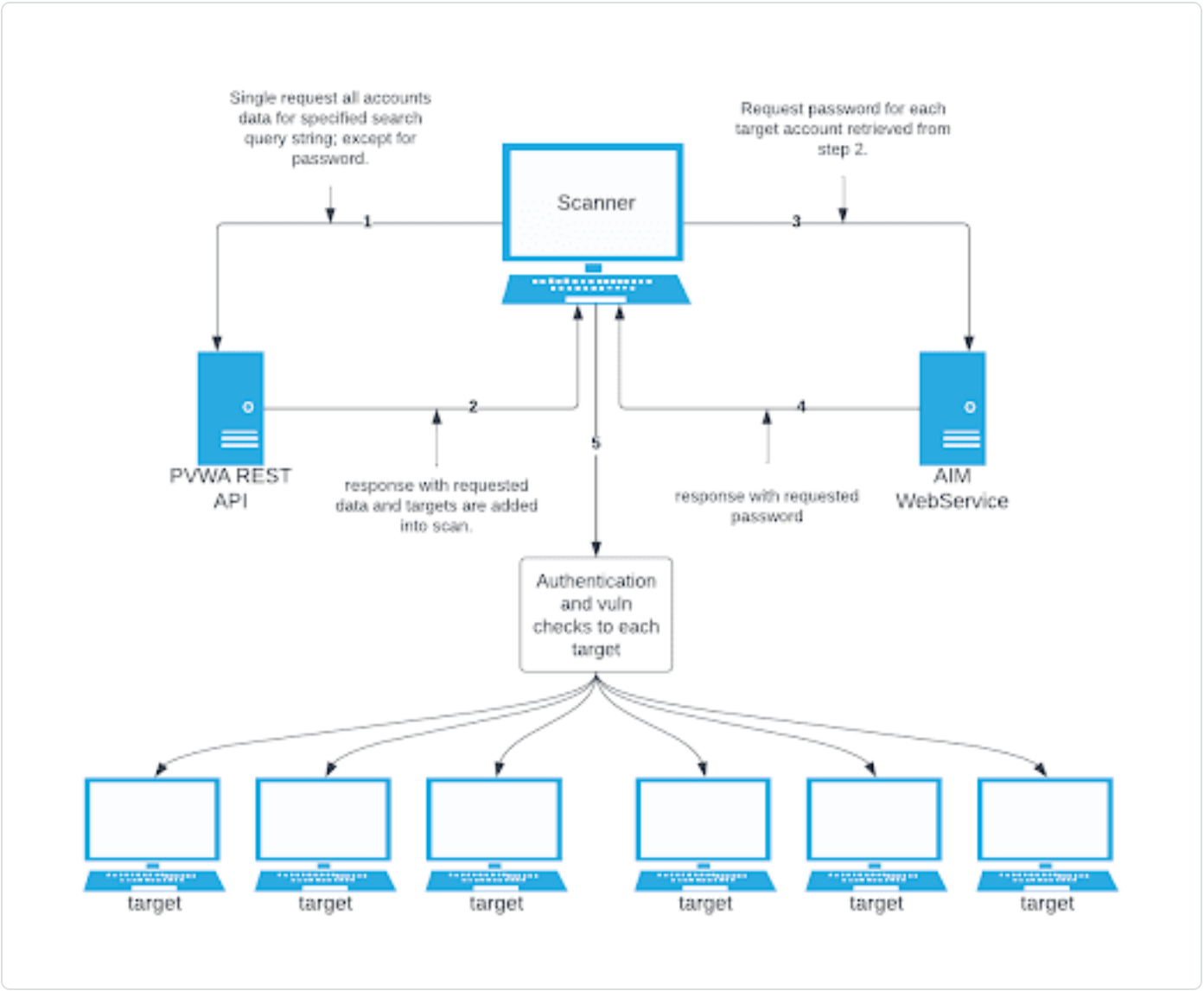
   ```
   For SNMPv3 : Plugin ID 141118. This result validates if It was possible to
   log into the target SNMPv3 host via the provided credentials from CyberArk.
   ```

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.

> **Caution:** Tenable recommends utilizing scanner groups with one scanner when using Auto-Discovery credentials and users should only enter only a single initial host in the scan. If multiple scanners are used in an Auto-Discovery scan, targets retrieved from the integration may be scanned multiple times.



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

> **Required User Role:** Standard, Scan Manager, or Administrator

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 the 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 types 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

Field name	Description	Field value
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

To configure database auto-discovery:

1. Log in to Tenable Vulnerability Management.
2. In the left navigation plane, click **Scans**.

   The **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.

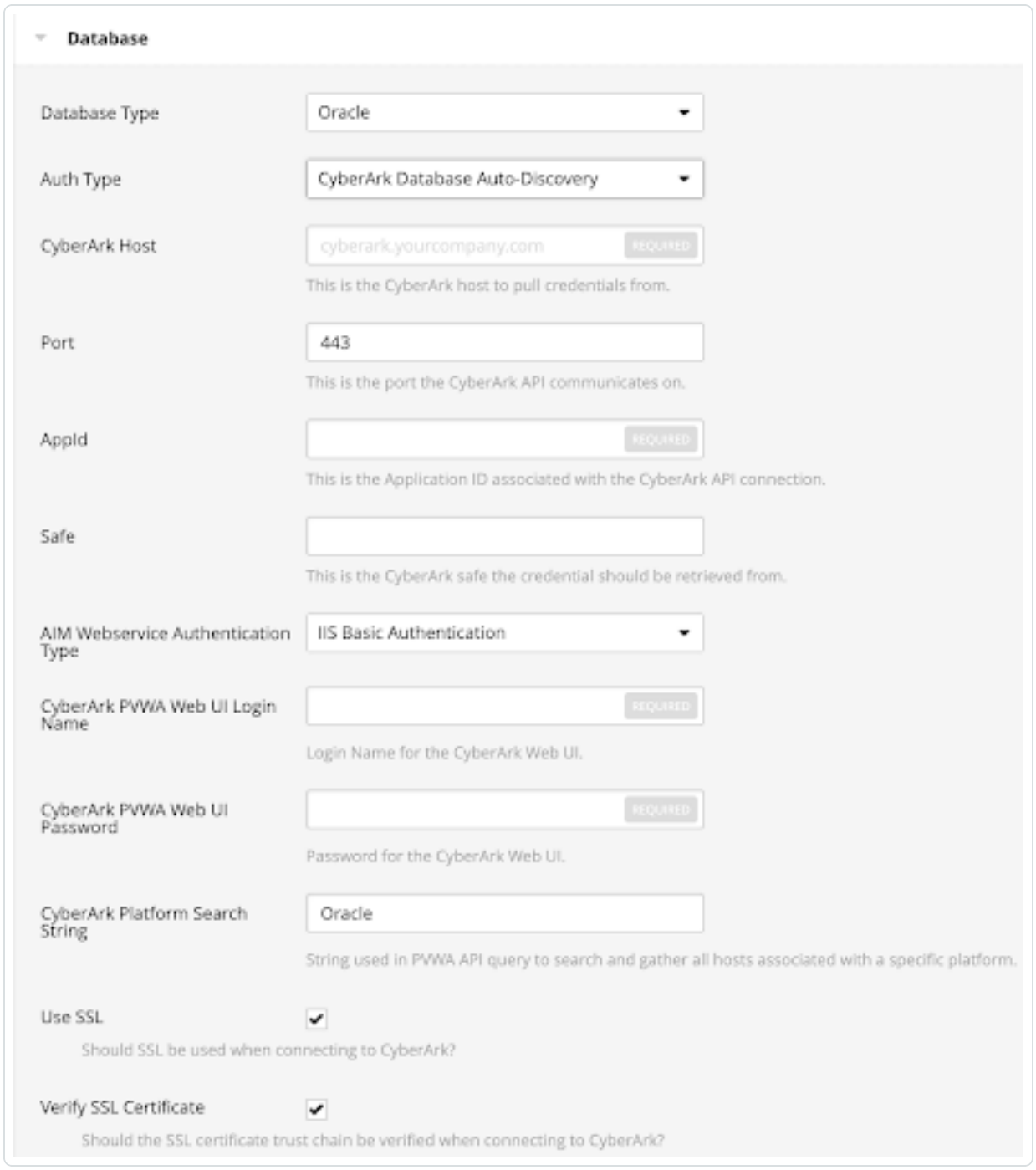
   The **Credentials** pane appears.

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:



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
	Note: Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	yes
CCP Host	The IP address or FQDN name for the user's CyberArk CCP component. (Not available with Tenable Security Center.) **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the CCP host.	no
CCP Port	The port on which the CyberArk CCP (AIM Web Service) API communicates. By default, Tenable uses 443. (Not available with Tenable Security Center.) **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the CCP host.	no
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

Option	Description	Required
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
PVWA REST API Authentication Method	Choose whether to authenticate to the PVWA by entering username and password or to gather credentials from the Central Credential Provider (CCP). (**Not available with Tenable Security Center.**)	yes
PVWA REST API Credential ID	The unique identifier ("Account name") of the CyberArk account containing CCP credentials. (**Not available with Tenable Security Center.**)	Yes, if the PVWA REST API Authentication Method is set to **Gather from CCP**.
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	yes

Option	Description	Required
	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.	
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 Vulnerability Management User Guide and the **Central Credential Provider Implementation Guide** located at cyberark.com (login required).

13. Click **Save**.

SSH Auto-Discovery

Required User Role: Standard, Scan Manager, or Administrator

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.

Note: Privilege Escalation is available, but only using the SUDO method at this time. More research is needed to explore other escalation methods.

Note: SSH Key authentication is supported, but escalated privileges after SSH Key authentication is not available at this time.

To configure SSH auto-discovery:

1. Log in to Tenable Vulnerability Management.
2. In the left navigation plane, click **Scans**.

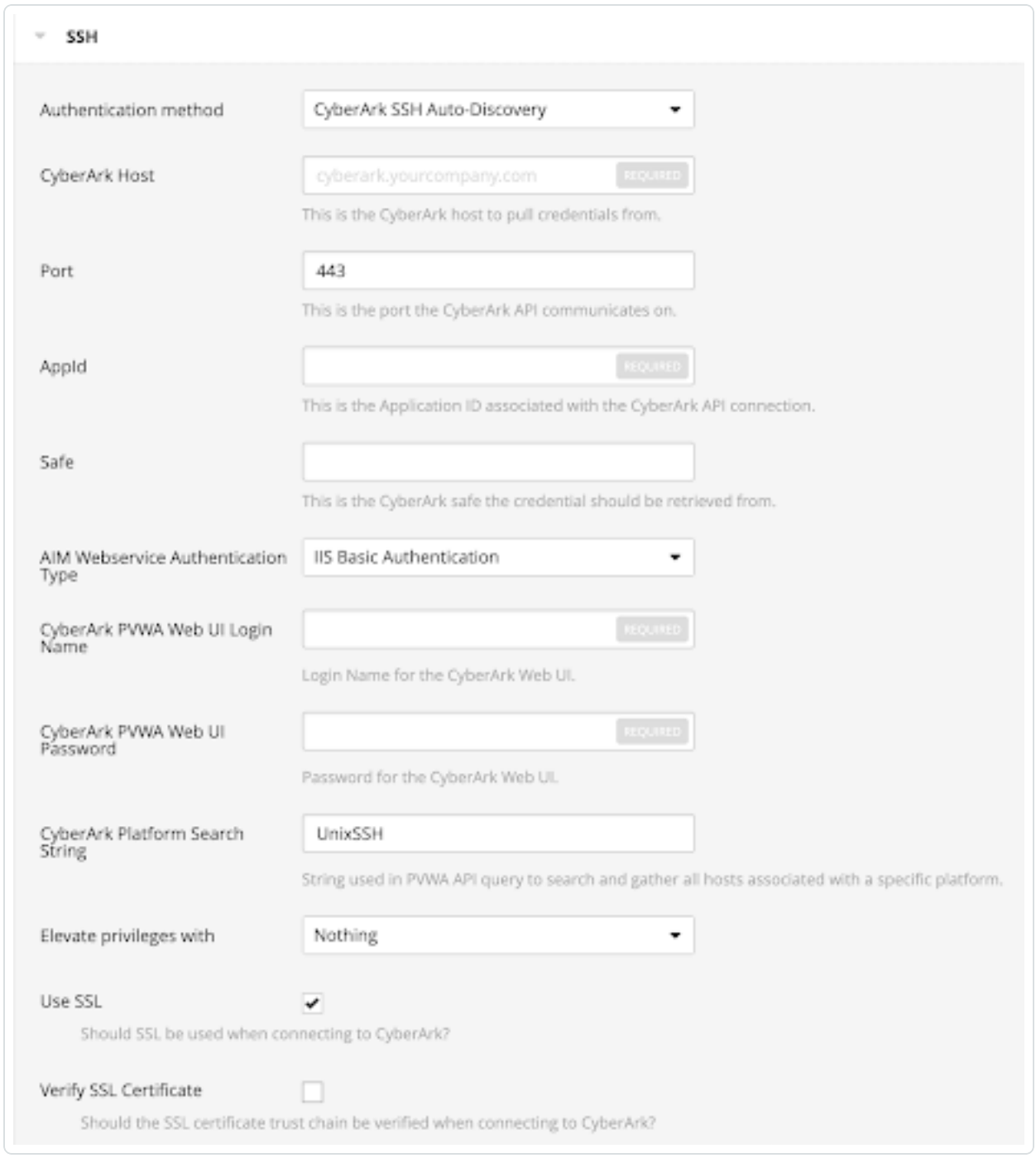
   The **Scans** page appears.
3. Click **+ New Scan**.

   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:



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
	Note: Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	yes
CCP Host	The IP address or FQDN name for the user's CyberArk CCP component. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	no
CCP Port	The port on which the CyberArk CCP (AIM Web Service) API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	no
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**	yes

Option	Description	Required
	Authentication and **Certificate Authentication**. Certificate Authentication can be either encrypted or unencrypted.	
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
PVWA REST API Authentication Method	Choose whether to authenticate to the PVWA by entering username and password or to gather credentials from the Central Credential Provider (CCP). (**Not available with Tenable Security Center.**)	yes
PVWA REST API Credential ID	The unique identifier ("Account name") of the CyberArk account containing CCP credentials. (**Not available with Tenable**	Yes, if the PVWA REST API Authentication

Option	Description	Required
	Security Center.)	Method is set to **Gather from CCP**.
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
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	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 Vulnerability Management User Guide and the **Central Credential Provider Implementation Guide** located at cyberark.com (login required).

13. Click **Save**.

Windows Auto-Discovery

Required User Role: Standard, Scan Manager, or Administrator

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 Vulnerability Management.
2. In the left navigation plane, click **Scans**.

   The **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 left navigation plane, click **Settings**.

   The **Settings** page appears.

10. Click the **Credentials** widget.

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

11. Click the ⊕ button next to the **Credentials** title.

    The credential form plane appears.

12. Click the **Host** option.

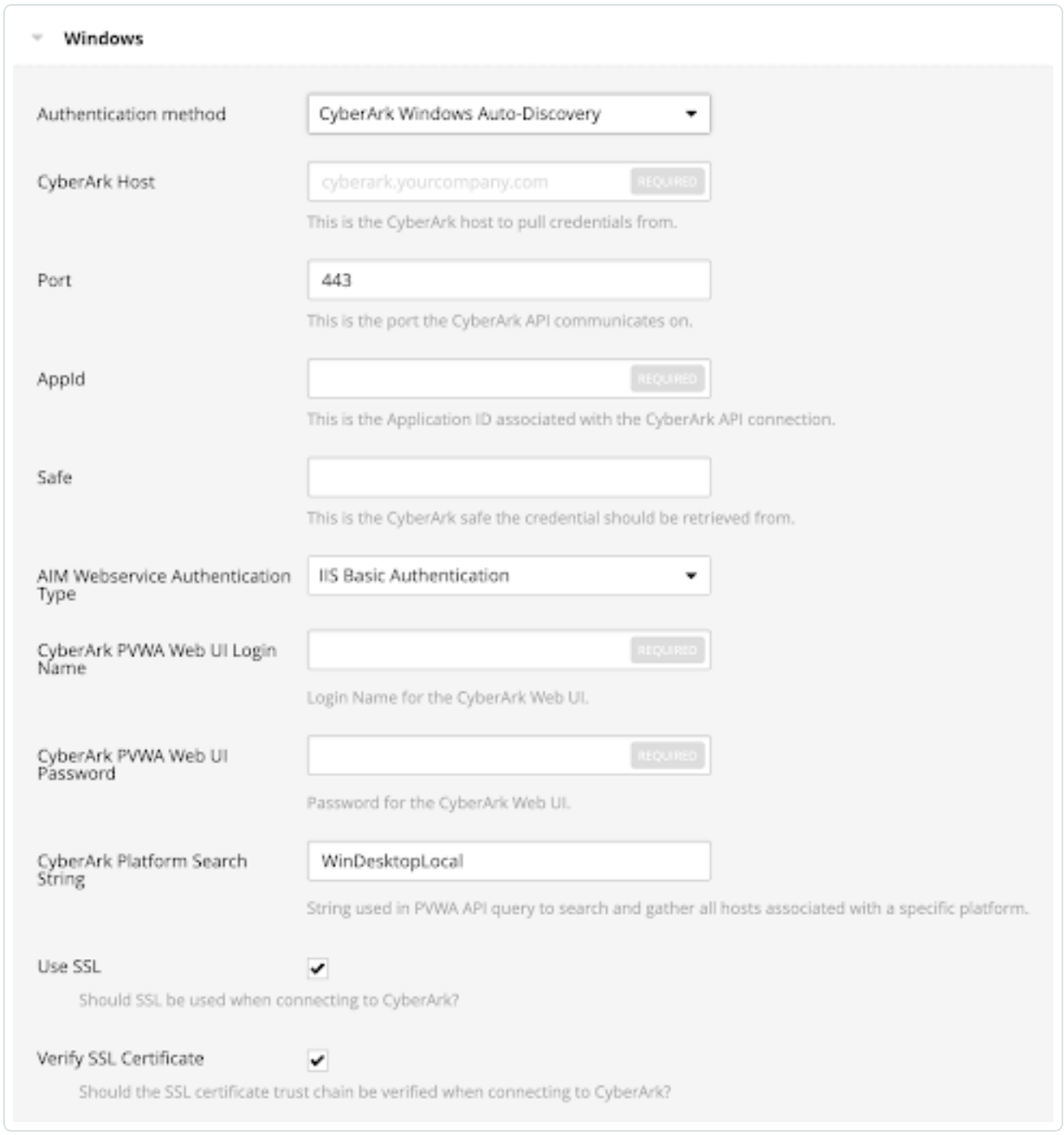
    The **Host** options appear.

13. In the **Host** section, click **Windows**.

    The selected credential options appear.

14. From the **Authentication Method** drop-down, select **CyberArk Windows Auto-Discovery**.

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



15. 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

Option	Description	Required
	Note: Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	
Port	The port on which the CyberArk API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	yes
CCP Host	The IP address or FQDN name for the user's CyberArk CCP component. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	no
CCP Port	The port on which the CyberArk CCP (AIM Web Service) API communicates. By default, Tenable uses 443. **Note:** Customers hosting the PVWA and CCP on separate servers should only use this field for the PVWA host.	no
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**	yes

Option	Description	Required
	Authentication and **Certificate Authentication**. Certificate Authentication can be either encrypted or unencrypted.	
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 practice would be to create a custom platform name in CyberArk and enter that value in this field to improve accuracy.	yes
PVWA REST API Authentication Method	Choose whether to authenticate to the PVWA by entering username and password or to gather credentials from the Central Credential Provider (CCP). (**Not available with Tenable Security Center.**)	yes
PVWA REST API Credential ID	The unique identifier ("Account name") of the CyberArk account containing CCP credentials. (**Not available with Tenable**	Yes, if the PVWA REST API Authentication

Option	Description	Required
	Security Center.)	Method is set to **Gather from CCP**.
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 Vulnerability Management User Guide and the **Central Credential Provider Implementation Guide** located at cyberark.com (login required).

16. Click **Save**.

CyberArk Legacy Integrations

Caution: Support for SOAP requests are no longer be supported by CyberArk as of December 31, 2024. If you are using the CyberArk Legacy Integration which utilizes SOAP for API requests, Tenable recommends using our non-Legacy CyberArk Integration which supports REST API requests.

View one of the following options for CyberArk Legacy integration steps.

Database (Legacy) Integration

SSH (Legacy) Integration

Privilege Escalation (Legacy)

Windows (Legacy) Integration

Database (Legacy) Integration

Caution: Support for SOAP requests are no longer be supported by CyberArk as of December 31, 2024. If you are using the CyberArk Legacy Integration which utilizes SOAP for API requests, Tenable recommends using our non-Legacy CyberArk Integration which supports REST API requests.

To configure database integration:

1. Log in to Tenable Vulnerability Management.
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**.

    The **CyberArk** field options appear.
12. Configure each field for the **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, Tenable uses `/AIMWebservice/v1.1/AIM.asmx`. **Note:** When the customer is using the default path, they can leave this blank.	no
Central Credential Provider Username	All	If the CyberArk Central Credential Provider (CCP) is configured to use basic authentication, you can fill in this field for authentication. **Note:** This field should be the Username to Authenticate to the AIM Web Service API.	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

Option	Database Types	Description	Required
CyberArk Client Certificate	All	The file that contains the PEM certificate used to communicate with the CyberArk host.	no
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	no

Option	Database Types	Description	Required
		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
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 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 Vulnerability Management User Guide and the **Central Credential Provider Implementation Guide** located at cyberark.com (login required).

13. Click **Save**.

SSH (Legacy) Integration

Caution: Support for SOAP requests are no longer be supported by CyberArk as of December 31, 2024. If you are using the CyberArk Legacy Integration which utilizes SOAP for API requests, Tenable recommends using our non-Legacy CyberArk Integration which supports REST API requests.

To configure SSH integration:

1. Log in to Tenable Vulnerability Management.
2. Click **Scans**.
3. Click **+ New Scan**.
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 options appear.

9. In the **Select a Credential** menu, select the **Host** drop-down.

10. Select **SSH**.

    The **CyberArk** field options appear.

11. Configure each field for **SSH** authentication.

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 uses `/AIMWebservice/v1.1/AIM.asmx`. **Note:** When the customer is using the default path, they can leave this blank.	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	If the CyberArk Central Credential Provider (CCP) is configured to use basic authentication, you can fill in this field for authentication. **Note:** This field should be the Username to Authenticate to the AIM Web Service API.	no
Central Credential	The password of the vault, if the CyberArk Central Credential Provider is configured to use basic	no

Option	Description	Required
Provider Password	authentication.	
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	no

Option	Description	Required
	communication.	
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 CyberArk receiving an unrecognized password prompt on the target host's interactive SSH shell.	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 Vulnerability Management User Guide and the **Central Credential Provider Implementation Guide** located at cyberark.com (login required).

12. 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.

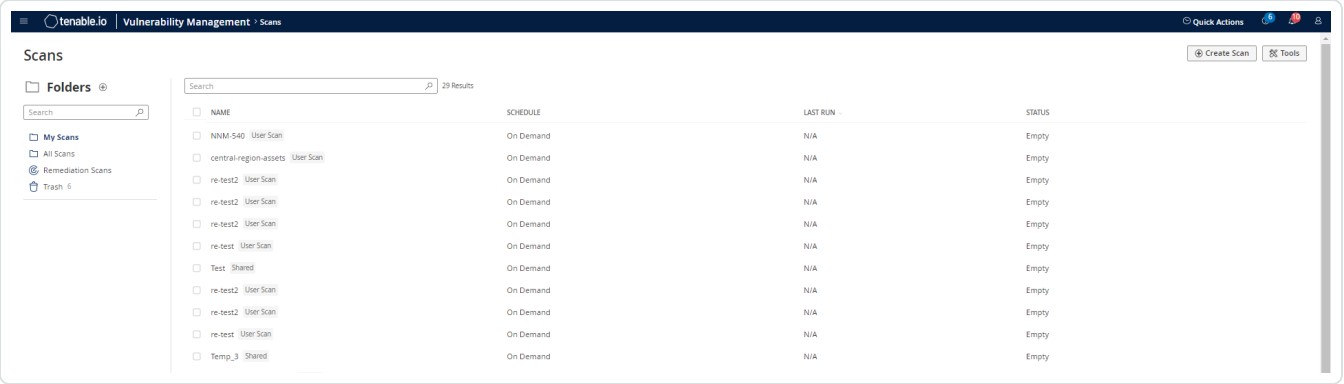
Privilege Escalation with CyberArk (Legacy) Credentials

Caution: Support for SOAP requests are no longer be supported by CyberArk as of December 31, 2024. If you are using the CyberArk Legacy Integration which utilizes SOAP for API requests, Tenable recommends using our non-Legacy CyberArk Integration which supports REST API requests.

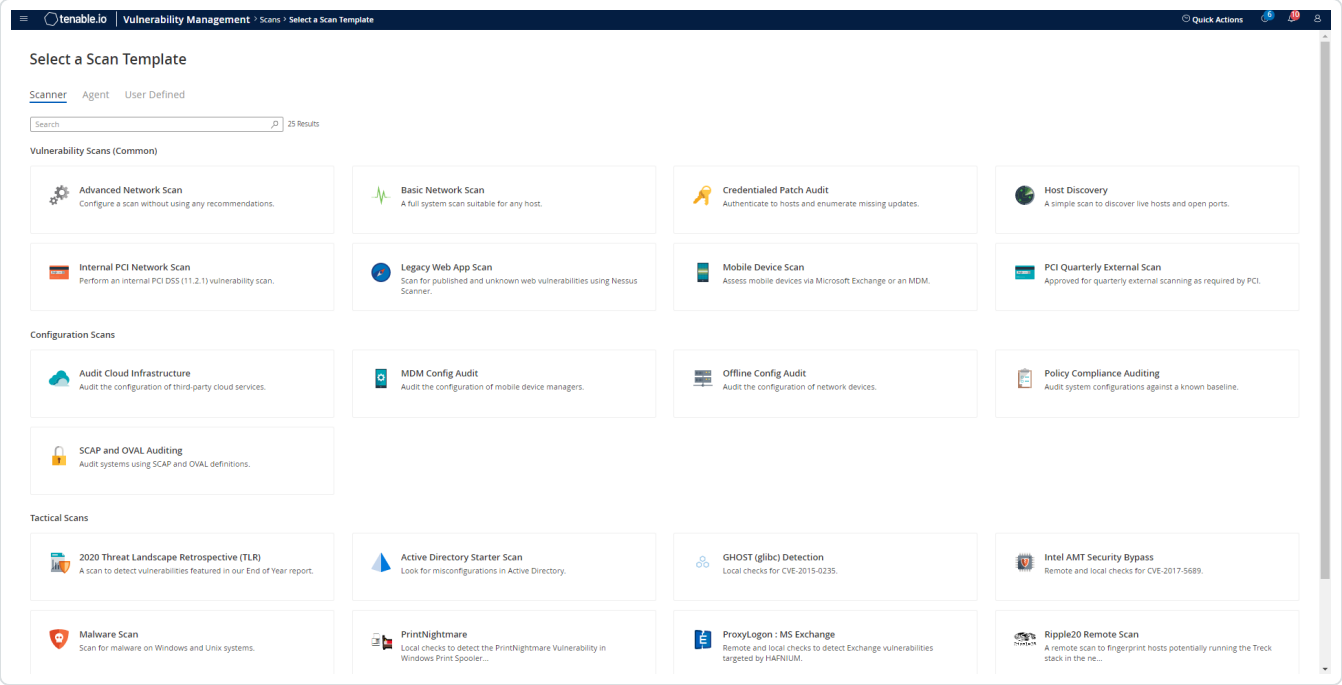
Tenable Vulnerability Management supports the use of privilege escalation, such as *su* and *sudo*, when using SSH through the CyberArk authentication method.

To configure SSH integration:

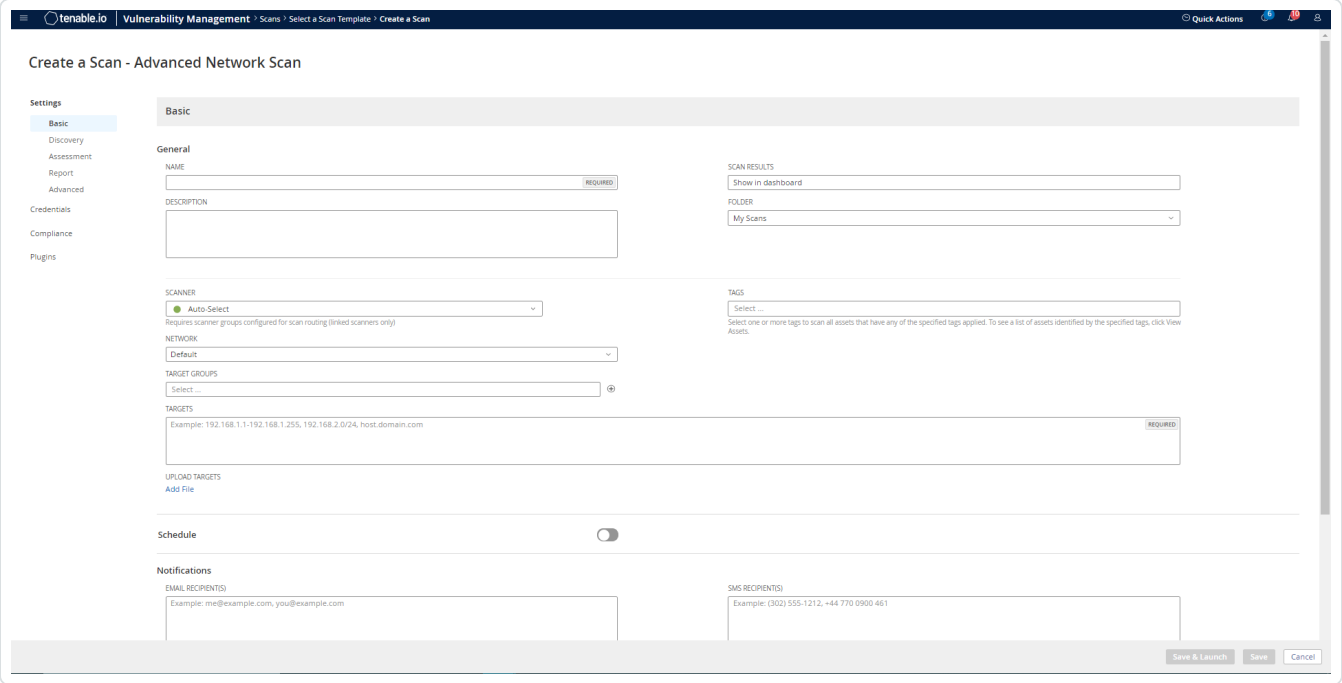
1. Log in to Tenable Vulnerability Management.
2. Click **Scans**.
3. Click **+ New Scan**.



4. Select a **Scan Template**.



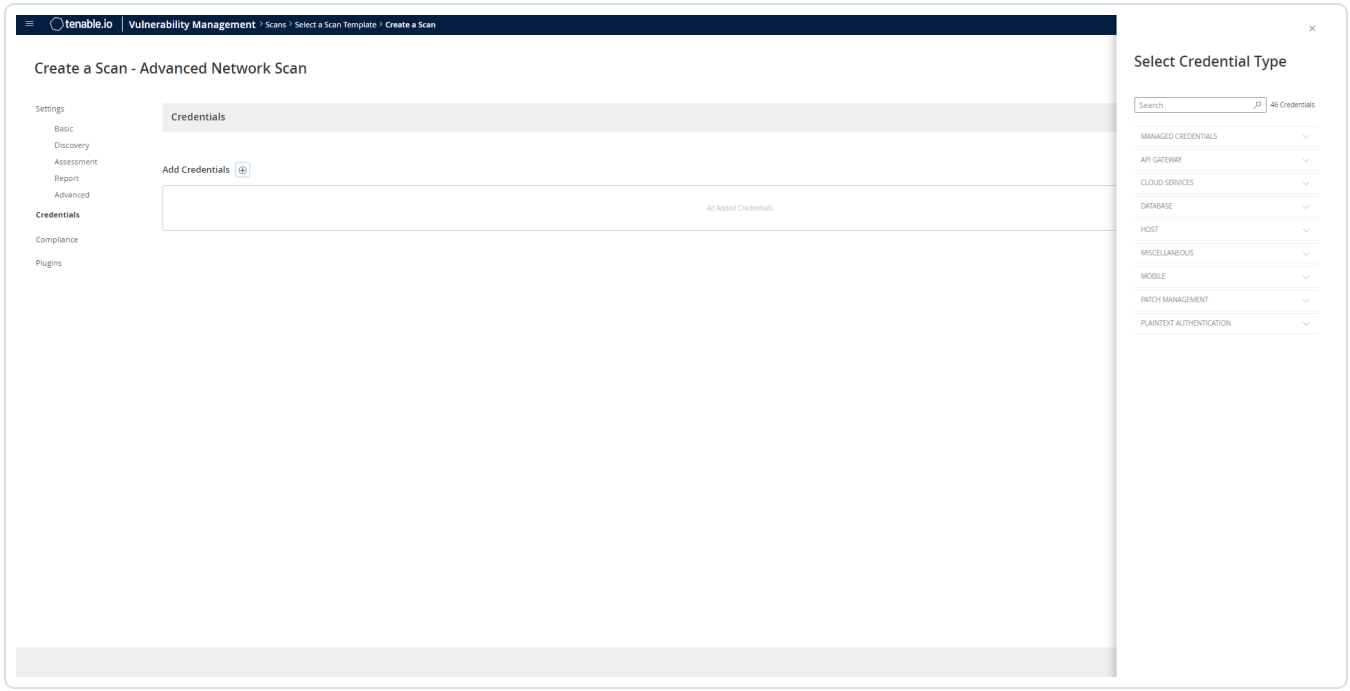
The scan configuration page appears.



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.

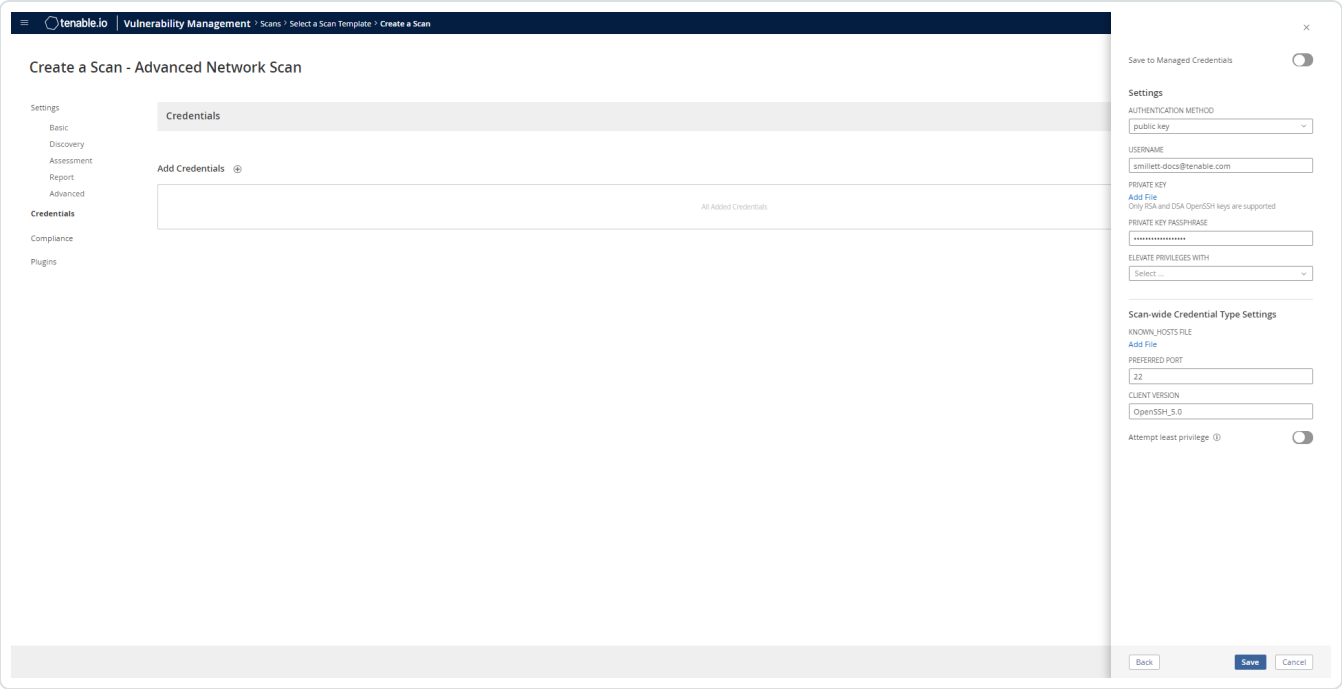
8. Click the **Credentials** tab.

   The Credentials options appear.



9. In the **Select a Credential** menu, select the **Host** drop-down.

10. Select **SSH** as the **Type** and CyberArk as the **Authentication Method.**



11. Select an option for the **CyberArk Elevate Privileges With** field.

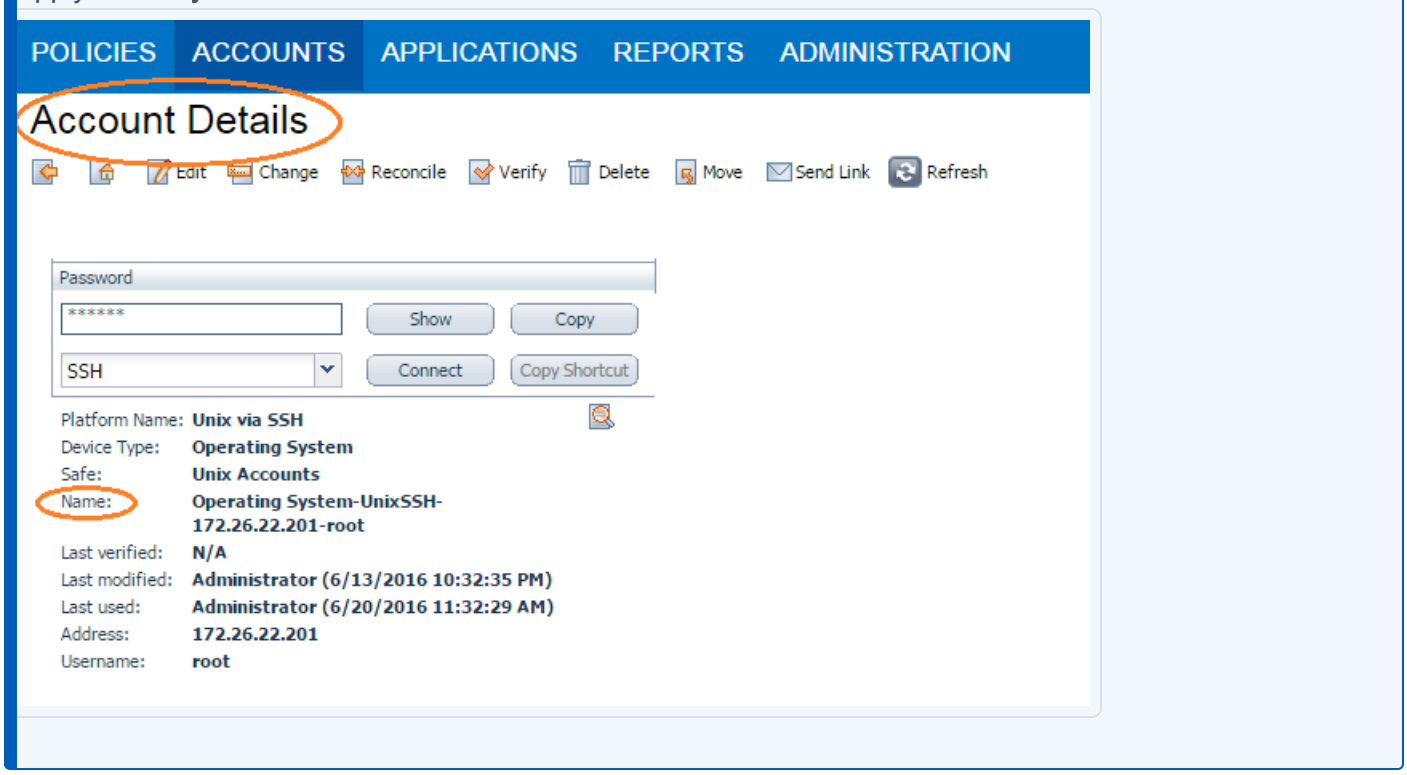
> **Note:** Multiple options for privilege escalation are supported, including *su*, *su+sudo* and *sudo*. For example, if **sudo** is selected, additional fields for **sudo user**, **CyberArk Account Details Name** and **Location of sudo** (directory) are provided and can be completed to support authentication 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 Vulnerability Management User Guide.

12. Complete the privilege escalation options and click **Save**.

> **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

upply in the **CyberArk Account Details Name** field.



Windows (Legacy) Integration

To configure Tenable Vulnerability Management with CyberArk using Windows integration:

1. Log in to Tenable Vulnerability Management.
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.

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 uses `/AIMWebservice/v1.1/AIM.asmx`. **Note:** When the customer is using the default path, they can leave this blank.	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
Central Credential Provider Username	If the CyberArk Central Credential Provider (CCP) is configured to use basic authentication, you can fill in this field for authentication. **Note:** This field should be the Username to Authenticate to the AIM Web Service API.	no
Central Credential	The password of the vault, if the CyberArk Central Credential Provider is configured to use basic	no

Option	Description	Required
Provider Password	authentication.	
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	no

Option	Description	Required
	to support SSL through IIS check for secure communication.	
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 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 Vulnerability Management User Guide and the **Central Credential Provider Implementation Guide** located at cyberark.com (login required).

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 authentication is not successful, refer to the Debugging CyberArk Issues section of this document.

Additional Information

[CyberArk Domain and DNS Support]

[Tenable Vulnerability Management Priority Scanning for CyberArk]

[Retrieving Addresses to Scan from CyberArk]

[Debugging CyberArk Issues]

CyberArk Integration Helpful Tips

The overall process of the CyberArk integration is like other PAM integrations, as follows:

- TVM or SC pass the policy and credential values down to Nessus. This would include values like the CyberArk host, port, object identifier, and client certificates.
- The Nessus scanner communicates with the API, and the API returns the username, password, and/or SSH key required for target authentication.
- The scanner uses these values for target authentication.

Overall Process with Auto-Discovery

With Auto-Discovery, the integration initiates an initial collection of hosts and the object identifiers that contain their respective credentials. The scan will inject the discovered hosts as new scan targets, and the object identifiers are stored as Knowledge Base (KB) items.

After the collection of hosts and KBs is complete, the authentication process kicks off on each of the hosts. For each host, the integration requests the following target credentials: username, password, SSH private key, private key passphrase, and, if applicable, the elevation command.

Client Authentication

All API authentication occurs directly between the scanner and the PAM API. In other words, neither Tenable Vulnerability Management nor SecurityCenter connect to the PAM API. API authentication occurs using one of the following supported authentication types.

Client Certificate Authentication (recommended)

Customers can configure a client certificate for authentication to the AIM Web Service. After creating and configuring the certificate on the Windows Service, adding the binding to the IIS application, and

properly configuring SSL settings on the IIS that hosts the AIM Web Service, customers will need to extract the private key from the certificate and import both the Certificate and Private Key files in the CyberArk scan credential.

Server IP Whitelisting

Customers can add the server IP of the Nessus Scanner host to the “Allowed Machines” of the configured CyberArk Application. This ensures that only specific machines can communicate with the Web Service API server. In addition, the Windows Server Internet Information Service (IIS) that is hosting the AIM Web Service application must be configured to allow this kind of communication.

Note: Whether using Server IP Whitelisting or Client Certification Authentication, customers must add the scanner IP to the list of “Allowed Machines” configuration for the CyberArk Application devoted to the AIM Web Service.

IIS Basic Authentication

Customers may use IIS Basic Authentication, but this is only available with Auto-Discovery. Tenable recommends using Client Certificates instead.

AIM Web Service API

The Tenable integration with CyberArk requires the presence of a self-hosted component called the Central Credential Provider (CCP). The CCP contains the AIM Web Service API that Tenable requests credentials (username, domain, password, private key, and private key passphrase) from. It has one API resource called GetPassword and returns a single password. It cannot be used to return multiple passwords in a single request.

- The default AIM Web Service URL is AIMWebService/V1.1/AIM.asmx
- Tenable recommends leaving `CyberArk AIM Service URL` blank when using the default path.
- The CyberArk (Legacy) integration uses the SOAP API, everything else uses the REST API. Note that the SOAP API has been deprecated by CyberArk.
- For the SNMPv3 credential type, the scanner needs to make two separate requests if the credential requires both Authentication and Privacy passwords.

When using Auto-Discovery, the integration also interfaces with the Password Vault Web App (PVWA) API. Therefore, Auto-Discovery requires credentials to both PVWA and CCP.

Testing Connectivity with curl

This section contains commands for testing the CCP and PVWA APIs.

Both the commands in this section use the -k option to disable SSL verification. This may not strictly be necessary, and may not be desirable. The commands in this section are split into several lines for readability. When copying it, be sure to copy the backslash (\) characters so that the command executes correctly.

Execute the following command to test connectivity to the CCP:

```
curl -k -X GET -G \
  https://CYBERARK_IP:PORT/AIMWebService/api/Accounts \
  --data-urlencode 'AppID=APP_ID' \
  --data urlencode 'Safe=SAFE' \
  --data-urlencode 'UserName=USER' \
  --data-urlencode 'Address=ADDRESS' \
  --cert /path/to/client_cert.pem \
  --key /path/to/client_cert_privatekey.pem
```

Replace the command values with the values in the following table.

Value	Replacement
CYBERARK_IP	The IP address of the CCP server.
PORT	The Port of the CCP server.
APP_ID	The registered app ID.
SAFE	The registered safe with the account.
USER	The username of the account to fetch.
ADDRESS	The username and address of the account to fetch.
/path/to/client_cert.pem	Path to the certificate file.
/path/to/client_cert_privatekey.pem	Path to the key file.

Expected Output:

```
{"Content":"PASSWORD_HERE", "creationmethod":"PVWA","address":
"ADDRESS","Safe":"SAFE","username":"USER","object": "OBJECT_ID",[...] }
```

Hints:

- The various --data-urlencode parameters are different query parameters for how to fetch an account. The example above uses App ID, Safe, User and Address.
- For example, omit --data-urlencode 'UserName=USER' to match any account with the given address regardless of username.
- Another example, to fetch a password by its object ID instead of username/address, replace the --data-urlencode 'UserName=USER' and --data-urlencode 'Address=ADDRESS' lines with --data-urlencode 'Object=OBJECT_ID'.
- This command assumes client certificate authentication, which Tenable strongly recommends.
- This command will return the literal password of the account, which can be useful for verifying its correctness.

For testing Auto-Discovery, test both the CCP as well as the PVWA service. To test PVWA connectivity, execute the following command:

```
curl -k -X POST --header 'Content-Type: application/json' \
--data '{"username":"USER","password":"PASSWORD"}' \
https://CYBERARK_IP:PORT/PasswordVault/API/auth/Cyberark/Logon
```

Value	Replacement
CYBERARK_IP	The IP address of the CCP server.
PORT	The Port of the CCP server.
USER	The PVWA username.
PASSWORD	The PVWA password.

The expected output should be an API token, a long string of random-looking characters.

Get Credential By

The following section only applies to CyberArk without Auto-Discovery.

The CyberArk integration allows users to specify the accounts to use in multiple ways: by username, by address, by object ID, or by parameters. The integration behaves differently in each of these cases. This can be adjusted through the “Get Credential By” drop-down menu.

Username

The integration gets the target account with the given username. It only returns accounts that also match the target IP address or FQDN. This means that different accounts are used across different targets.

Address

The integration gets the target account with the given address. If left blank, it returns the account that matches the target IP address or FQDN.

Identifier

The integration gets the account with the given Account Name, its global identifier. Account names are unique across the entire CyberArk environment, so in this case the integration disregards the value of the current target IP address. In other words, it uses the same account across all targets.

Parameters

The integration will get the account matching the supplied parameters. This option is an advanced option that provides more direct control of the exact API query parameters. In this mode, it is possible to toggle whether or not to include the target’s IP address or FQDN in the API query.

Number of API requests

The overall number of API requests are higher when using a query which returns accounts matching the target IP address or FQDN (for example, “by username”), because each query is different for each target. There is one request per target.

Additionally, although the integration uses a cache to reduce unnecessary requests, the cache is not shared among scan chunks. Therefore, when using “by identifier”, the number of requests will still be one per scan chunk.

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

Frequently Asked Questions (FAQ)

How many API requests does the integration make?

The number of requests depends on the value of Get Credential By, and also by how the scan is "chunked." For example, getting a credential by username gets a separate credential for each target, but getting a credential by identifier just gets a single credential for all targets. However, in this latter case, the requests are repeated for each scan chunk.

Do you support Privilege Cloud or ISPSS?

Privilege Cloud is supported in the current integration as long as the customer has deployed the Central Credential Provider (CCP). The CCP is required for the current integration. Tenable plans to release support for ISPSS through an integration with CyberArk Secrets Manager (formerly known as "Conjur").

> **Note:** CyberArk Secrets Manager is not yet supported in SecurityCenter (release TBD),

The API call said "server did not respond to request."

This may be caused by several issues.

- The scanner may be unable to connect to the CyberArk server. Try checking connectivity with ping or curl commands.
- Windows Server 2022 and newer do not support TLS 1.3 with Client Certificates. Try disabling TLS 1.3.
- The scanner may be unable to verify the CyberArk server's SSL certificate. Try importing the signing certificate authority (CA) as a custom CA, or disable "verify SSL" in the credential.
- There may be a problem with the file format of the client certificate. Make sure that certificate and private key are separate files and in .pem format, not pfx format.

The error "Password object matching query [...] was not found" appears in the debug log.

This error means that the supplied query parameters did not match an account in CyberArk. It can be caused by many different things, but it usually means that the supplied query parameters were incorrect. To resolve this issue:

- Review the exact query parameters that were entered in the credential. Review the debug log to see the exact API call that the integration used.
- Determine if Safe needs to be specified, or if it can be omitted.
- Check if the Application has appropriate permissions.

The error "Too many password objects matching query [...] were found" appears in the debug log.

The CCP GetPassword endpoint can only return a single object, but the supplied parameters were not specific enough to specify a single object. Try refining

The query is not specific enough as CCP GetPassword endpoint can only return a single entity. Try refining query parameters, or using "Get Credential By": Identifier.

A generic HTTP 404 error appears in the logs with HTML in the response body.

This is likely due to an incorrect base URL. In the credential, enter the full URL in the CyberArk Host field including the trailing "`/subdirectory/AIMWebService/api`" part.

Does the integration use FQDN or IP?

It depends on what was entered as the scan target. If the scan target is an IP, then the integration looks for CyberArk accounts matching the IP. If it was an FQDN, then the integration looks for accounts matching the FQDN. If using "Get Credential By": Identifier, then the integration disregards FQDN and IP and uses the account with the specified Account Name.

The scan successfully connected to CyberArk but the authentication is still failing.

Review Integration Status to check the success of the integration itself (i.e., did it get a password?). If authentication is failing, this is usually due to:

- Retrieved password/key is incorrect.
- Retrieved password/key in wrong format (CyberArk does not support encrypted SSH keys).
- Password rotation occurring before the scan is done using it.
- Issue in target operating system environment (review `ssh_get_info2.log`).

Do you support Windows domain accounts?

Tenable recommends configuring Windows domain accounts with a template that supports the "LogonDomain" or "Log on to" field, so that the domain can be retrieved from CyberArk.

What goes in the host field?

Users can enter either the host IP/FQDN or also the full base URL (e.g., `https://cyberark.corp.customer.com/AIMWebService/api`).

When does the integration collect credentials?

The integration collects credentials at the start of a scan, as a part of one of the authentication type's respective "settings" plugin. When using auto-discovery, target hosts are also collected at the start of a scan. Review the "Plugin Families and Plugins" for more detail.

Where are the logs?

Refer to the Debug Log Reporting section in the Scan Results Review page.

How does privilege escalation work?

Privilege escalation over SSH allows users to optionally specify a second account that contains the escalation password. In some cases (for example, sudo), the scan would use the same password for escalation as it would for login, in which case the escalation account does not need to be specified. In other cases (for example, su) the scan would need a different escalation password from the login password. In this case, users may specify the account containing this separate password. When necessary, users may also specify the account (username) to escalate to.

Note that sudo is the only supported privilege escalation method with Auto-Discovery.

How does passwordless SSH work?

The CyberArk integration can use either a password or SSH private key to authenticate. In the case of SSH private keys, the integration automatically detects if the received object is an SSH key. The integration does not support passphrase-encrypted private keys, because these are not currently supported by CyberArk. If using passwordless SSH in combination with privilege escalation, a separate escalation account may be specified, which contains the escalation password if necessary. Otherwise, the scan uses passwordless escalation.

How does the "Import" type credential work?

This option is only available with the CyberArk (Legacy) integration, which uses the CyberArk SOAP API and is currently deprecated by CyberArk. Tenable recommends using Auto-Discovery instead.

The Import/Entry options are an alternative way of specifying different target hosts and their respective credentials.

A user must specify parameters such as CyberArk Host, Port, and Client Certificate in a “Type: Entry” credential. Second, a user must create a “Type: Import” credential, and upload a comma-separated value (CSV) file containing extra parameters such as Target Host and CyberArk Object ID. This allows each row in the CSV file to function as its own, target-specific credential.

In Tenable Security Center, the “Import” type credential must be created after the “Entry” type credential.

What IP(s) do I need to whitelist on the CyberArk side?

All communication occurs between the PAM and the scanner. Therefore, focus on allowing scanner IP addresses.

CyberArk Domain and DNS Support

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

Tenable Priority Scanning for CyberArk

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

1. Tenable queries CyberArk with the target value entered into the Tenable **Targets** configuration field. For example, if you put a FQDN in the target list, Tenable queries CyberArk with the address value of the FQDN. If you enter an IP address or range such as 192.0.2.1-20, Tenable tries 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 then looks to see if there is a domain value (for a Windows system). If a domain value is present, Tenable queries 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 then pulls the IP address of the system. If the IP address does not match one of the IP addresses supplied in the target list, Tenable then queries 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.

Scan Results Review

This section can help you interpret the results of your scans and debug failures.

Plugin Families and Plugins

The CyberArk integration is available for several different credential types, but in all cases the Privileged Access management (PAM) integration executes within the credential's specific "settings" plugin, which is found in the "Settings" family.

The plugins that call the CyberArk integration are:

- Windows: logins.nasl
- SSH: ssh_settings.nasl
- Database: database_settings.nasl
- Nutanix: nutanix_settings.nasl
- VMware vCenter: vmware_vcenter_settings.nasl
- VMware ESXi: vmware_soap_settings.nasl
- SNMPv3: snmp_settings.nasl
- Auto Discovery Only:
    - pam_database_auto_collect.nasl
    - pam_ssh_auto_collect.nasl
    - pam_smb_auto_collect.nasl

Debug Log Reporting

To find debug logs specific to the CyberArk integration, look for logs within the Debugging Log Report plugin output. The plugin output will contain debugging logs for the Nessus plugins, including

the respective “settings” plugins which use the CyberArk integration. Users will see logs in the debug log reporting for the associated plugin with **~CyberArk** appended to it. For example, for SSH settings, debugging logs are found in “ssh_settings.nasl~CyberArk”.

For CyberArk credentials with “Auto-Discovery”, additional collection logs can be found in the Debugging Log. Reporting is logged for each particular host in the following logs:

- Database: pam_database_collect.nbin~CyberArk
- SSH: pam_ssh_collect.nbin~CyberArk
- Windows: pam_smb_collect.nbin~CyberArk

The debug logs for CyberArk will contain the details of how the settings plugin communicated with the PAM API. If an error occurred, its details are included in this log file. Errors may result in credentialed checks for the target failing. Common causes of errors include:

- Incorrect client certificate
- Error verifying CyberArk SSL certificate
- Incorrect value given for Object Identifier, Username, or Safe.
- Scanner unable to connect to CyberArk API
- Incorrect permissions

The Tenable Vulnerability Management 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 can discern from the previous log 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 Vulnerability Management 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.

To pull the target system values and how to use them.

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

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.