Tenable and CyberArk Secrets Manager Integration Guide

Last Revised: January 16, 2026

Table of Contents

Welcome to Tenable for CyberArk Secrets Manager

This document provides information and steps for integrating Tenable Vulnerability Management or Tenable Nessus with CyberArk Secrets Manager.

The Tenable CyberArk Secrets Manager integration provides scans the ability to use credentials from the CyberArk Secrets Manager in credentialed scans. This is useful for the management of credentials in credentialed scanning and provides an improved view of cyber exposure.

Please note that the CyberArk Secrets Manager product was previously known as CyberArk Conjur.

What information does the CyberArk Secrets Manager integration collect?

The integration gathers target credentials for use in credentialed scans. For example, it may gather usernames, passwords, or 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.

Configure a Tenable Vulnerability Management Scan

Required User Role: Standard, Scan Manager, or Administrator

Before you begin:

- You must create a CyberArk Secrets Manager workload with API key authentication which has read access to the secrets you plan to use.

To configure scans:

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. Select a credential with support for CyberArk Secrets Manager as an authentication type. For example, SSH, Windows or SNMP (in the Host category), or Database, Nutanix Prism Central, VMware vCenter API or VMware ESXi SOAP API.

   The **Settings** options appear.
10. In the Authentication Type drop-down box, click **CyberArk Secrets Manager**.

The CyberArk Secrets Manager options appear.

11. Configure each option for the CyberArk Secrets Manager authentication type.

Option	Description	Required
CyberArk Secrets Manager Host	The CyberArk Secrets Manager IP address or DNS address.	Yes
CyberArk Secrets Manager Port	The port on which the CyberArk API communicates. By default, Tenable uses 443.	Yes
CyberArk Secrets Manager Login Name	The login name used to authenticate to CyberArk Secrets Manager. For workload (host) authentication, it is the workload (host) ID with the prefix `host/`. For example, a host `data/MyWorkload` would use `host/data/MyWorkload`.	Yes
CyberArk Secrets Manager API Key	The API key of the workload or login.	Yes
CyberArk Secrets Manager Authentication Base URL	This value is combined with the login name to form the authentication API endpoint. The default value is `/api/authn/conjur`. For example, a secret ID of MySecret and vault path of variable/data/vault/MyVault would result in the following request endpoint: `/api/secrets/conjur/variable/data/vault/MyVault/MySecret`	No
CyberArk	The kind of resource which contains the secret. In most	Yes

Option	Description	Required
Secrets Manager Kind	configurations, this should be the literal string `variable`.	
CyberArk Secrets Manager Credential ID	This is the unique identifier of the Secrets Manager variable which contains the credential. In most configurations, this value should begin with data/ It may include the path to the CyberArk Vault as well. For example, to retrieve a secret named MySecret from the vault named `MyVault`, use: `data/vault/MyVault/MySecret`	Yes
Domain	Windows Only: the domain to use for authentication.	Required if Kerberos is enabled.
Fetch Domain	Windows Only: pull the value of the Windows domain from the CyberArk Secrets Manager API.	No
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified target.	No
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled.) This host supplies the session tickets for the user.	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,	No

Option	Description	Required
	depending on the implementation.	
Realm	(Required if Kerberos Target Authentication is enabled.) SSH Only: the realm to use for Kerberos authentication.	Yes
SSL	Use SSL for secure communications.	Yes
Verify SSL Certificate	Validate the SSL certificate. Recommended.	No

12. Click **Save**.

Configure a Tenable Nessus Scan

Required User Role: Standard, Scan Manager, or Administrator

Before you begin:

- You must create a CyberArk Secrets Manager workload with API key authentication which has read access to the secrets you plan to use.

To configure scans:

1. Log in to Tenable Nessus.
2. In the upper-right corner, click **+ New Scan.**

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

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

   The **Credentials** pane appears.
8. Select a credential with support for CyberArk Secrets Manager as an authentication type. For example, SSH, Windows or SNMP (in the Host category), or Database, Nutanix Prism Central, VMware vCenter API or VMware ESXi SOAP API.

   The **Settings** options appear.
9. In the Authentication Type drop-down box, click **CyberArk Secrets Manager**.

   The CyberArk Secrets Manager options appear.
10. Configure each option for the CyberArk Secrets Manager authentication type.

Option	Description	Required
CyberArk Secrets Manager Host	The CyberArk Secrets Manager IP address or DNS address.	Yes
CyberArk Secrets Manager Port	The port on which the CyberArk API communicates. By default, Tenable uses 443.	Yes
CyberArk Secrets Manager Login Name	The login name used to authenticate to CyberArk Secrets Manager. For workload (host) authentication, it is the workload (host) ID with the prefix `host/`. For example, a host `data/MyWorkload` would use `host/data/MyWorkload`.	Yes
CyberArk Secrets Manager API Key	The API key of the workload or login.	Yes
CyberArk Secrets Manager Authentication Base URL	This value is combined with the login name to form the authentication API endpoint. The default value is `/api/authn/conjur`. For example, a secret ID of MySecret and vault path of variable/data/vault/MyVault would result in the following request endpoint: `/api/secrets/conjur/variable/data/vault/MyVault/MySecret`	No
CyberArk Secrets Manager Kind	The kind of resource which contains the secret. In most configurations, this should be the literal string `variable`.	Yes

Option	Description	Required
CyberArk Secrets Manager Credential ID	This is the unique identifier of the Secrets Manager variable which contains the credential. In most configurations, this value should begin with data/ It may include the path to the CyberArk Vault as well. For example, to retrieve a secret named MySecret from the vault named `MyVault`, use: `data/vault/MyVault/MySecret`	Yes
Domain	Windows Only: the domain to use for authentication.	Required if Kerberos is enabled.
Fetch Domain	Windows Only: pull the value of the Windows domain from the CyberArk Secrets Manager API.	No
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified target.	No
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled.) This host supplies the session tickets for the user.	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.	No
Realm	(Required if Kerberos Target Authentication is enabled.) SSH Only: the realm to use for Kerberos authentication.	Yes

Option	Description	Required
SSL	Use SSL for secure communications.	Yes
Verify SSL Certificate	Validate the SSL certificate. Recommended.	No

11. Click **Save**.

Configure a Tenable Security Center Scan

Required User Role: Standard, Scan Manager, or Administrator

Before you begin:

- You must create a CyberArk Secrets Manager workload with API key authentication which has read access to the secrets you plan to use.

To configure a scan:

1. Log in to Tenable Security Center.
2. Click **Scanning > Credentials** (administrator users) or **Scans > Credentials** (organizational users).

   The **Credentials** pane appears.
3. Click **Add**.

   The Credential Templates page appears.
4. Select CyberArk Secrets Manager under the specific authentication type you wish to configure (for example, SSH or Windows).

   The Add Credentials configuration page appears.
5. In the Name box, type a name for the credentials.
6. In the Description box, type a description for the credentials.
7. (Optional) Type or select a Tag. For more information, refer to Asset Tags in the *Tenable Security Center User Guide*.
8. Configure each option for the CyberArk Secrets Manager authentication type.

Option	Description	Required
CyberArk Secrets Manager Host	The CyberArk Secrets Manager IP address or DNS address.	Yes

Option	Description	Required
CyberArk Secrets Manager Port	The port on which the CyberArk API communicates. By default, Tenable uses 443.	Yes
CyberArk Secrets Manager Login Name	The login name used to authenticate to CyberArk Secrets Manager. For workload (host) authentication, it is the workload (host) ID with the prefix `host/`. For example, a host `data/MyWorkload` would use `host/data/MyWorkload`.	Yes
CyberArk Secrets Manager API Key	The API key of the workload or login.	Yes
CyberArk Secrets Manager Authentication Base URL	This value is combined with the login name to form the authentication API endpoint. The default value is `/api/authn/conjur`.	No
CyberArk Secrets Manager Secret Base URL	This value is combined with the login name to form the authentication API endpoint. The default value is `/api/authn/conjur`. For example, a secret ID of MySecret and vault path of variable/data/vault/MyVault would result in the following request endpoint: `/api/secrets/conjur/variable/data/vault/MyVault/MySecret`	No
CyberArk Secrets Manager	The kind of resource which contains the secret. In most configurations, this should be the literal string `variable`.	Yes

Option	Description	Required
Kind		
CyberArk Secrets Manager Credential ID	This is the unique identifier of the Secrets Manager variable which contains the credential. In most configurations, this value should begin with data/ It may include the path to the CyberArk Vault as well. For example, to retrieve a secret named MySecret from the vault named `MyVault`, use: `data/vault/MyVault/MySecret`	Yes
Domain	Windows Only: the domain to use for authentication.	Required if Kerberos is enabled.
Fetch Domain	Windows Only: pull the value of the Windows domain from the CyberArk Secrets Manager API.	No
Kerberos Target Authentication	If enabled, Kerberos authentication is used to log in to the specified target.	No
Key Distribution Center (KDC)	(Required if Kerberos Target Authentication is enabled.) This host supplies the session tickets for the user.	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.	No
Realm	(Required if Kerberos Target Authentication is enabled.)	Yes

Option	Description	Required
	SSH Only: the realm to use for Kerberos authentication.	
SSL	Use SSL for secure communications.	Yes
Verify SSL Certificate	Validate the SSL certificate. Recommended.	No

9. Click **Save**.

Scan Results Review

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

Plugin Families and Plugins

The CyberArk Secrets Manager authentication 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 Secrets Manager authentication are:

- **Windows (SMB):** 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

Debug Log Reporting

To find debug logs specific to the CyberArk Secrets Manager, look for logs within the Debugging Log Report plugin output. The plugin output contains debugging logs for the Nessus plugins, including the respective settings plugins which use the CyberArk integration. You will see logs in the debug log reporting for the associated plugin with **~CyberArk Secrets Manager** appended to it. For example, for SSH settings, debugging logs are found in `ssh_settings.nasl~CyberArk`.

The debug logs for CyberArk 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 API key
- Incorrect value given for base URL, vault path or object ID

- Scanner unable to connect to CyberArk API
- Incorrect permissions

CyberArk Integration Helpful Tips

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

- Tenable Vulnerability Management or Tenable Security Center pass the policy and credential values down to Tenable Nessus. This includes values like the CyberArk host, port, object identifier, and client certificates.
- The Tenable 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.

Testing Connectivity with curl

Customers may test connectivity and API functionality using the curl command. CyberArk also documents curl commands in the Secrets Manager Documentation:

- Secrets Manager (Self-Hosted) REST APIs
- Secrets Manager SaaS REST APIs

This section contains two example commands, one to test login and one to test fetching a secret. The commands require substituting in site-specific values such as host, port and API key. Refer to the scan configuration section for additional detail on these values.

Authentication

```
curl -s -X POST -d API_KEY -H 'Accept-Encoding: base64'
https://HOST:PORT/AUTH_BASE_URL/LOGIN_NAME/authenticate
```

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

Value	Replacement
API_KEY	The API key of the workload.
HOST	The secrets manager host
PORT	The secrets manager port.

`AUTH_BASE_URL`	The authentication base URL.
`LOGIN_NAME`	The login name or workload.

For example, a CyberArk Secrets Manager SaaS configuration using a workload named “MyWorkload” would use:

```
curl -s -X POST -d API_KEY -H 'Accept-Encoding: base64'
https://CUSTOMER.secretsmgr.cyberark.cloud:443/api/authn/conjur/host%2Fdata%2FMyWorkload/authenticate
```

If successful, this command outputs a token which should be used in the next command.

Retrieve Secret

After authenticating, retrieve a secret from CyberArk Secrets Manager.

```
$ curl -X GET -H 'Content-Type: application/json' -H 'Authorization: Token token="TOKEN"'
https://HOST:PORT/BASE_URL/variable/CREDENTIAL_ID/password
```

Substitute the following values:

Value	Replacement
`API_KEY`	The API key of the workload.
`HOST`	The secrets manager host
`PORT`	The secrets manager port.
`AUTH_BASE_URL`	The authentication base URL.
`LOGIN_NAME`	The login name or workload.

For example, a CyberArk Secrets Manager SaaS configuration that uses “Conjur Sync” would use the following command to fetch an account named UnixSSH-MyHost from the vault MyVault:

```
$ curl -X GET -H 'Content-Type: application/json' -H 'Authorization: Token token="TOKEN"'
https://CUSTOMER.secretsmgr.cyberark.cloud:443/api/secrets/conjur/variable/data/vault/MyVault/UnixSS
H-MyHost/password
```

If successful, this command displays the password for `UnixSSH-MyHost`.