Tenable Vulnerability Management and CyberArk Enterprise Password Vault Integration Guide

Last Revised: May 18, 2023

Table of Contents

Welcome to Tenable.io for CyberArk 3

CyberArk Integrations 4

Database Integration 5

SSH Integration 12

Privilege Escalation with CyberArk Credentials 18

Windows Integration 22

CyberArk Legacy Integrations 26

Database (Legacy) Integration 27

SSH (Legacy) Integration 31

Privilege Escalation with CyberArk (Legacy) Credentials 35

Windows (Legacy) Integration 39

Additional Information 42

CyberArk Domain and DNS Support 43

Tenable.io Priority Scanning for CyberArk 44

Debugging CyberArk 45

Retrieving Addresses to Scan from CyberArk 47

About Tenable 48

Welcome to Tenable.io for CyberArk

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

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

The benefits of integrating Tenable.io with CyberArk include:

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

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

CyberArk Integrations

View one of the following options for CyberArk integration steps.

Database Integration

SSH Integration

Privilege Escalation

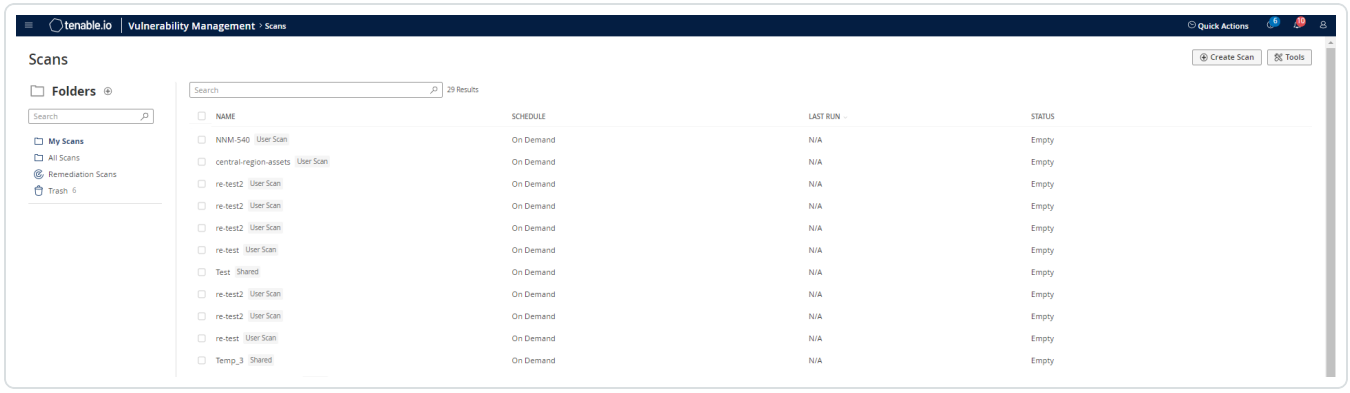
Windows Integration

Database Integration

To configure database integration:

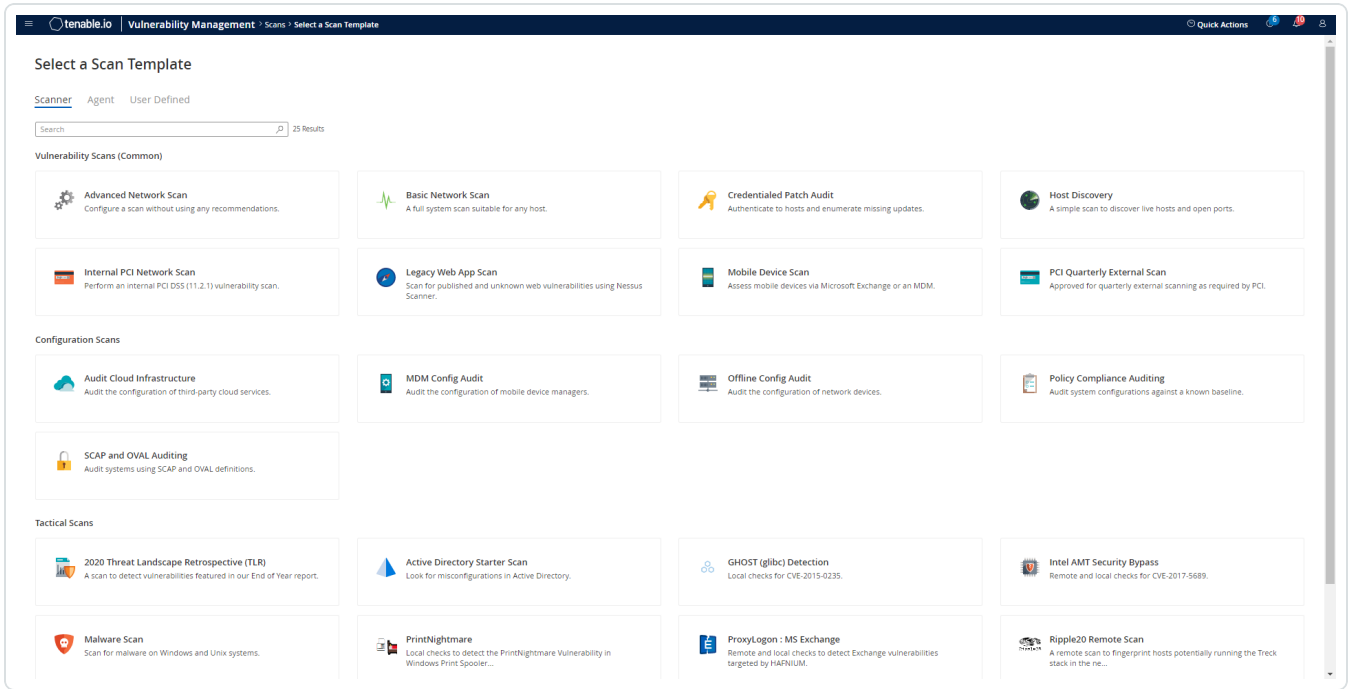
1. Log in to Tenable.io.
2. Click **Scans**.

   The **My Scans** page appears.



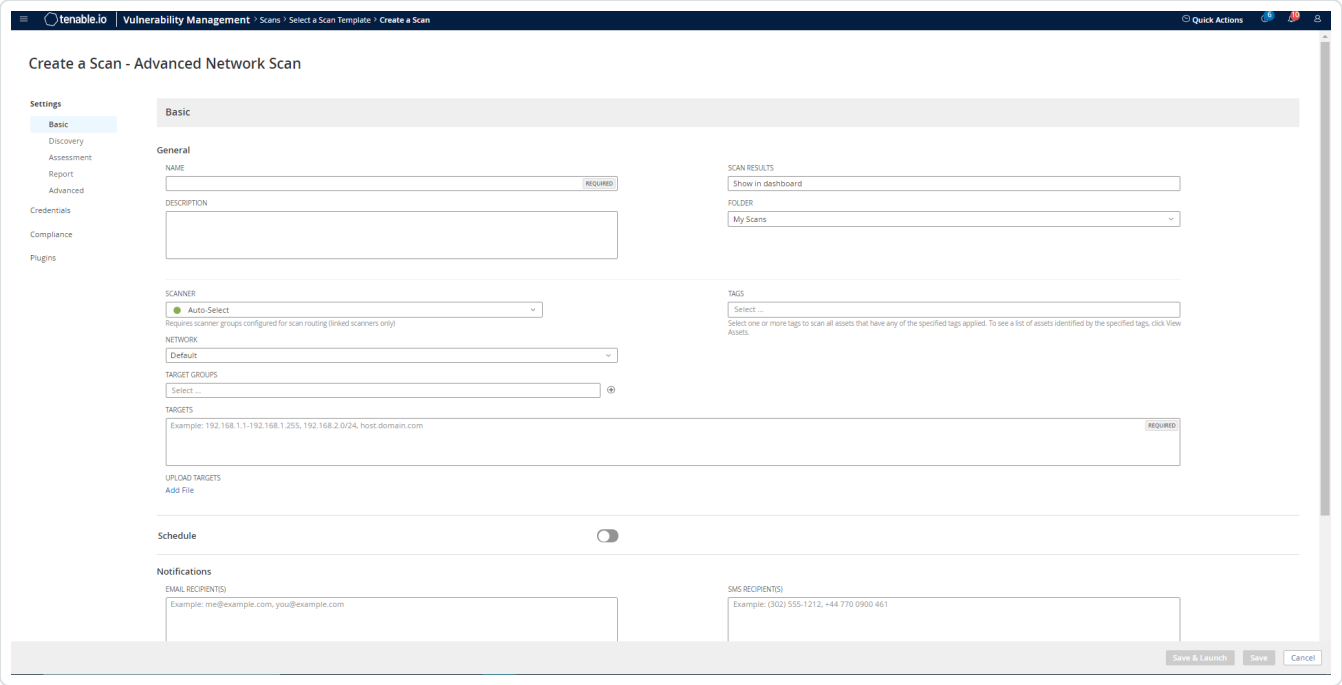
3. Click **+ New Scan.**

   The **Scan Templates** page appears.

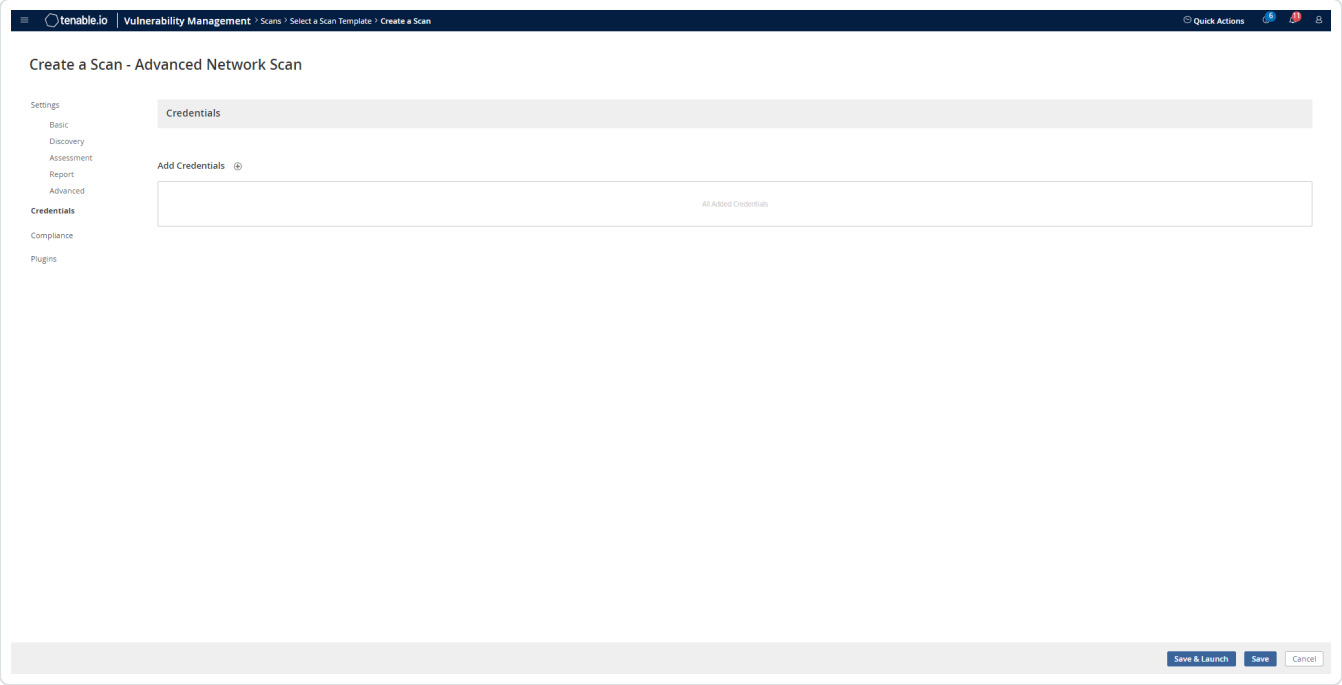


4. Select a **Scan Template**. For demonstration, the **Advanced Network Scan** template is used.

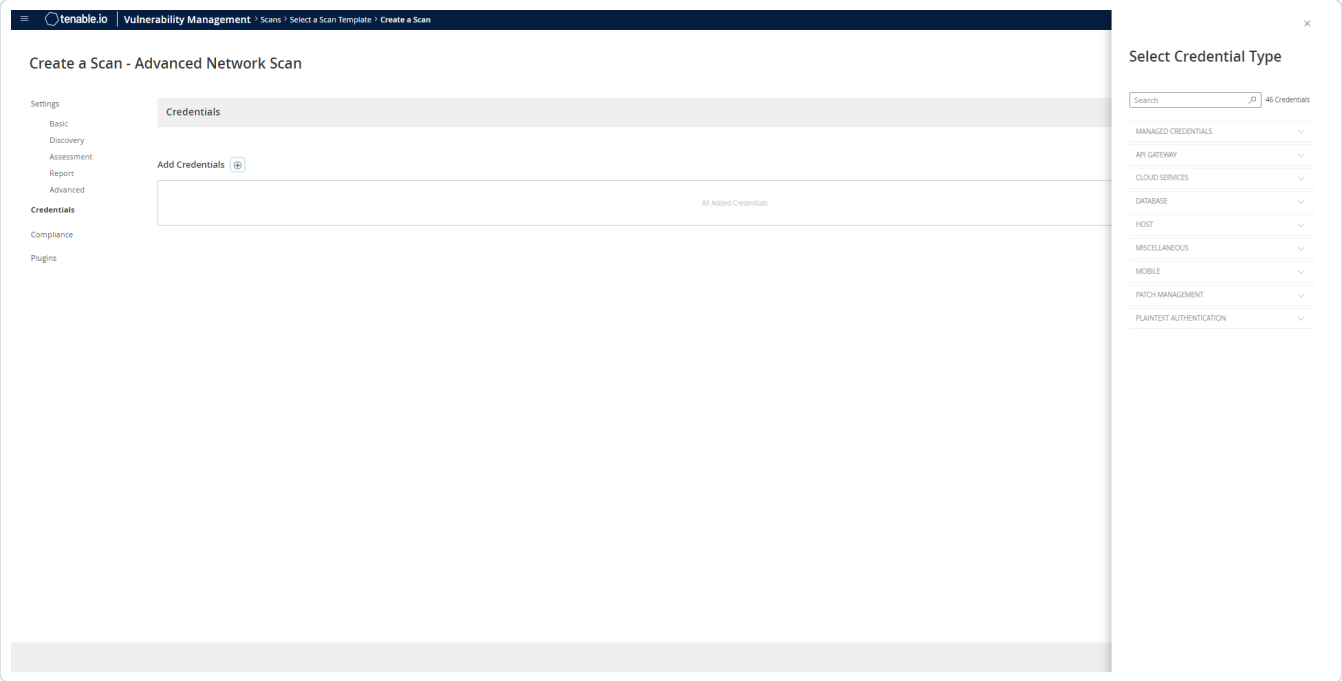
   The scan configuration page appears.



5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
7. (Optional) Add a description, folder location, scanner location, and specify target groups.
8. Click the **Credentials** tab.

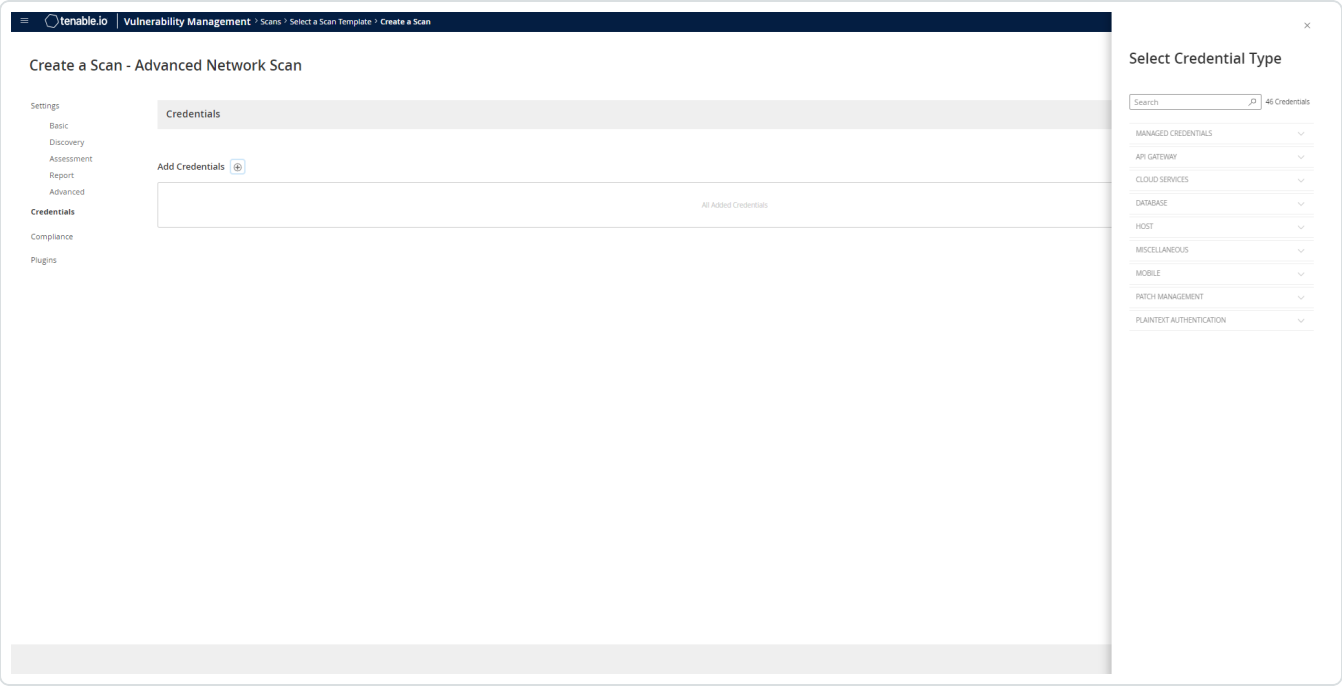


The **Credentials** pane appears.

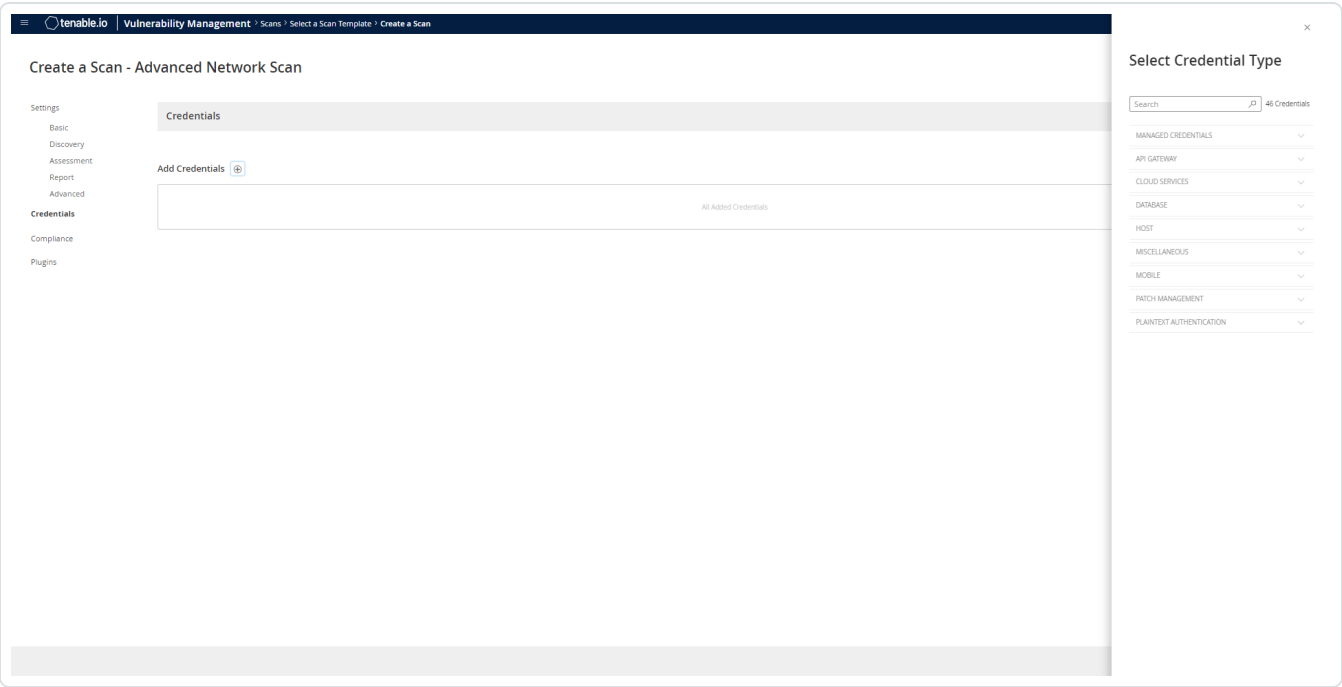


9. Click the **Database** option.

   The **Database** options appear.

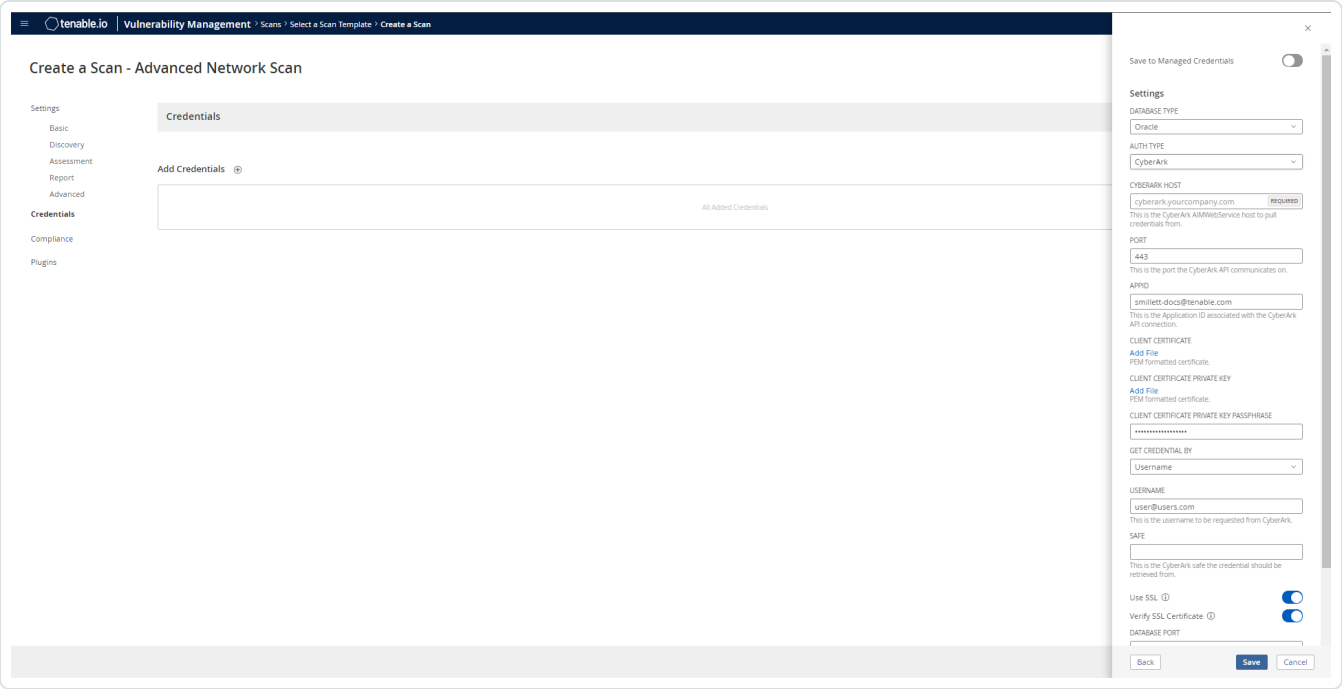


10. From the **Database Type** drop-down, select **Oracle**.



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.	no
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	yes, if private key is applied
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	yes, if private key is applied

Option	Description	Required
Get credential by	The method with which your CyberArk API credentials are retrieved. Can be **Username**, **Identifier**, or **Address**. **Note:** The frequency of queries for **Username** is one query per target. The frequency of queries for **Identifier** is one query per chunk. This feature requires all targets have the same identifier. **Note:** The **Username** option also adds the **Address** parameter of the API query and assigns the target IP of the resolved host to the **Address** parameter. This may lead to failure to fetch credentials if the CyberArk Account Details **Address** field contains a value other than the target IP address.	yes
Username	(If **Get credential by** is **Username**) The username of the CyberArk user to request a password from.	no
Safe	The CyberArk safe the credential should be retrieved from.	no
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 con-	no

Option	Description	Required
	figured to support SSL through IIS and you want to validate the certificate.	

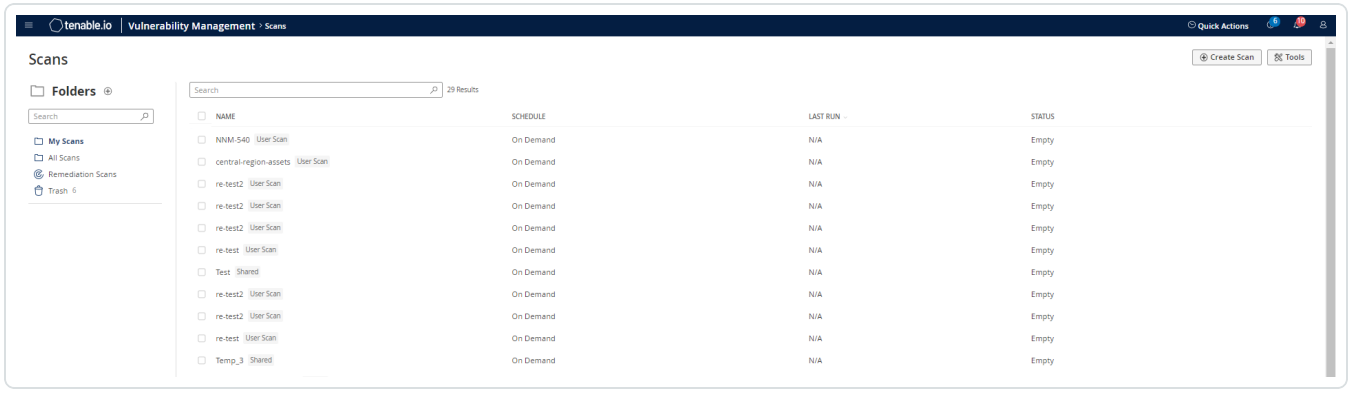
Caution: Tenable strongly recommends encrypting communication between your on-site scanner and the CyberArk AIM gateway using HTTPS and/or client certificates. For information on securing the connection, refer to the Tenable.io User Guide and the **Central Credential Provider Implementation Guide** located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

13. Click **Save**.

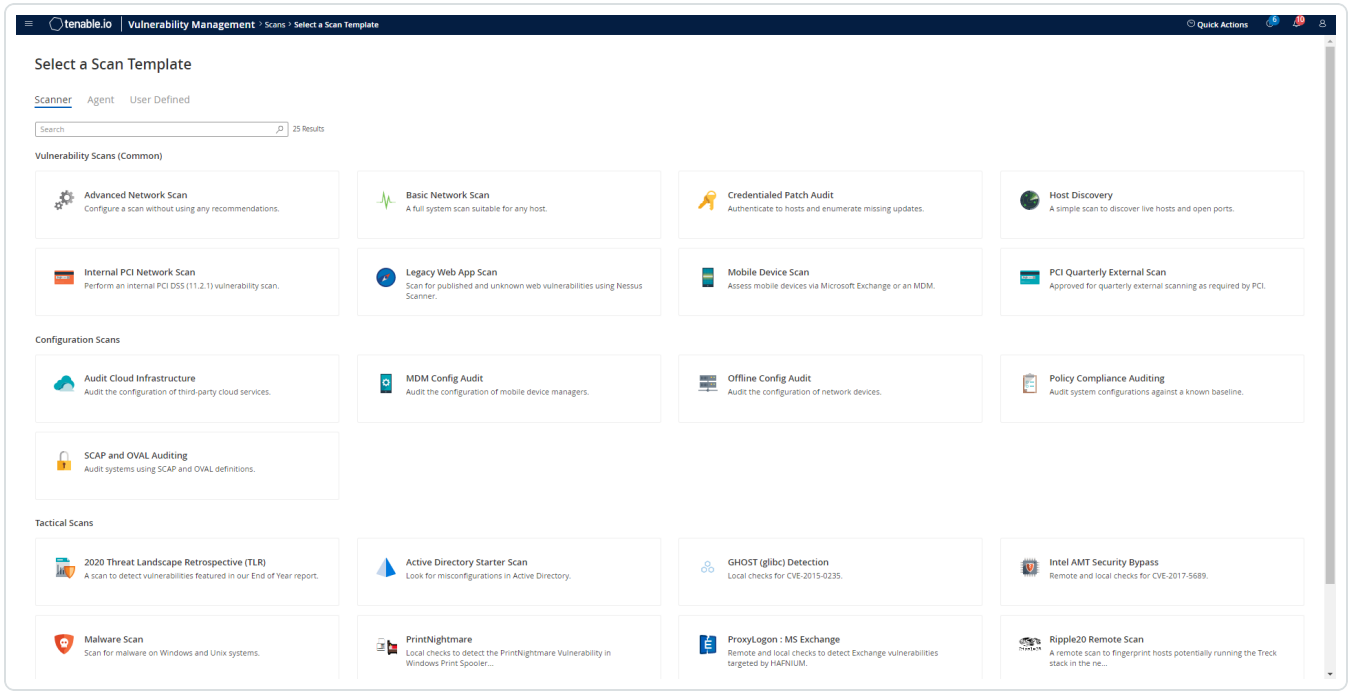
SSH Integration

To configure SSH integration:

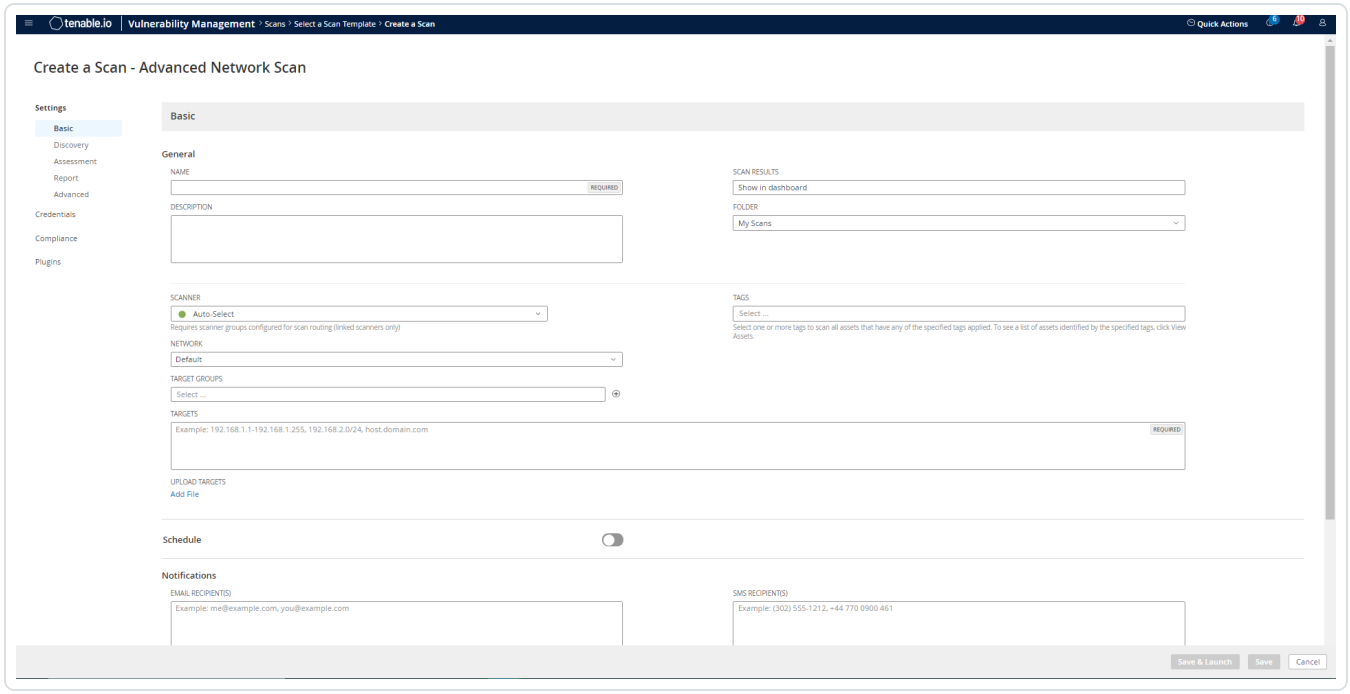
1. Log in to Tenable.io.
2. Click **Scans**.
3. Click **+ New Scan**.



4. Select a **Scan Template**.

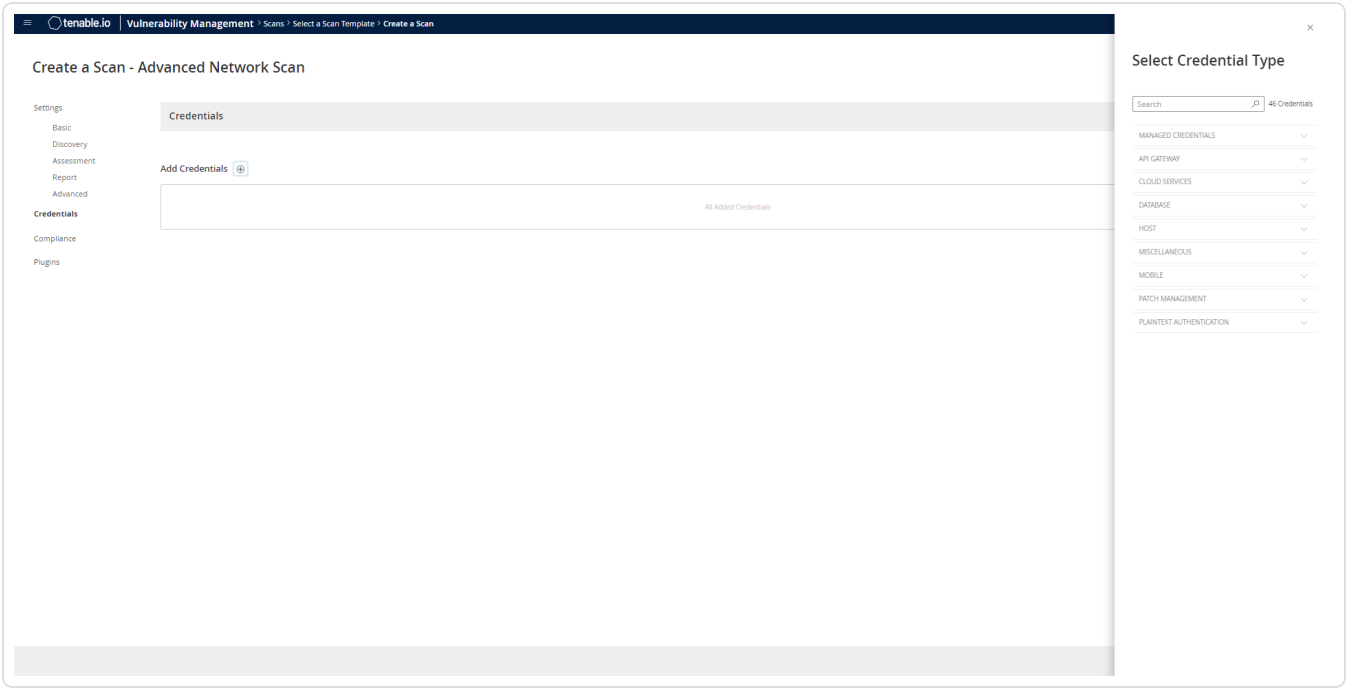


The scan configuration page appears.



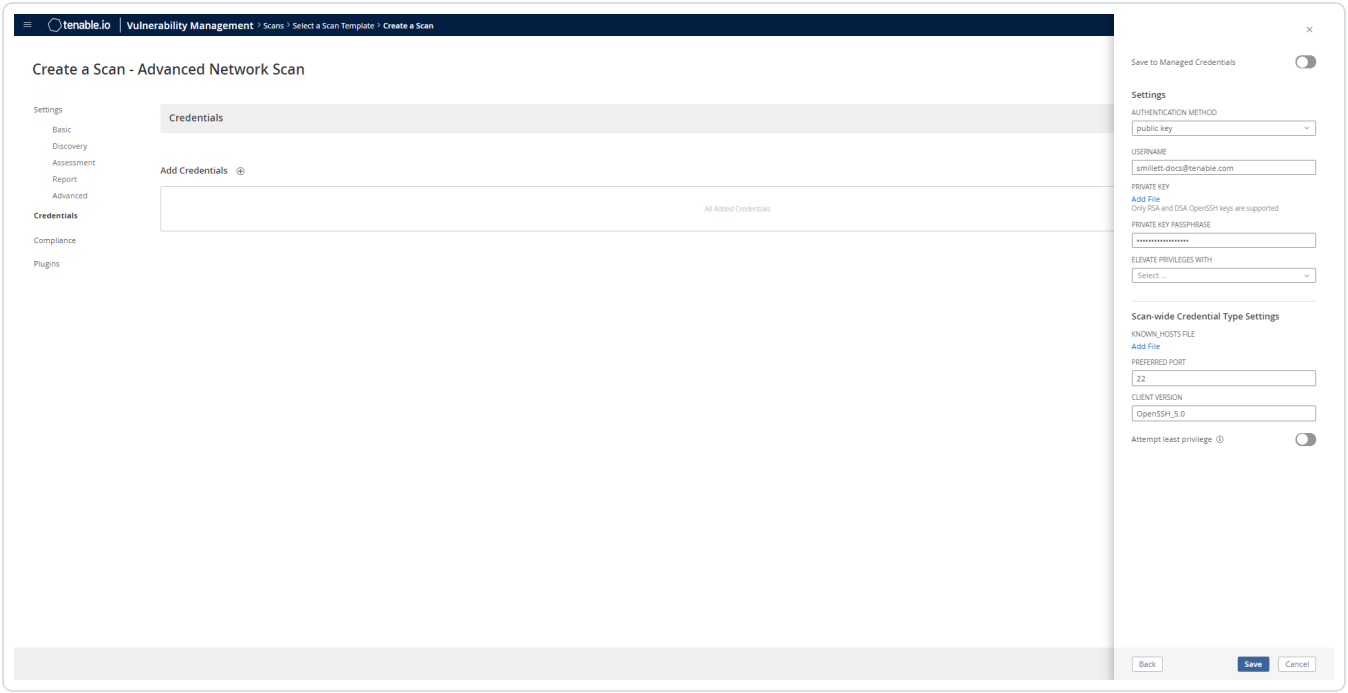
5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
7. (Optional) Add a description, folder location, scanner location, and specify target groups.
8. Click the **Credentials** tab.

   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.	no
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	yes, if private key is applied
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	yes, if private key is applied
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	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	no
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.	no
Realm	(Required if Kerberos Target Authentication	yes

Option	Description	Required
	is enabled.) The Realm is the authentication domain, usually noted as the domain name of the target (for example, example.com). By default, Tenable Vulnerability ManagementTenable Nessus uses 443.	
Get credential by	The method with which your CyberArk API credentials are retrieved. Can be **Username**, **Identifier**, or **Address**. **Note:** The frequency of queries for **Username** is one query per target. The frequency of queries for **Identifier** is one query per chunk. This feature requires all targets have the same identifier. **Note:** The **Username** option also adds the **Address** parameter of the API query and assigns the target IP of the resolved host to the **Address** parameter. This may lead to failure to fetch credentials if the CyberArk Account Details **Address** field contains a value other than the target IP address.	yes
Username	(If **Get credential by** is **Username**) The username of the CyberArk user to request a password from.	no
Safe	The CyberArk safe the credential should be retrieved from.	no
Address	The option should only be used if the Address value is unique to a single CyberArk account credential.	no
Account Name	(If **Get credential by** is **Identifier**) The unique	no

Option	Description	Required
	account name or identifier assigned to the CyberArk API credential.	
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

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

12. Click **Save**.

Verification

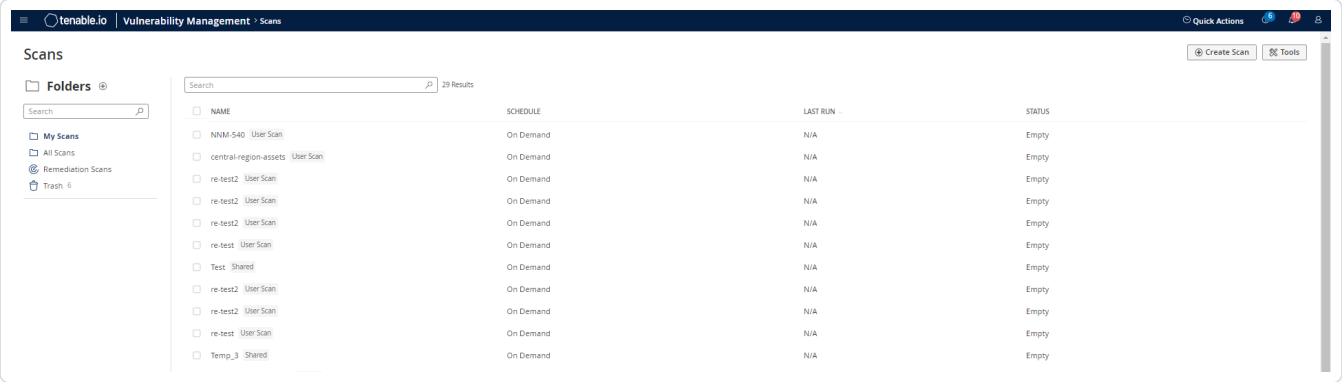
1. To verify the integration is working, click the **launch** button (highlighted below) to initiate an on-demand scan.
2. Once the scan has completed, select the completed scan and look for **Plugin ID 12634**, which validates that authentication was successful. If the authentication is not successful, refer to the Debugging CyberArk Issues section of this document.

Privilege Escalation with CyberArk Credentials

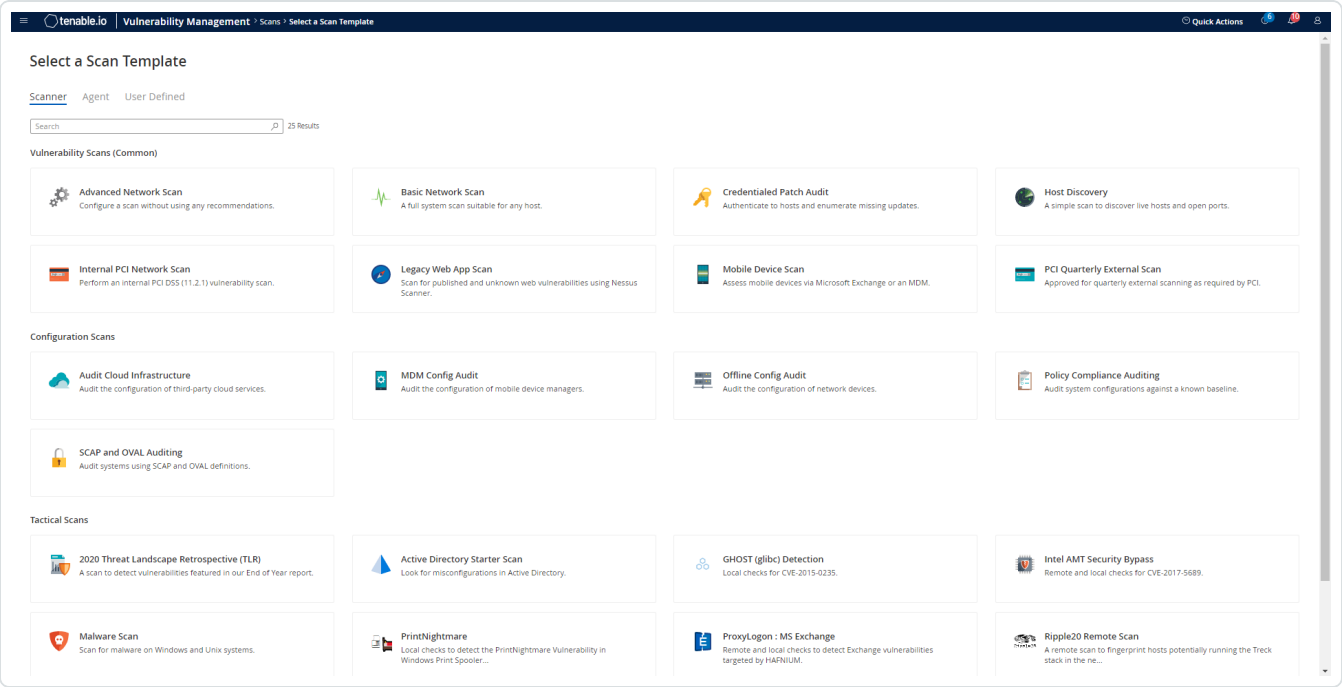
Tenable.io supports the use of privilege escalation, such as *su* and *sudo*, when using SSH through the CyberArk authentication method.

To configure SSH integration:

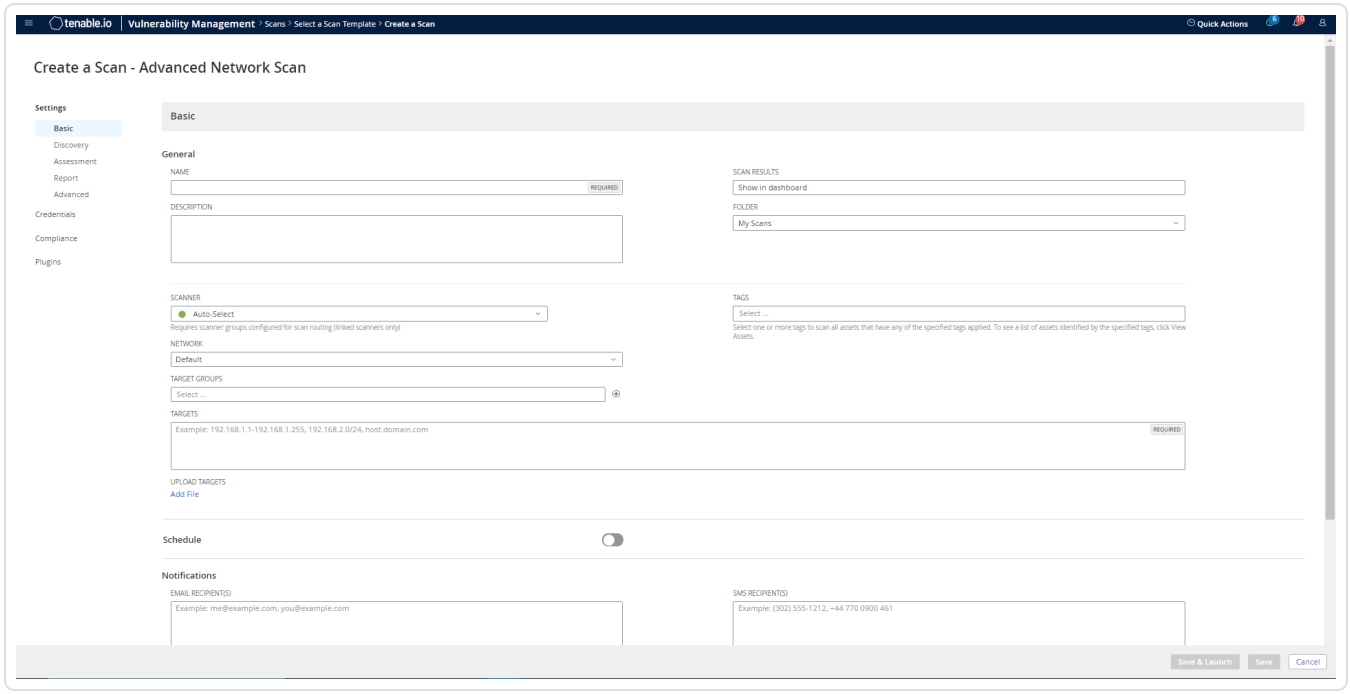
1. Log in to Tenable.io.
2. Click **Scans**.
3. Click **+ New Scan**.



4. Select a **Scan Template**.

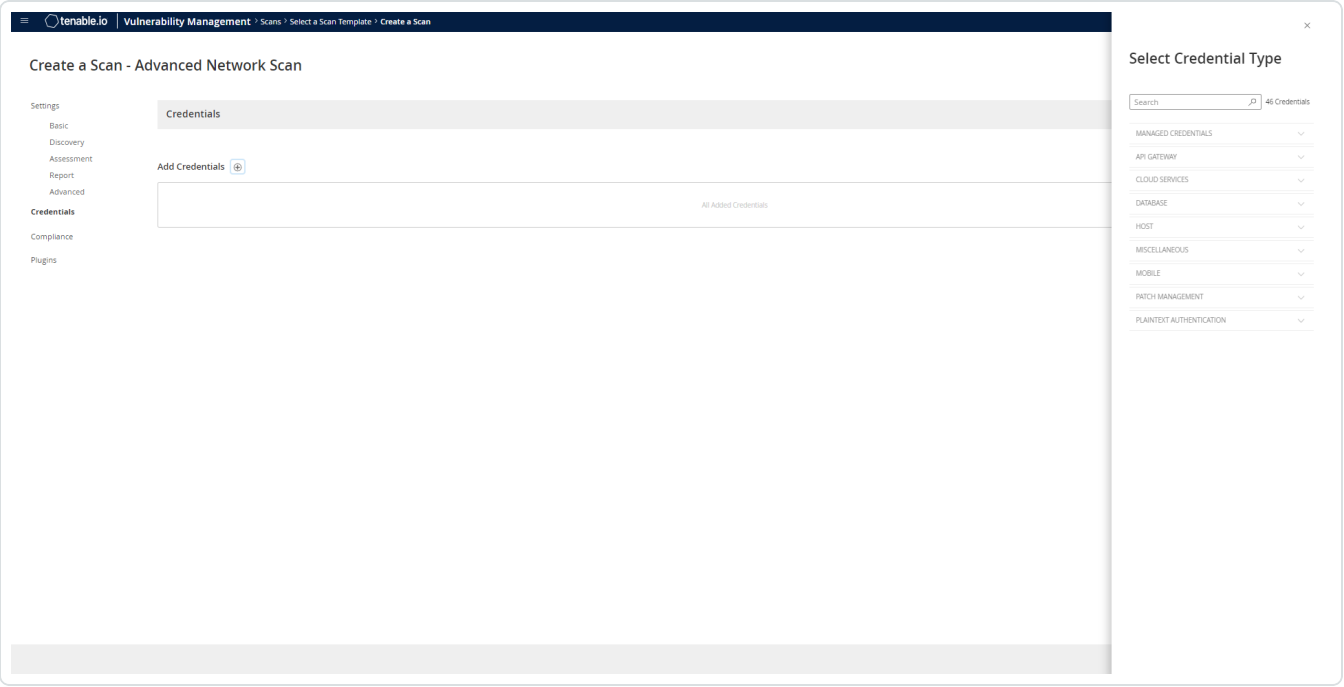


The scan configuration page appears.



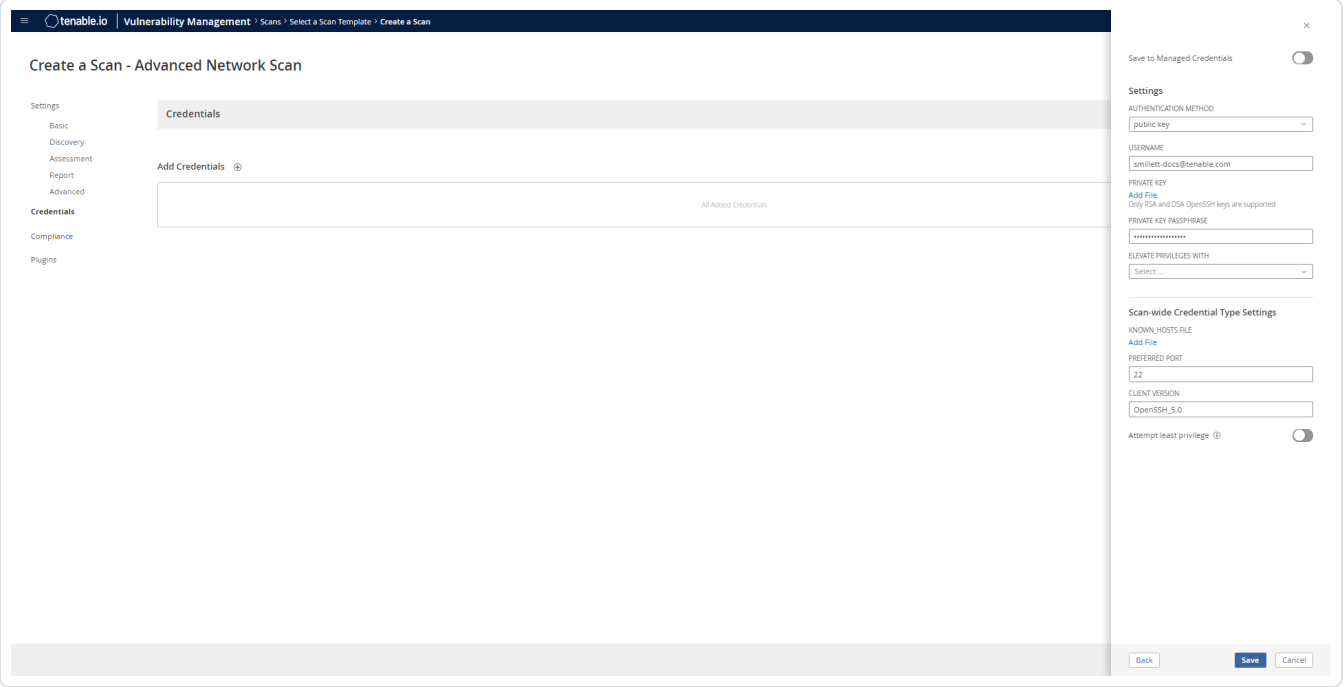
5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
7. (Optional) Add a description, folder location, scanner location, and specify target groups.
8. Click the **Credentials** tab.

   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 **Elevate Privileges With** field.

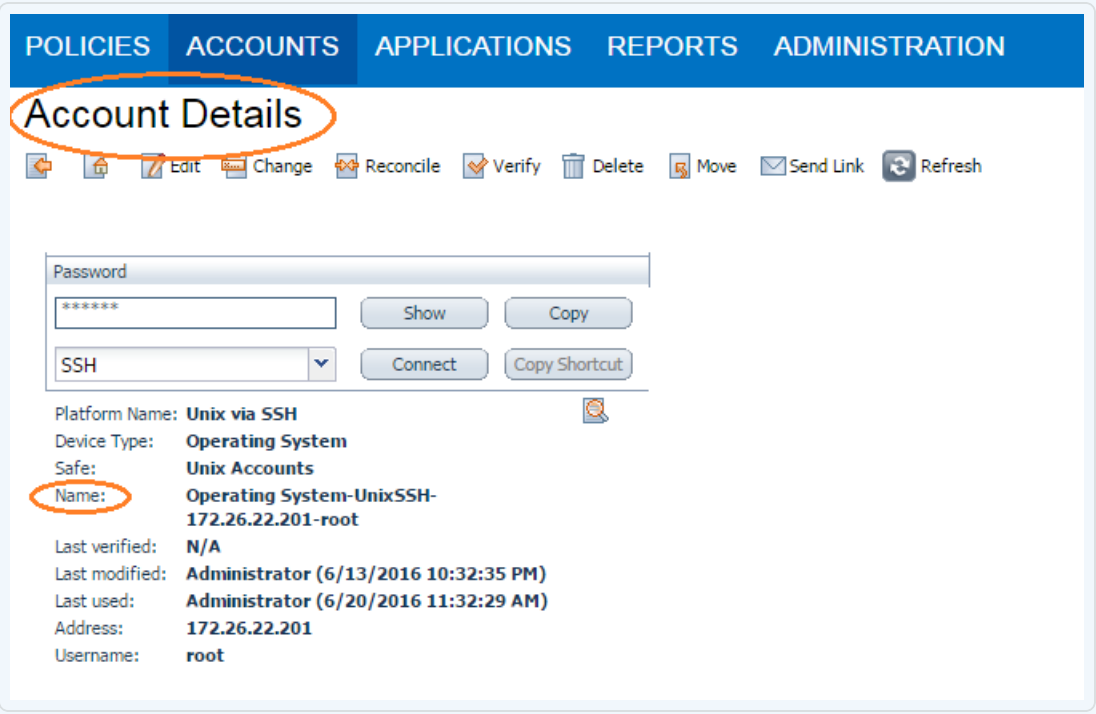
Note: Multiple options for privilege escalation are supported, including *su*, *su+sudo* and *sudo*. For example, if **sudo** is selected, additional fields for **sudo user**, **CyberArk Account Details Name** and **Location of sudo** (directory) are provided and can be completed to support authentication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

Note: The **Username** option for the **Get Credential By** field 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.

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



Windows 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
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

Option	Description	Required
AppID	The Application ID associated with the CyberArk API connection.	yes
Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host.	no
Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	yes, if private key is applied
Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	yes, if private key is applied
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	The port on which the Kerberos authentication API communicates. By default, Tenable uses 88.	no
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.	no
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 **User-**	yes

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

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

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

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.

CyberArk Legacy Integrations

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

To configure database integration:

1. Log in to Tenable.io.
2. Click **Scans**.

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

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

   The scan configuration page appears.
5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
7. (Optional) 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 Cre-	All	The CyberArk Central Credential Pro-	yes

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

Option	Database Types	Description	Required
Private Key Passphrase		requires it.	
CyberArk AppId	All	The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.	yes
CyberArk Folder	All	The folder on the CyberArk Central Credential Provider server that contains the authentication information you would like to retrieve.	no
CyberArk Account Details Name	All	The unique name of the credential you want to retrieve from CyberArk.	yes
PolicyId	All	The PolicyID assigned to the credentials that you want to retrieve from the CyberArk Central Credential Provider.	no
Use SSL	All	If CyberArk Central Credential Provider is configured to support SSL through IIS check for secure communication.	no
Verify SSL Certificate	All	If CyberArk Central Credential Provider is configured to support SSL through IIS and you want to validate the certificate, select this option. Refer to the custom_CA.inc documentation for how to use self-signed certificates.	no
Database Port	All	The port on which Tenable Vulnerability ManagementTenable Secur-	yes

Option	Database Types	Description	Required
		ity Center communicates with the database.	
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
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.io User Guide and the **Central Credential Provider Implementation Guide** located at cyberark.com (login required).

13. Click **Save**.

SSH (Legacy) Integration

To configure SSH integration:

1. Log in to Tenable.io.
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 Vulnerability Management uses `/AIMWebservice/v1.1/AIM.asmx`.	no
Central Credential Provider Host	The CyberArk Central Credential Provider IP/DNS address.	yes

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

Option	Description	Required
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. For more information, see Privilege Escalation.	no
Custom password prompt	The password prompt used by the target host. Only use this setting when an interactive SSH session fails due to Tenable Vulnerability Management receiving an unrecognized password prompt on the target host's interactive SSH shell.	no

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

12. Click **Save**.

Verification

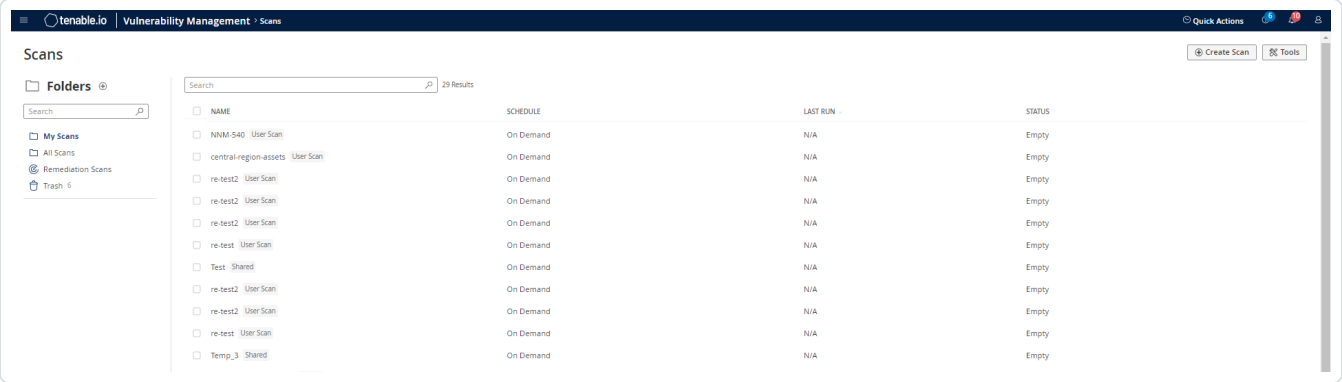
1. To verify the integration is working, click the **launch** button (highlighted below) to initiate an on-demand scan.
2. Once the scan has completed, select the completed scan and look for **Plugin ID 12634**, which validates that authentication was successful. If the authentication is not successful, refer to the Debugging CyberArk Issues section of this document.

Privilege Escalation with CyberArk (Legacy) Credentials

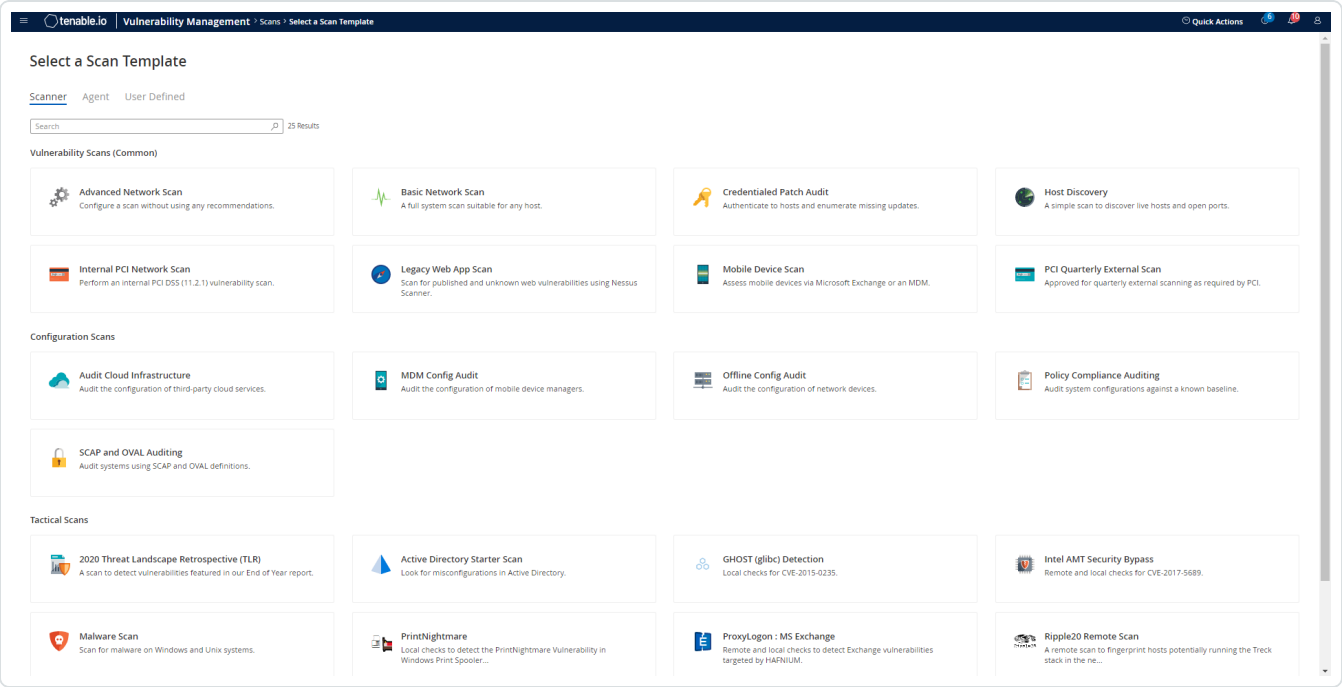
Tenable.io supports the use of privilege escalation, such as *su* and *sudo*, when using SSH through the CyberArk authentication method.

To configure SSH integration:

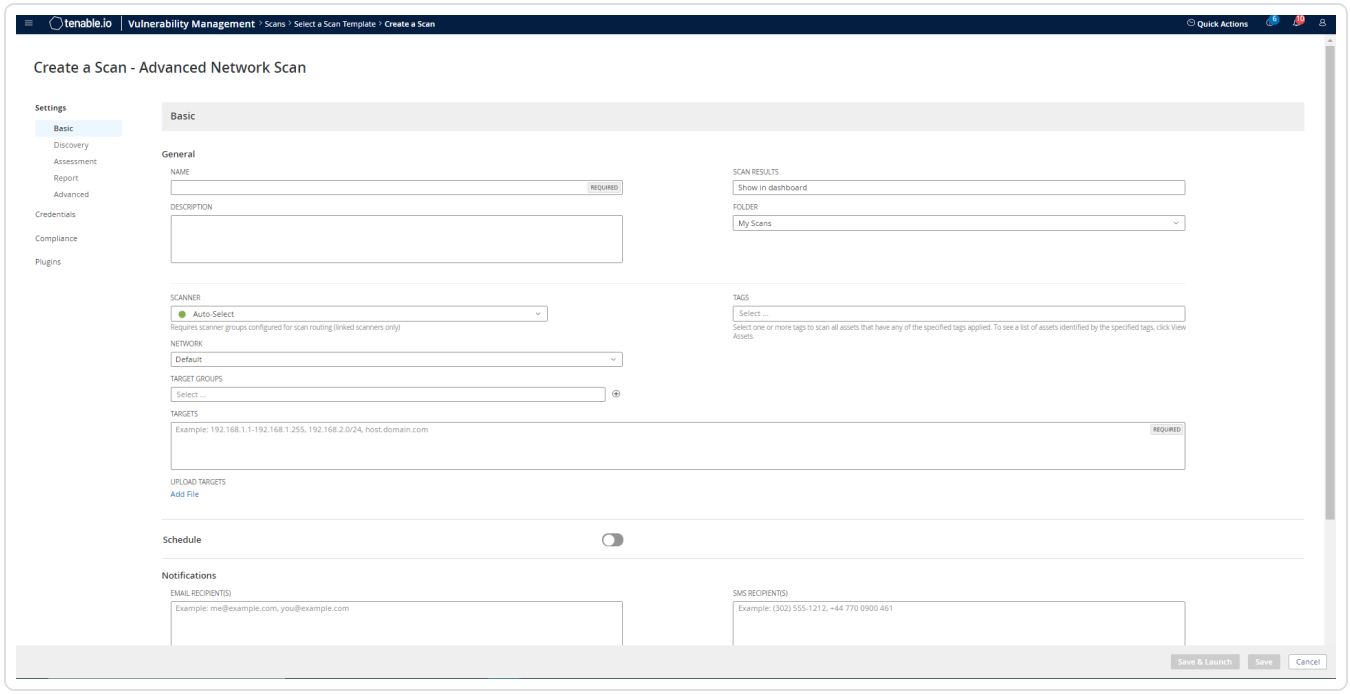
1. Log in to Tenable.io.
2. Click **Scans**.
3. Click **+ New Scan**.



4. Select a **Scan Template**.

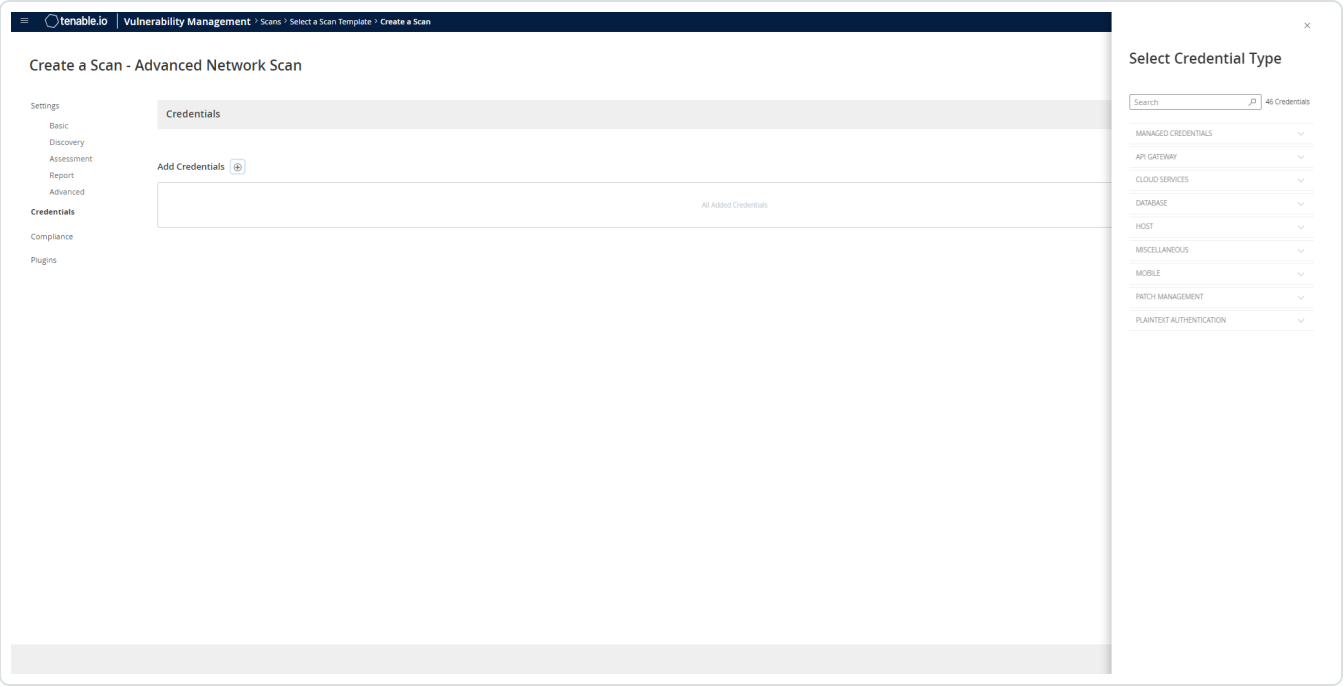


The scan configuration page appears.

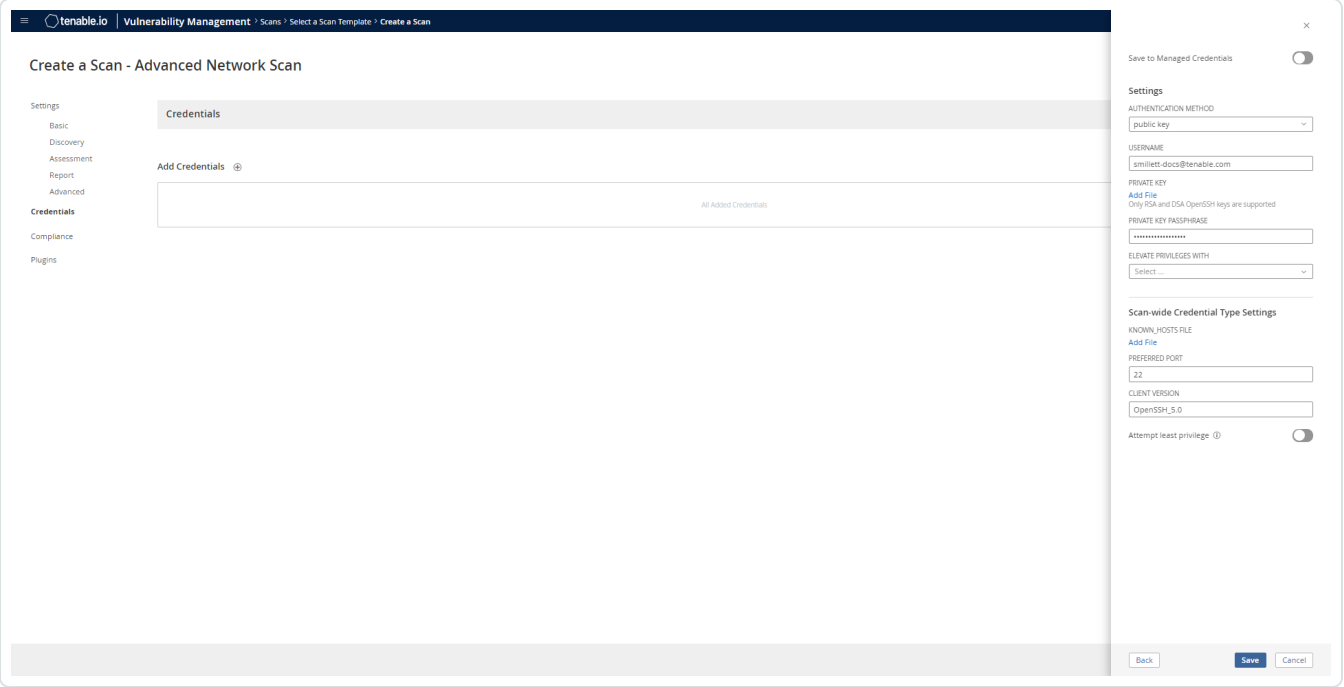


5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
7. (Optional) Add a description, folder location, scanner location, and specify target groups.
8. Click the **Credentials** tab.

   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.**



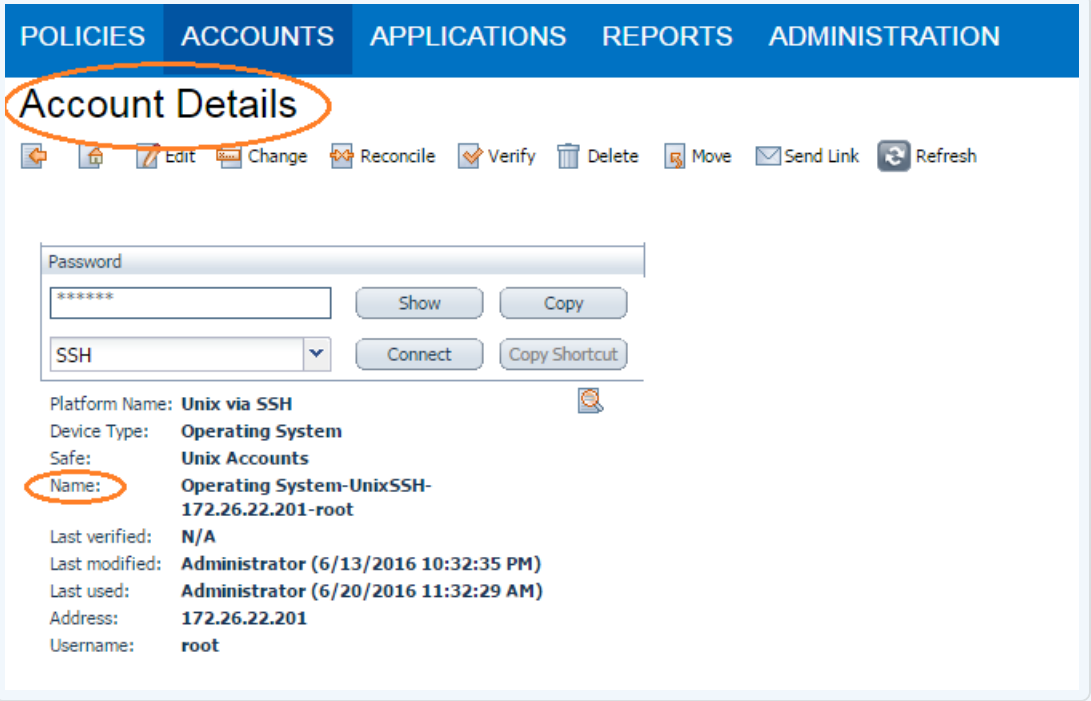
11. Select an option for the **CyberArk Elevate Privileges With** field.

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.io 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 supply 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 Vulnerability Management uses `/AIMWebservice/v1.1/AIM.asmx`.	no
Domain	The domain to which the username belongs.	no

Option	Description	Required
Central Credential Provider Host	The CyberArk Central Credential Provider IP/DNS address.	yes
Central Credential Provider Port	The port on which the CyberArk Central Credential Provider is listening.	yes
Central Credential Provider Username	The username of the vault, if the CyberArk Central Credential Provider is configured to use basic authentication.	no
Central Credential Provider Password	The password of the vault, if the CyberArk Central Credential Provider is configured to use basic authentication.	no
Safe	The safe on the CyberArk Central Credential Provider server that contained the authentication information that you want to retrieve.	yes
CyberArk Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host.	no
CyberArk Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	no
CyberArk Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	no
AppId	The AppId that has been allocated permissions on the CyberArk Central Credential Provider to retrieve the target password.	yes

Option	Description	Required
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

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

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.io Priority Scanning for CyberArk

Retrieving Addresses to Scan from CyberArk

Debugging CyberArk Issues

CyberArk Domain and DNS Support

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

Tenable.io Priority Scanning for CyberArk

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

1. Tenable.io will query CyberArk with the target value entered into the Tenable.io **Targets** configuration field. For example, if you put a FQDN in the target list, Tenable.io will query CyberArk with the address value of the FQDN. If you enter an IP address or range such as 192.0.2.1-20, Tenable.io will try to query using the IP address or IP range of the target system(s) in the CyberArk **Address** value. If the target system uses FQDN and can be resolved, then it will be contacted.
2. If the target value fails, Tenable.io will then look to see if there is a domain value (for a Windows system). If a domain value is present, Tenable.io will query CyberArk using the domain value for the address value to attempt to use domain credentials.
3. If the configured target value and the domain value both fail, Tenable.io will then pull the IP address of the system. If the IP address does not match one of the IP addresses supplied in the target list, Tenable.io will then query CyberArk using the IP address of the target itself. This is checked against the target value in the configuration to prevent querying CyberArk twice with the same value.

Debugging CyberArk

To enable debugging when you configure a scan in Tenable.io, go to **Settings->Advanced->Debug Settings** and Check **Enable plugin debugging**. If an issue is found, review the results of plugin **Debugging Log Report** (84239). If debug output for the system exists in the debug log, one or more of the following files will be present:

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

Example of output:

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

```
Safe=Unix Accounts;Folder=Root;Object=Operating System-WinDesktopLocal-
192.0.2.66-admin and more. See trace log for more information). (Diagnostic
Info: 41)
```

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

Retrieving Addresses to Scan from CyberArk

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

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

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

About Tenable

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