How-to Guide: Nessus® for CyberArk

Last Updated: February 11, 2020

Table of Contents

Welcome to Nessus for CyberArk

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

Security administrators utilize CyberArk to access and manage usernames, passwords, and privileges. By integrating CyberArk with Nessus Manager, customers have more choice and flexibility.

The benefits of integrating Nessus Manager with CyberArk include:

- Credential updates directly in Nessus Manager.
- Reduced time and effort documenting where credentials are stored in the organizational environment.
- Automatic enforcement of security policies in specific departments or business unit requirements, simplifying compliance.
- Reduced risk of unsecured privileged accounts and credentials across the enterprise.

Integrating With CyberArk Enterprise Password Vault

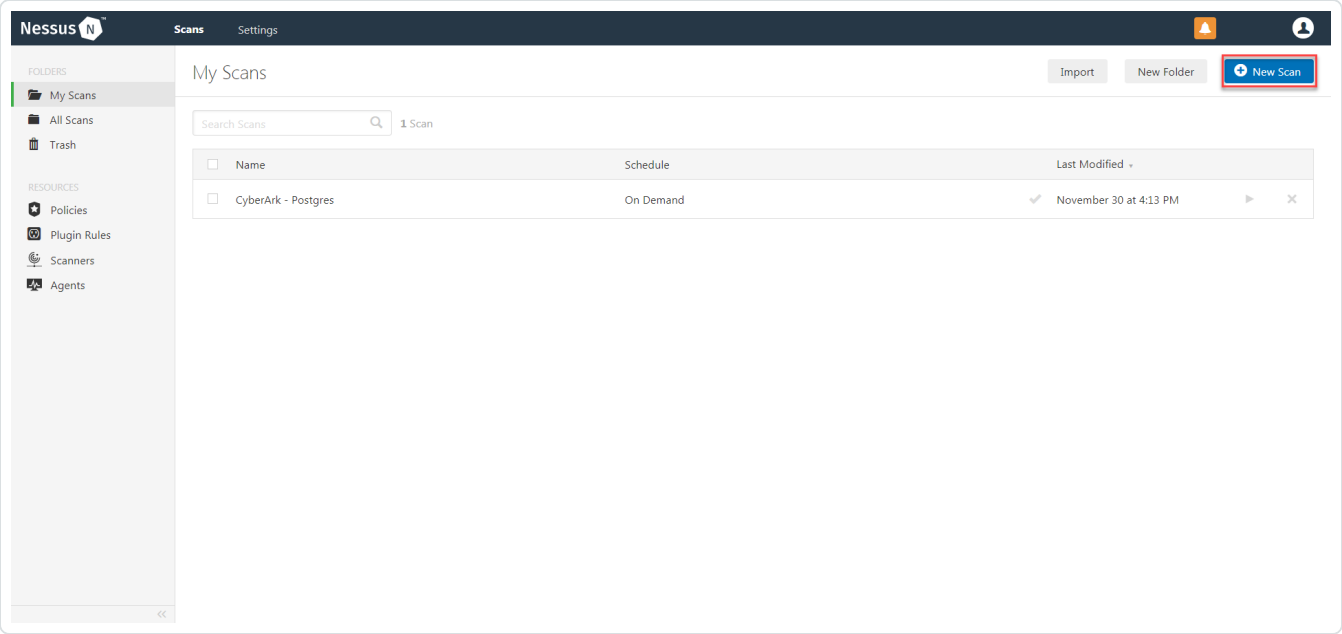
Nessus Manager provides an option for CyberArk Windows integration. Complete the following steps to configure Nessus Manager with CyberArk for Windows.

Requirements:

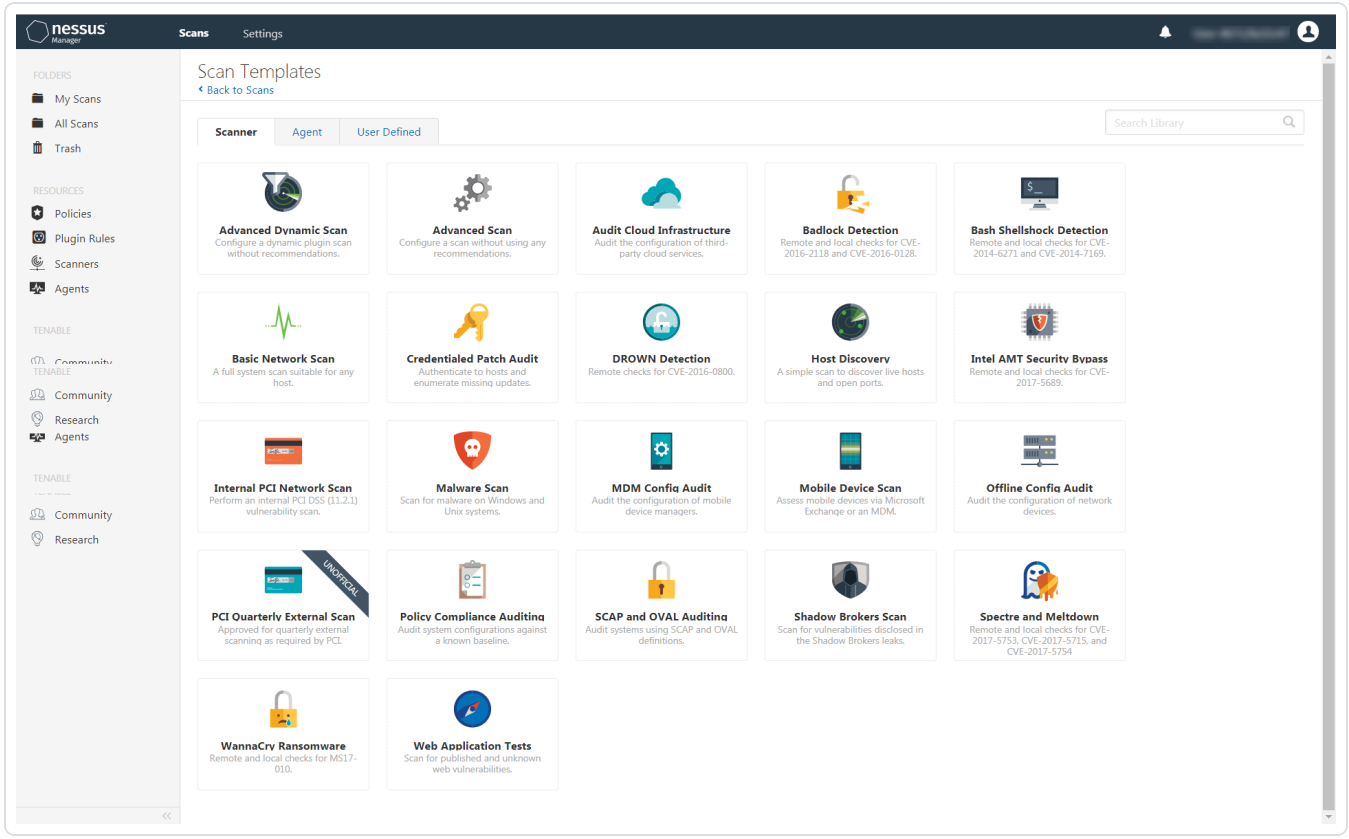
- CyberArk account
- Nessus Manager account

To configure Windows integration:

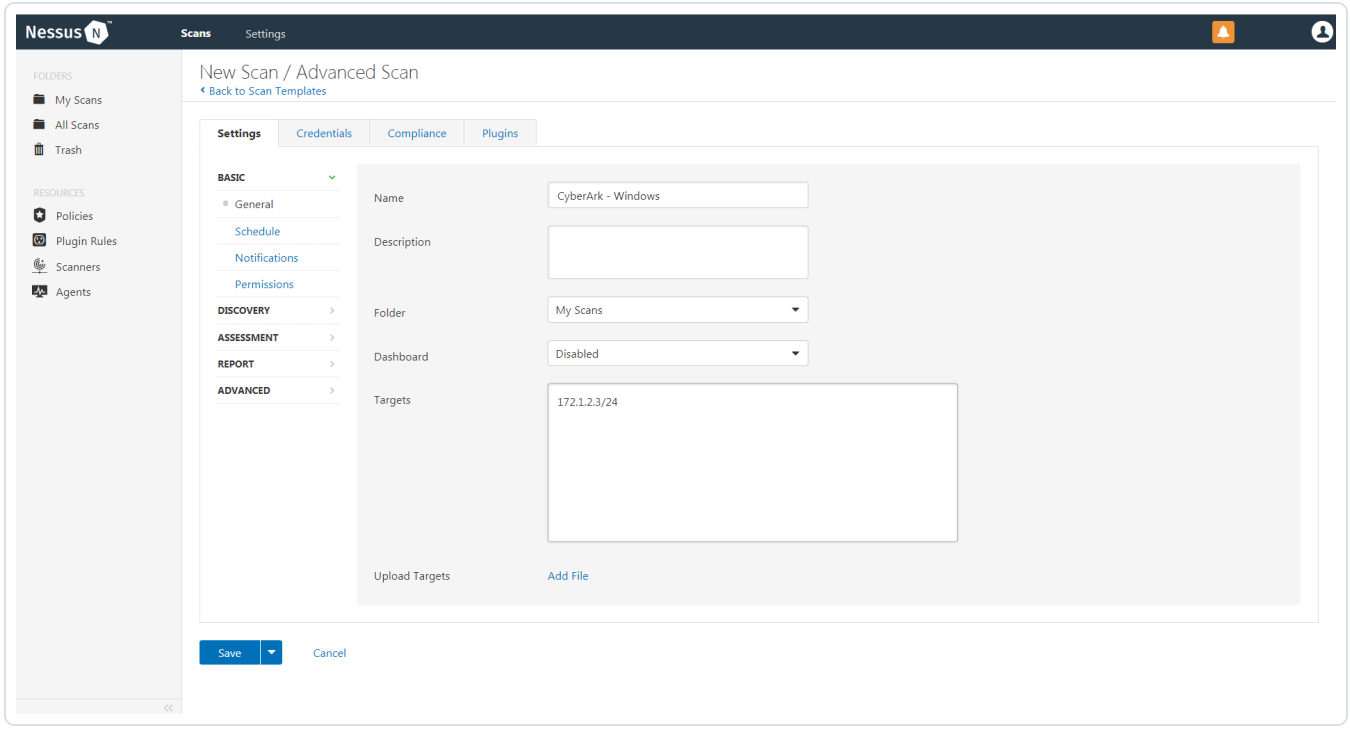
1. Log in to Nessus.
2. Click **Scans**.
3. Click **+ New Scans**.



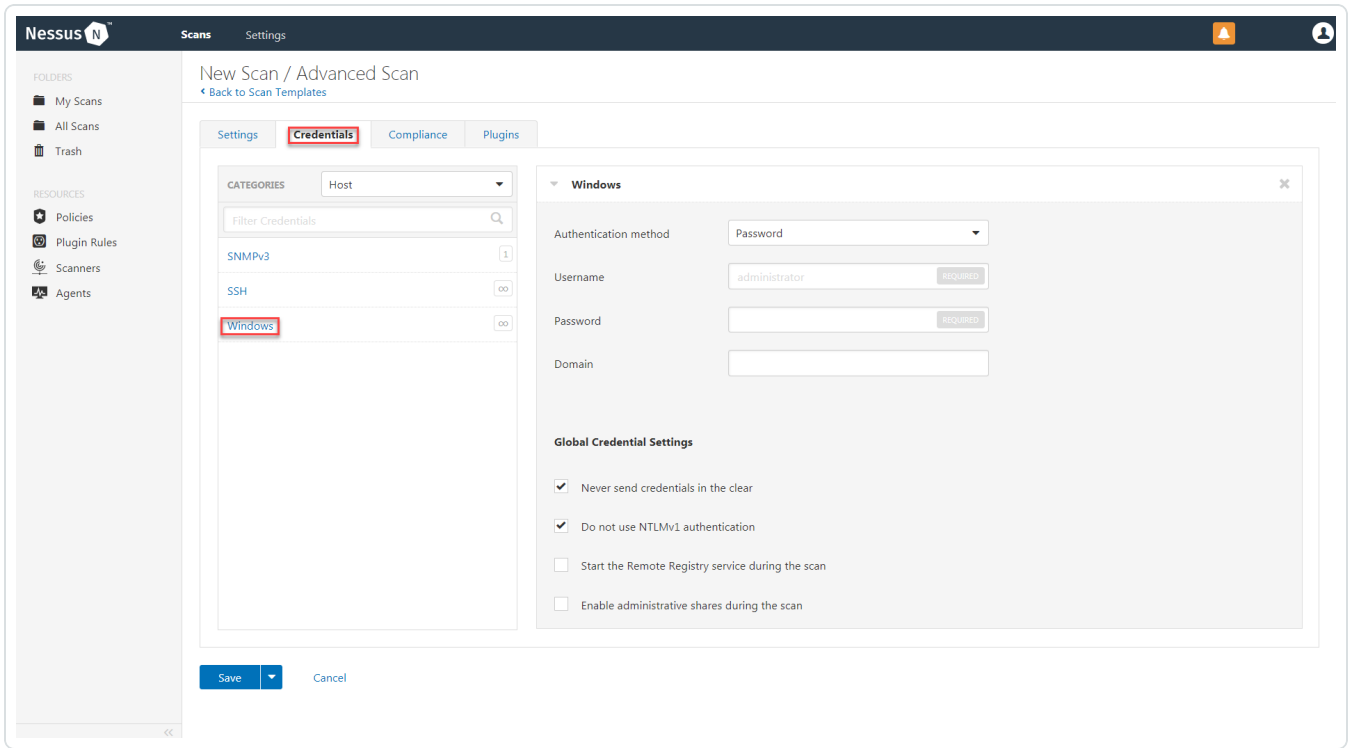
4. Select a **Scan Template** for the scan type required for your scan. For demonstration purposes, the **Advanced Network Scan** template is used.



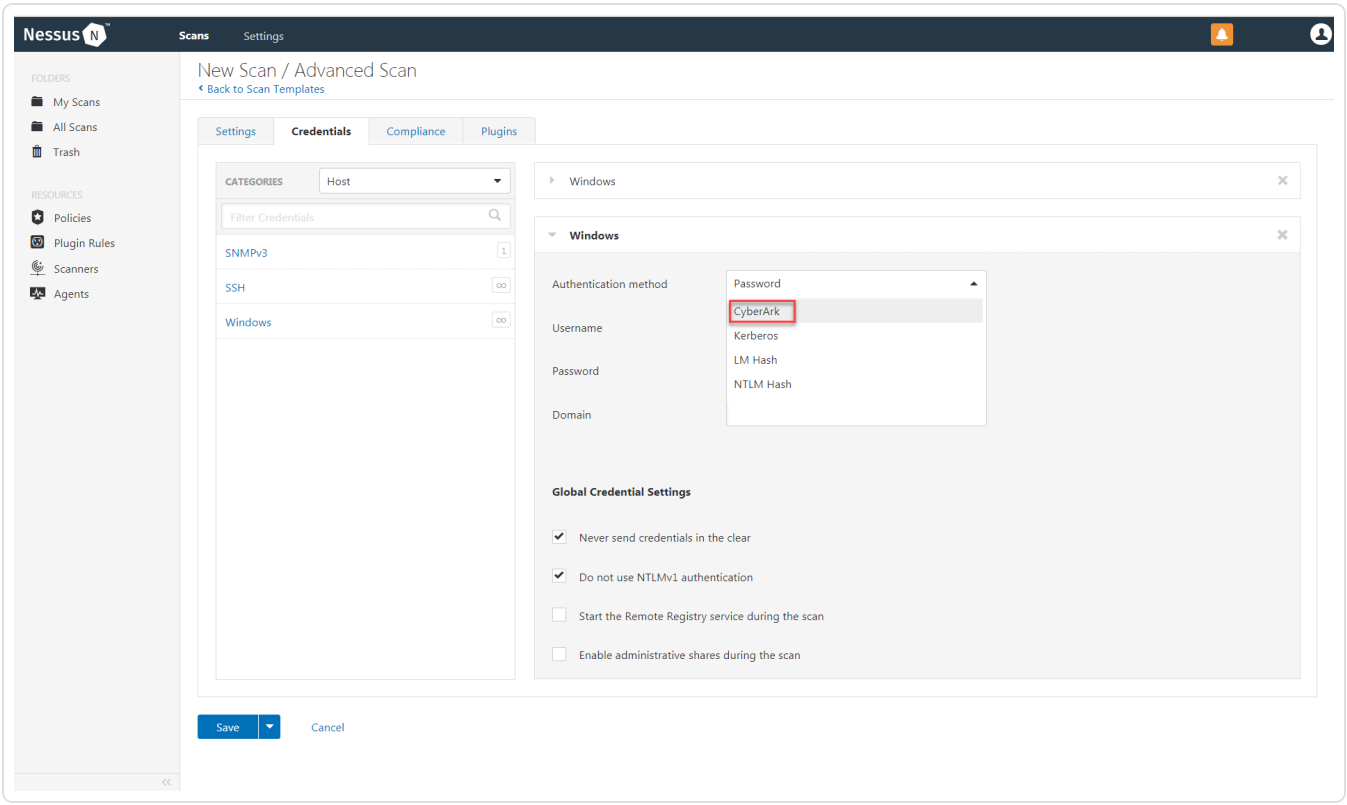
5. To configure a credentialed scan for **Windows** systems using CyberArk, enter a descriptive **Name**, the IP address(es) or hostname(s) of the scan **Targets**.



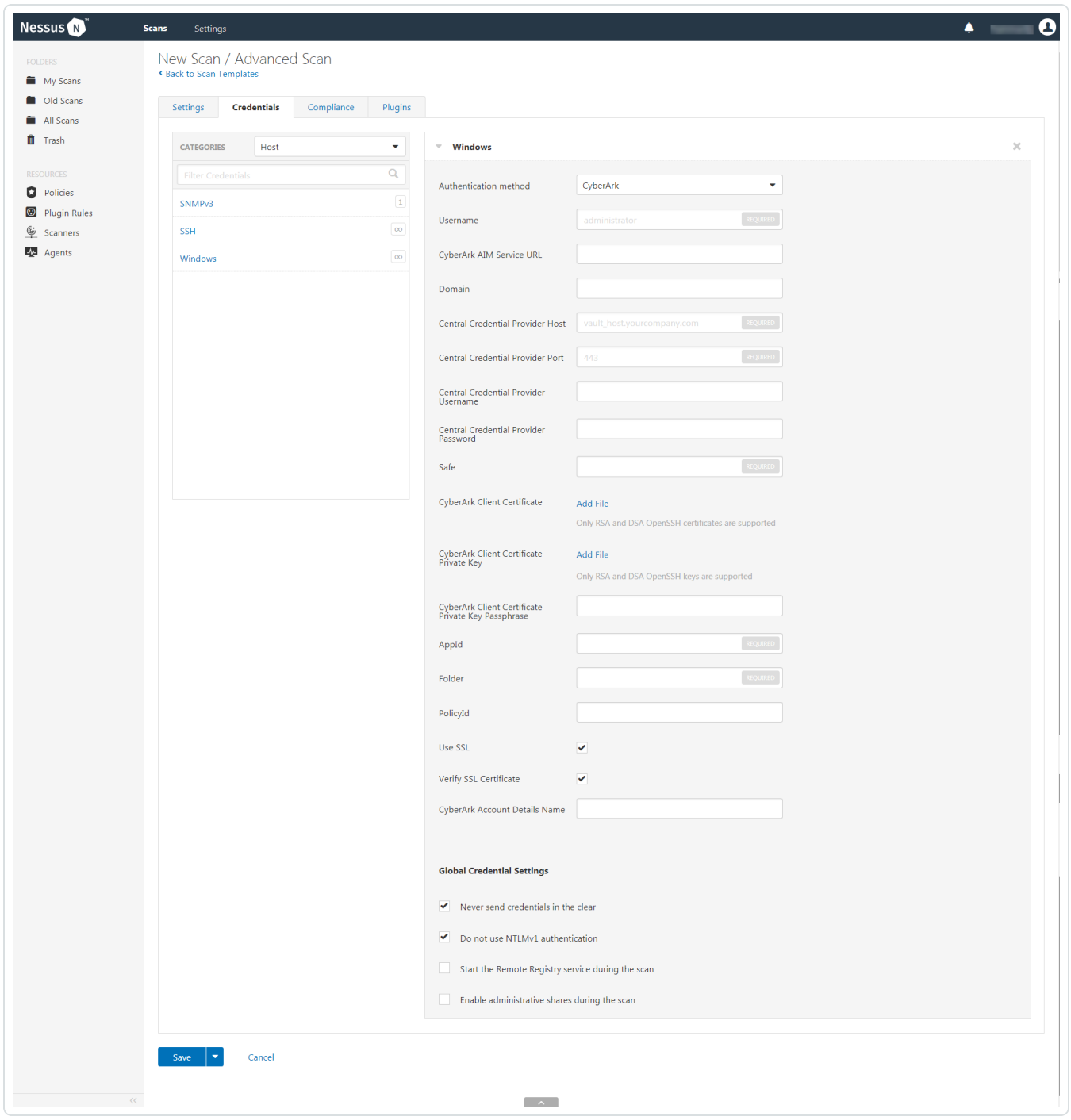
6. Once the **Name** and **Targets** have been configured, click **Credentials** (highlighted below) and then select **Windows** from the left-hand menu (highlighted below).



7. Click the **Authentication method** drop-down and select **CyberArk**.



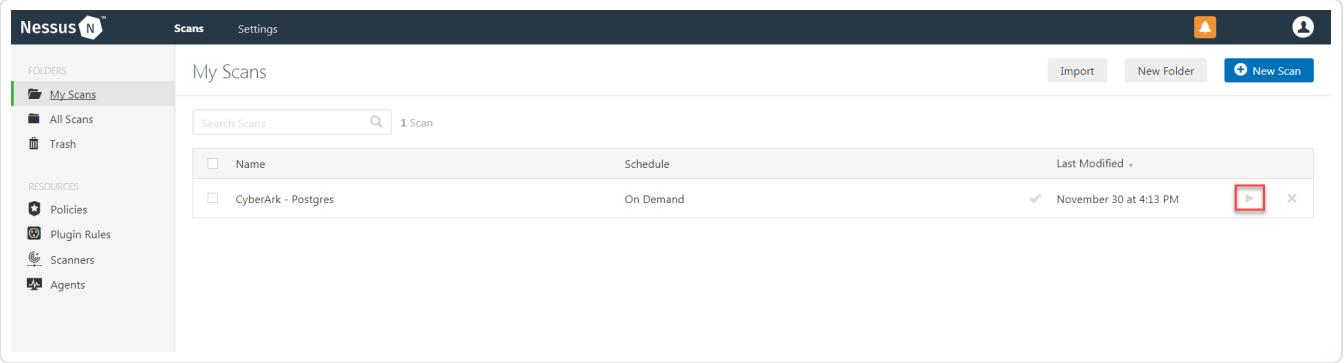
8. Configure each field for **Windows** authentication. See the **Credentials** section in the Nessus User Guide for detailed descriptions for each field option.



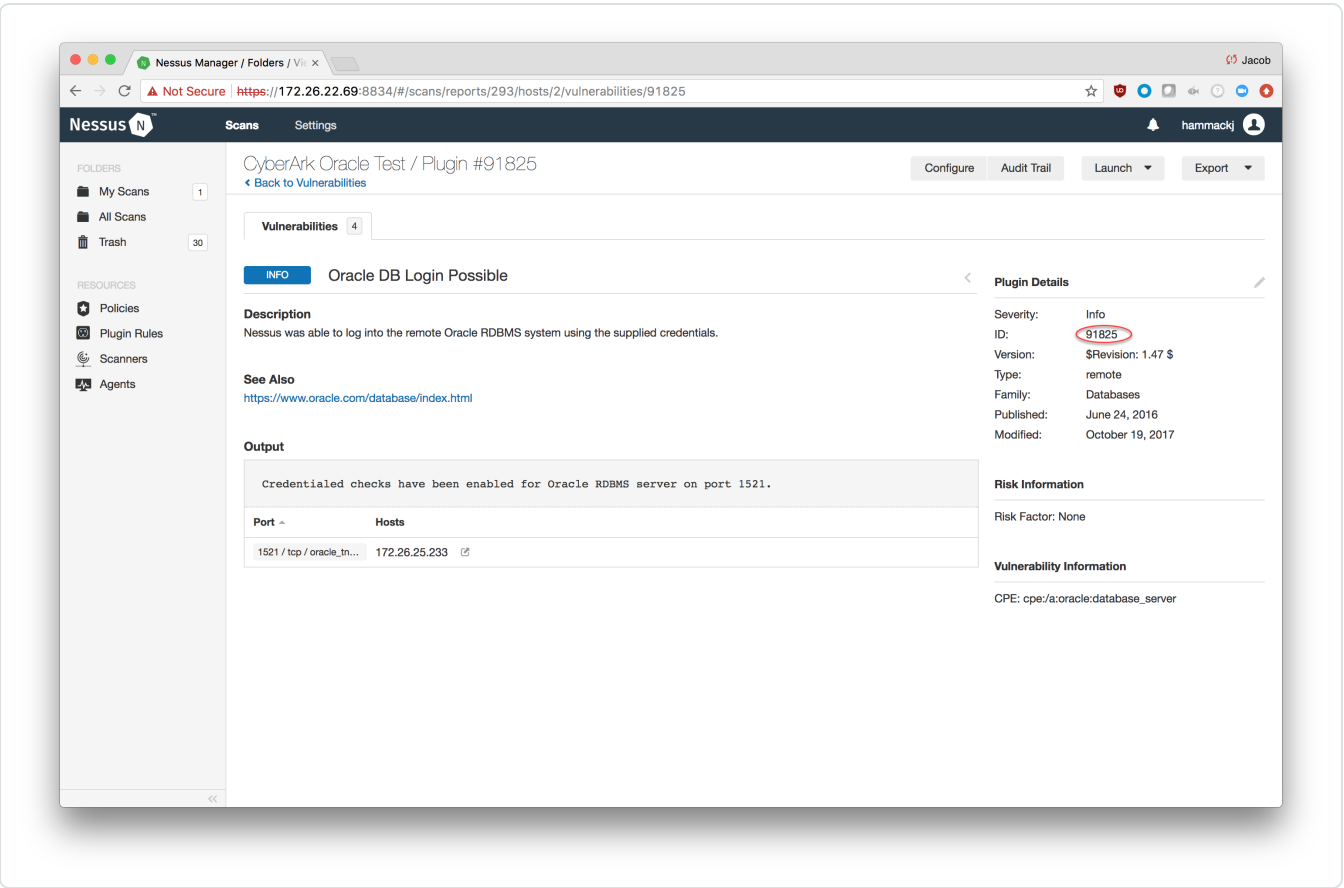
Caution: Tenable strongly recommends encrypting communication between the Nessus scanner and the CyberArk AIM gateway using HTTPS and/or client certificates. For information on securing the connection, refer to the Nessus User Guide and the **Central Credential Provider Implementation Guide** located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

9. Click **Save**.

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



11. Once the scan has completed, select the completed scan and look for the corresponding Login Successful 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.



Plugin Type	Plugin ID
Postgres	91826
SQL	91825
MySQL	91823

Database Integration

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

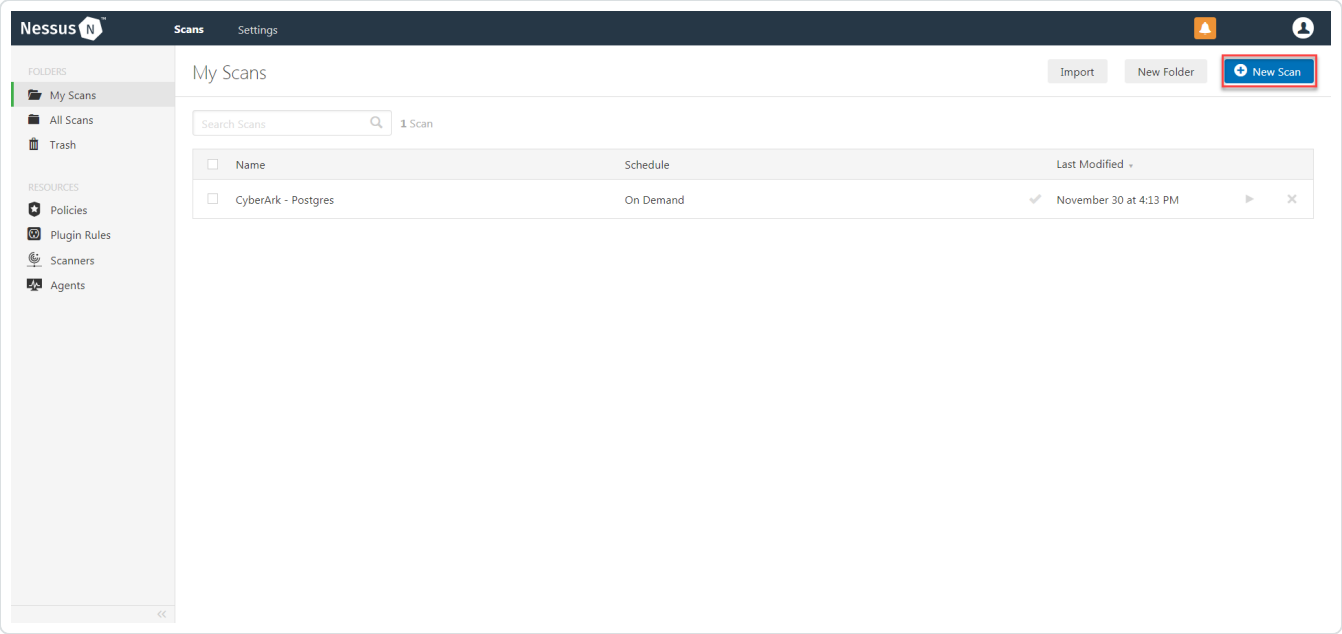
Requirements:

- CyberArk account
- Nessus Manager account

To configure Database integration:

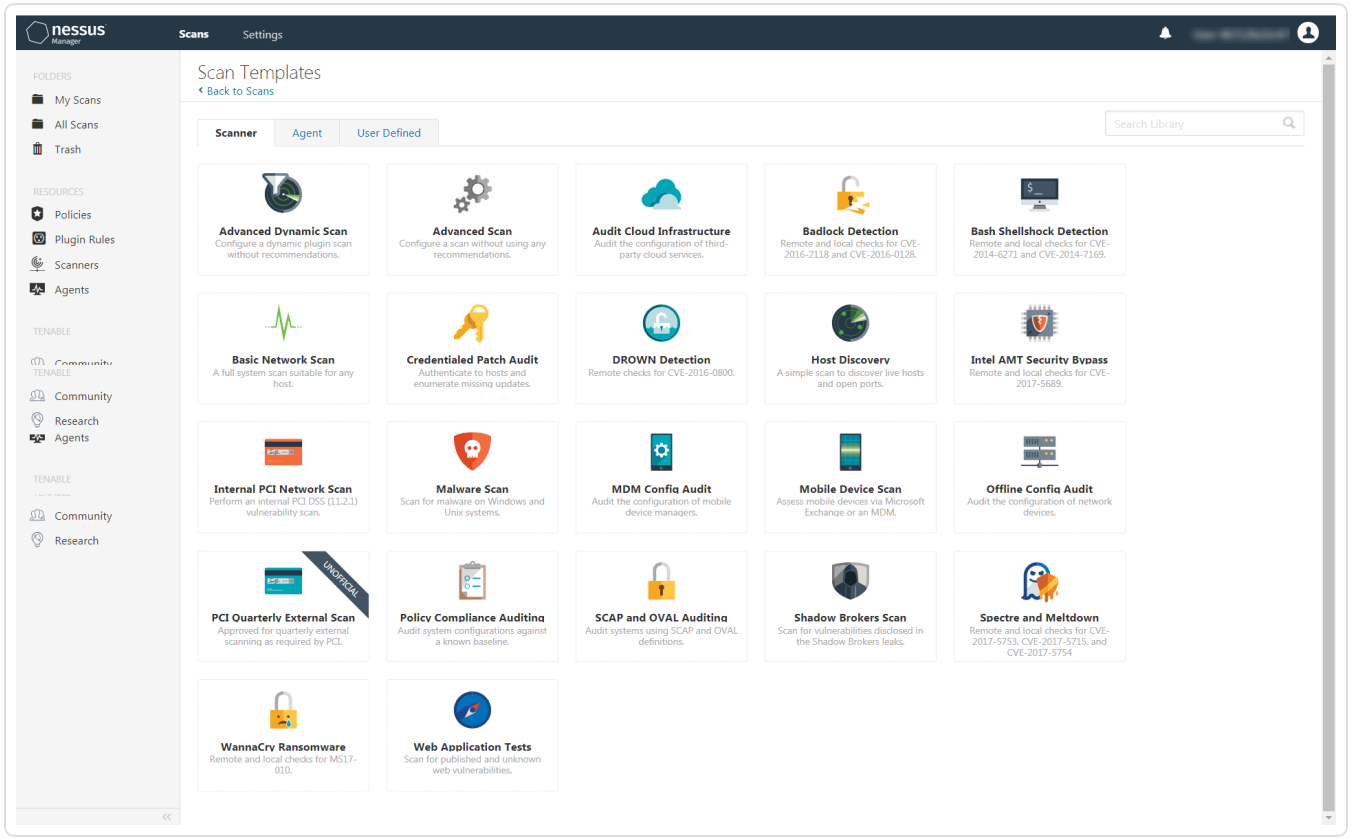
1. Log in to Nessus Manager-.
2. Click **Scans**.

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



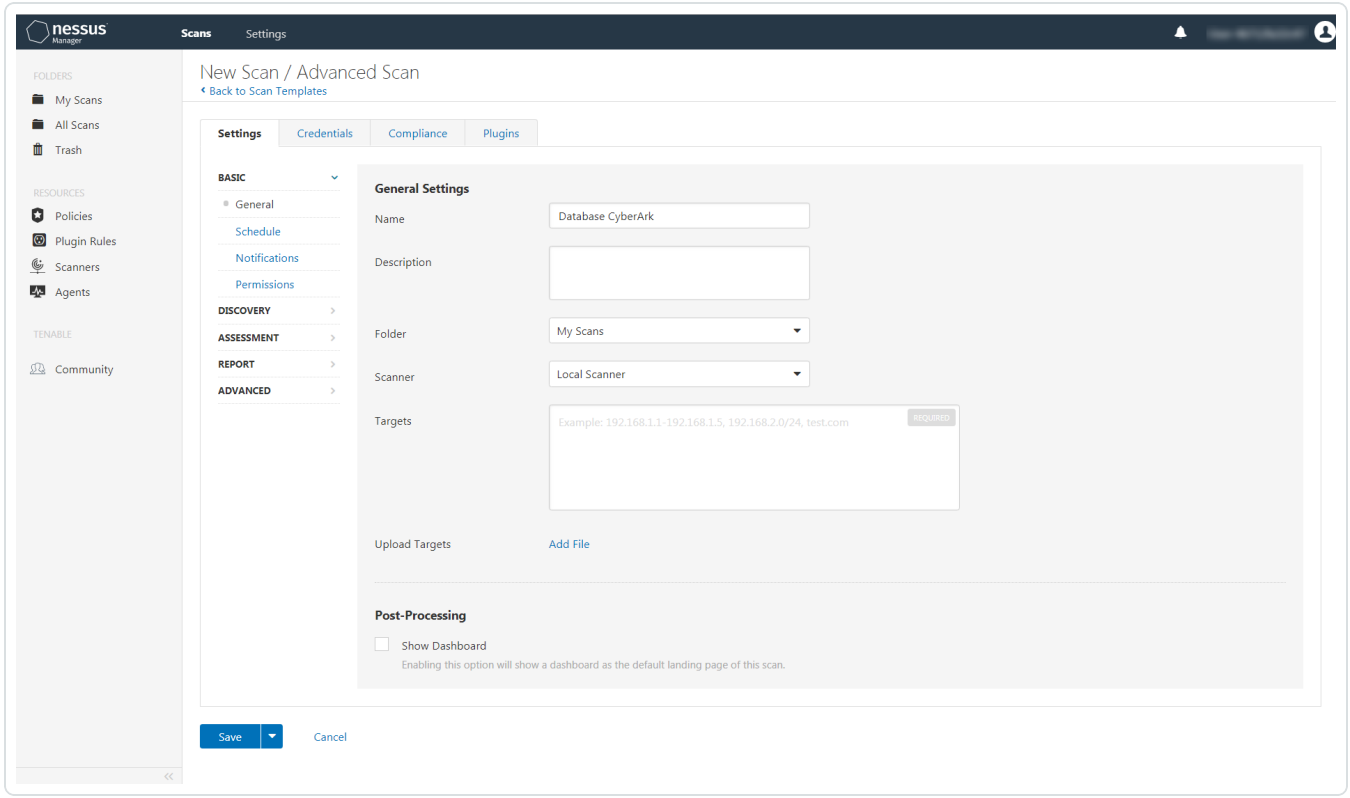
   The **Scan Templates** page appears.

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.

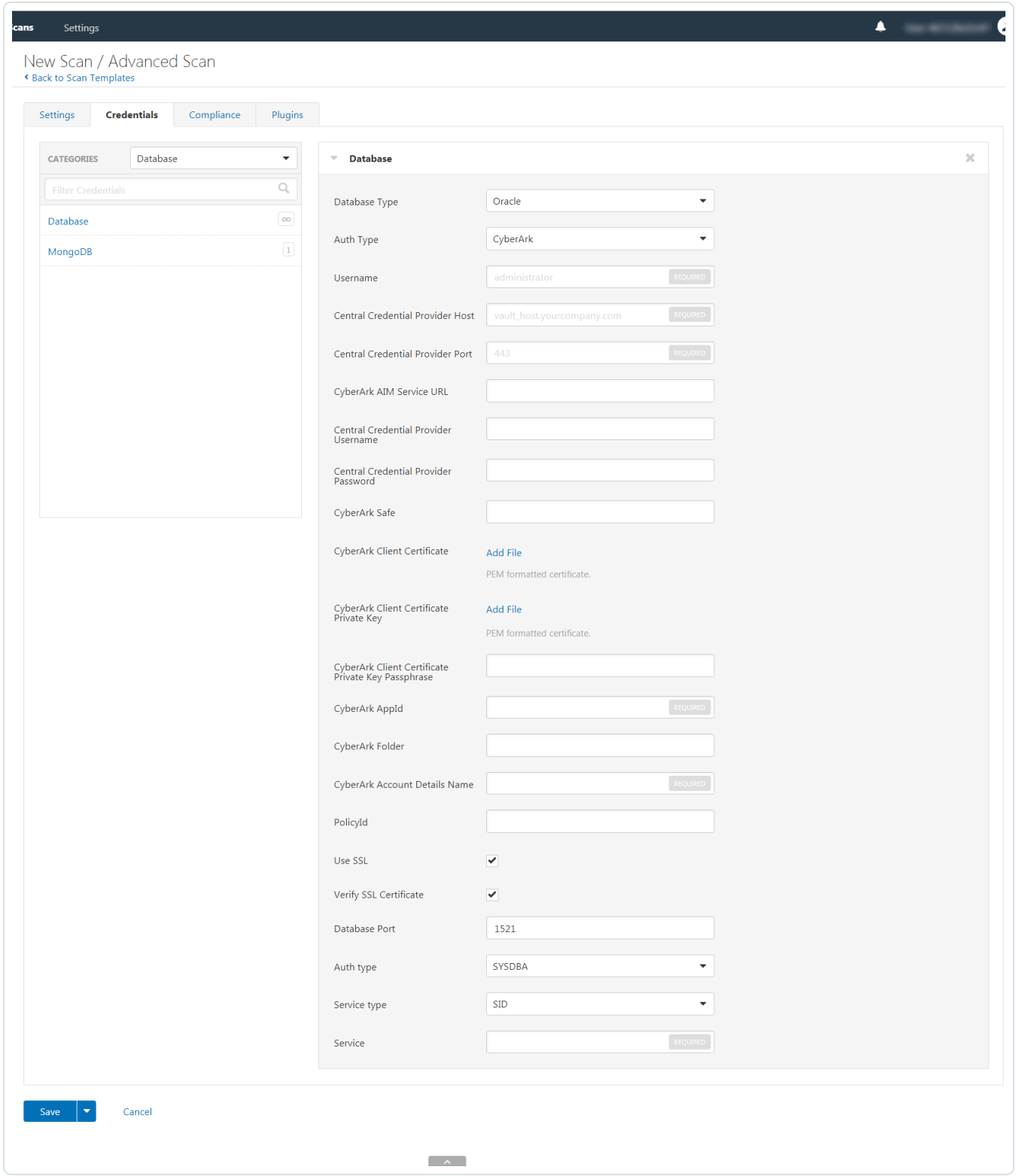
13. From the **Database Type** drop-down, select **Oracle**.

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.**

Privilege Escalation With CyberArk Credentials

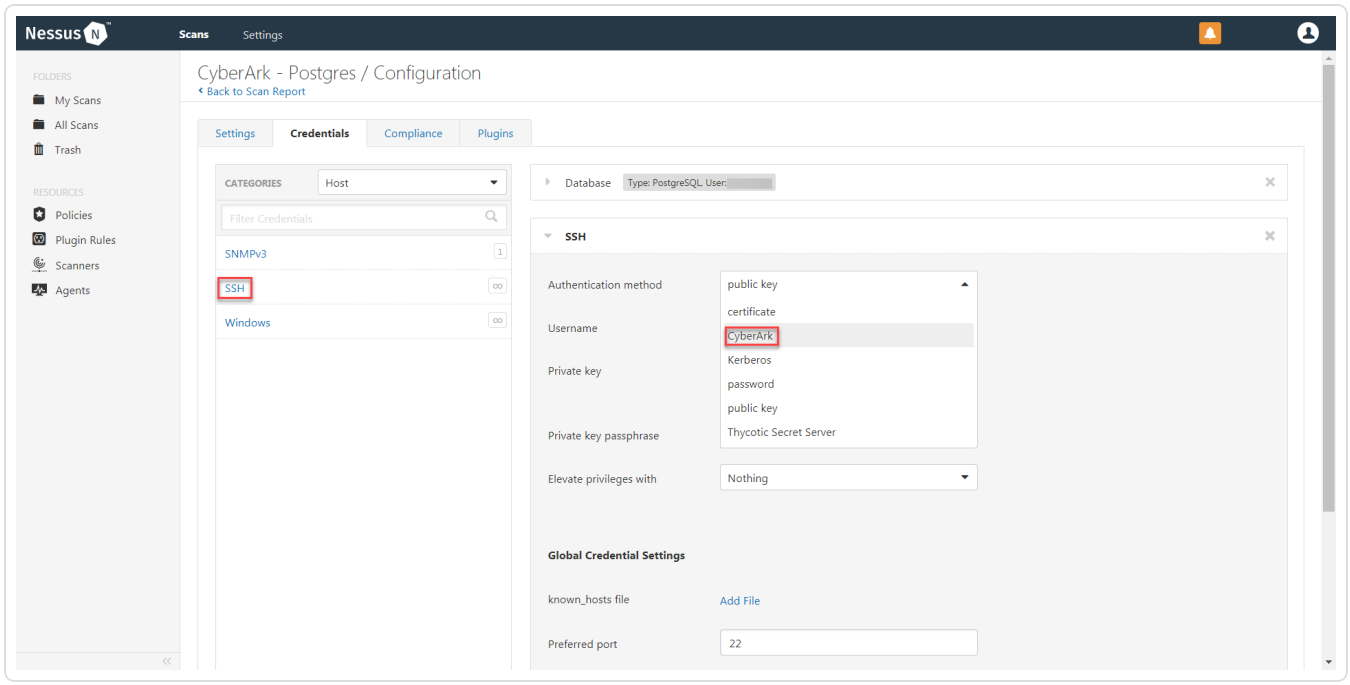
Nessus Manager supports the use of privilege escalation, such as *su* and *sudo*, when using SSH through the CyberArk authentication method.

Requirements:

- CyberArk account
- Nessus Manager account

To configure SSH integration:

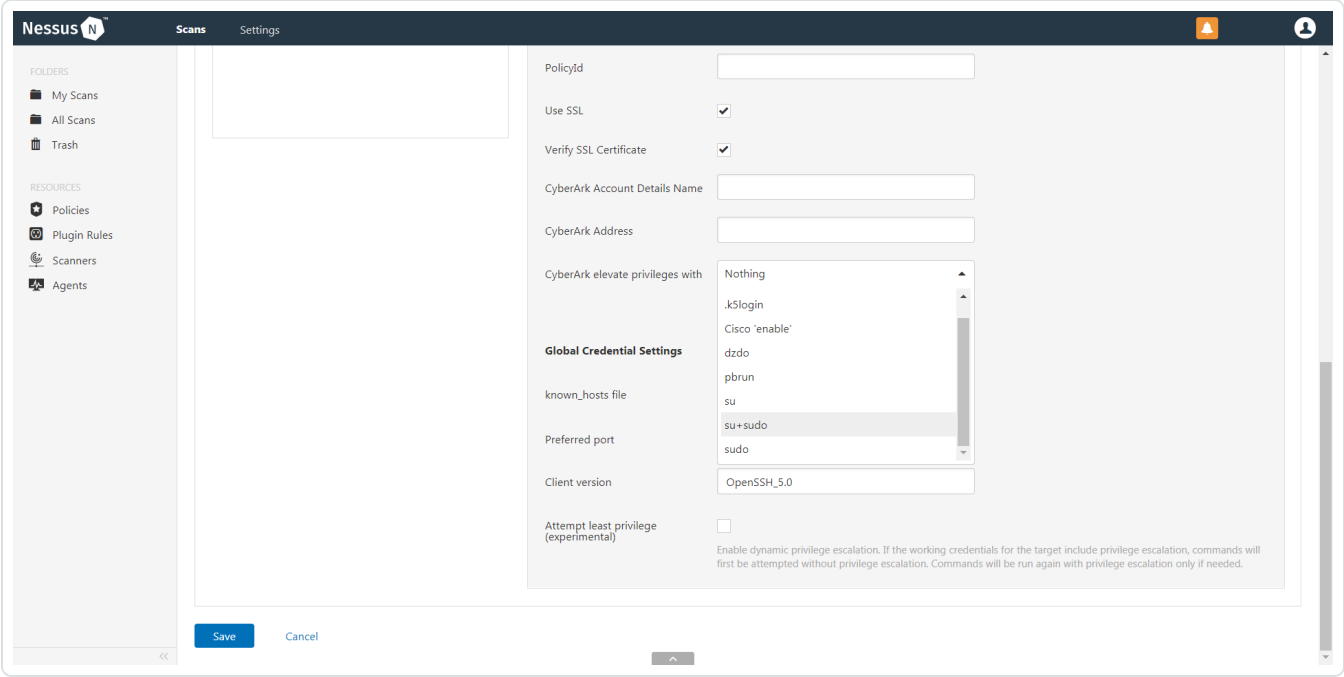
1. Select **SSH** as the **Type** and CyberArk as the **Authentication Method.**



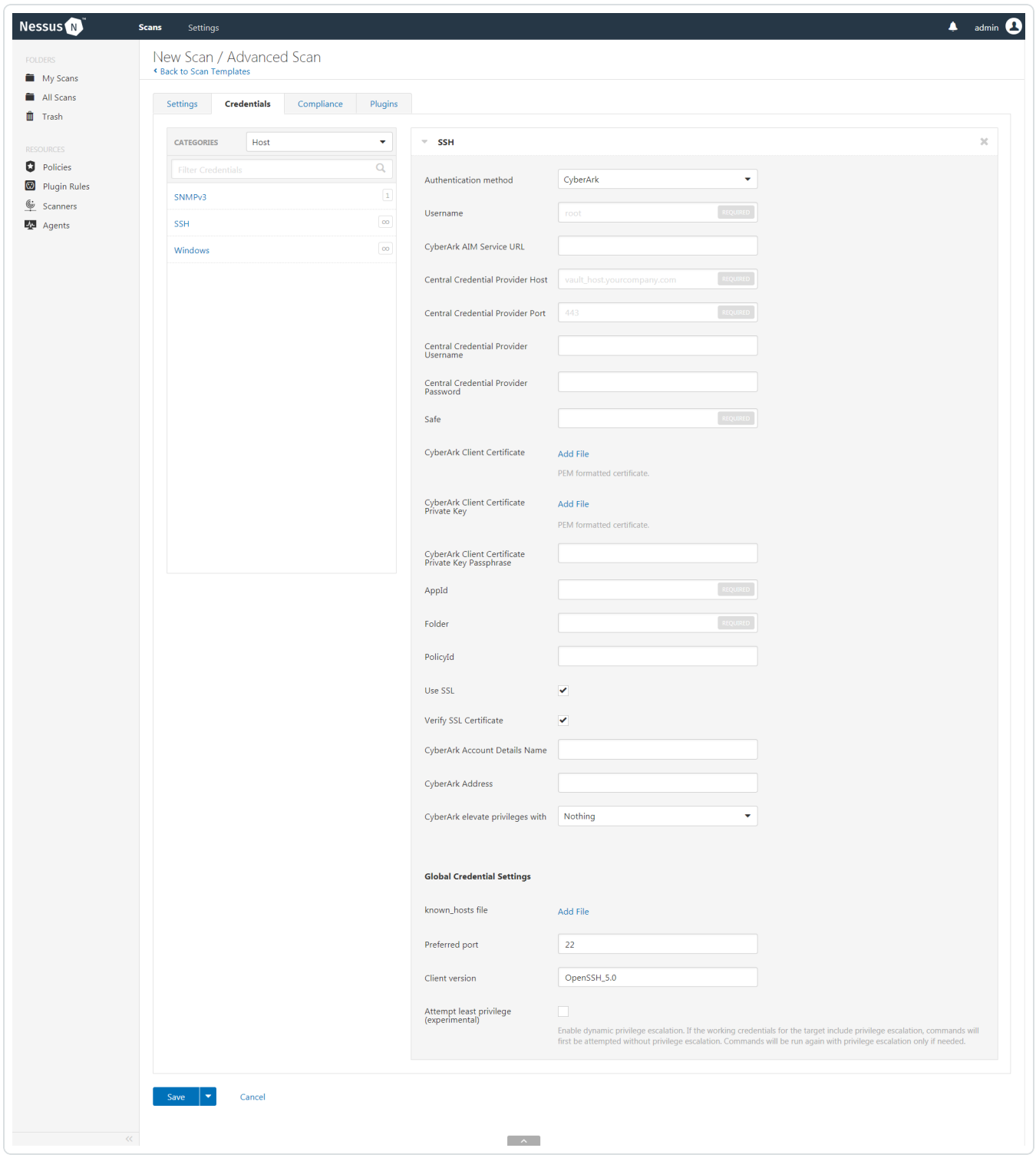
2. An option for **CyberArk elevate privileges with** appears near the bottom of the configuration page.

> **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 Windows authentication. See the Nessus User Guide to get detailed descriptions for each option.



4. Click **Save**.

Additional Information

CyberArk Domain and DNS Support

Tenable's support for CyberArk has been extended to allow Nessus to use its target list to query CyberArk Enterprise Password Vault for the target system's credentials, and Tenable's solutions can now use a flexible system to allow for DNS and domain support. See Nesssus Priority Scanning for CyberArk for explanation of the logic used by Nessus for scans using credentials from CyberArk Enterprise Password Vault.

Nessus Priority Scanning for CyberArk

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

1. Nessus will query CyberArk with the target value entered into the Nessus **Targets** configuration field. For example, if you put a FQDN in the target list, Nessus will query CyberArk with the address value of the FQDN. If you enter an IP address or range such as 192.168.1.1-20, Nessus 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, Nessus will then look to see if there is a domain value (for a Windows system). If a domain value is present, Nessus 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, Nessus 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, Nessus 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.

Retrieving Addresses to Scan from CyberArk

Use Nessus Manager to access a feature in CyberArk to pull a list of targets to scan. Complete the following steps to pull target system values.

> **Note:** You cannot retrieve a target address with a default administrator account. You must create an account that is a member of the PVWAMonitor group to generate the following reports.

1. Log in to CyberArk.
2. At the top of the page, click **Report**.
3. Click **Generate Report**.
4. Choose **Privileged Account Inventory**.
5. Click **Next**.
6. Specify the search parameters for the systems you want to scan.
7. Click **Next**.
8. Click **Finish**.
9. Download the CSV or XLS report.
10. Confirm the targets for Nessus to scan.
11. Confirm that all values can be resolved by Nessus.
12. Copy the values from the **Target system address** column.
13. Enter the values into Nessus Manager using one of the following methods.
    a. Paste the values from addresses into the target list in Nessus.
    b. Paste the values into a file and use that file as the target list in Nessus.

Debugging CyberArk

To enable debugging when you configure a scan in Nessus, 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=172.26.22.26] 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 applic-
ation 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=172.26.22.26] 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 applic-
ation 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
```

```
Accounts;Folder=Root;Object=Operating System-WinDesktopLocal-
172.26.22.205-admin, Safe=Unix Accounts;Folder=Root;Object=Operating Sys-
tem-WinDesktopLocal-172.26.22.66-admin and more. See trace log for more
information). (Diagnostic Info: 41)
```

The Nessus 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 172.26.22.66 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.

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.