How-to Guide: SecurityCenter for CyberArk

Last Updated: September 20, 2018

Table of Contents

Introduction

This document describes how to deploy Tenable SecurityCenter® for integration with CyberArk Enterprise Password Vault. Please email any comments and suggestions to support@tenable.com.

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 the CyberArk Enterprise Password Vault with Tenable's solutions, customers are now granted even more choice and flexibility for reducing the credentials headache.

Benefits of integrating Tenable SecurityCenter with CyberArk Enterprise Password Vault include:

- Credentials stored in CyberArk Enterprise Password Vault no longer need to be managed and updated directly within a Tenable solution
- Reduce the time and effort needed to document where credentials are stored within the entire organizational environment
- Automatically enforce security policies within specific departments or for specific business unit requirements, which simplifies compliance
- Reduce the risk of unsecured privileged accounts and credentials across the enterprise

Integrations

Configure CyberArk with either Windows or SSH. Click the corresponding link to view the configuration steps.

Windows Integration

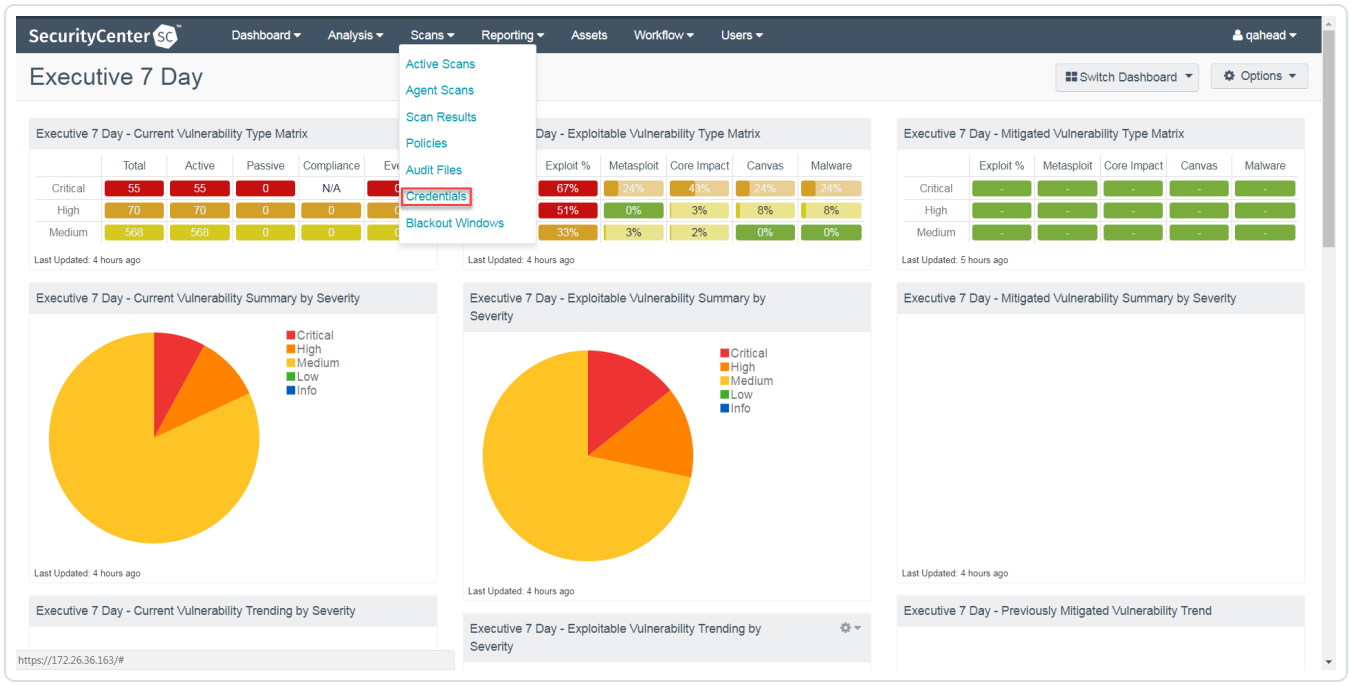
SSH Integration

Windows Integration

To configure Windows integration:

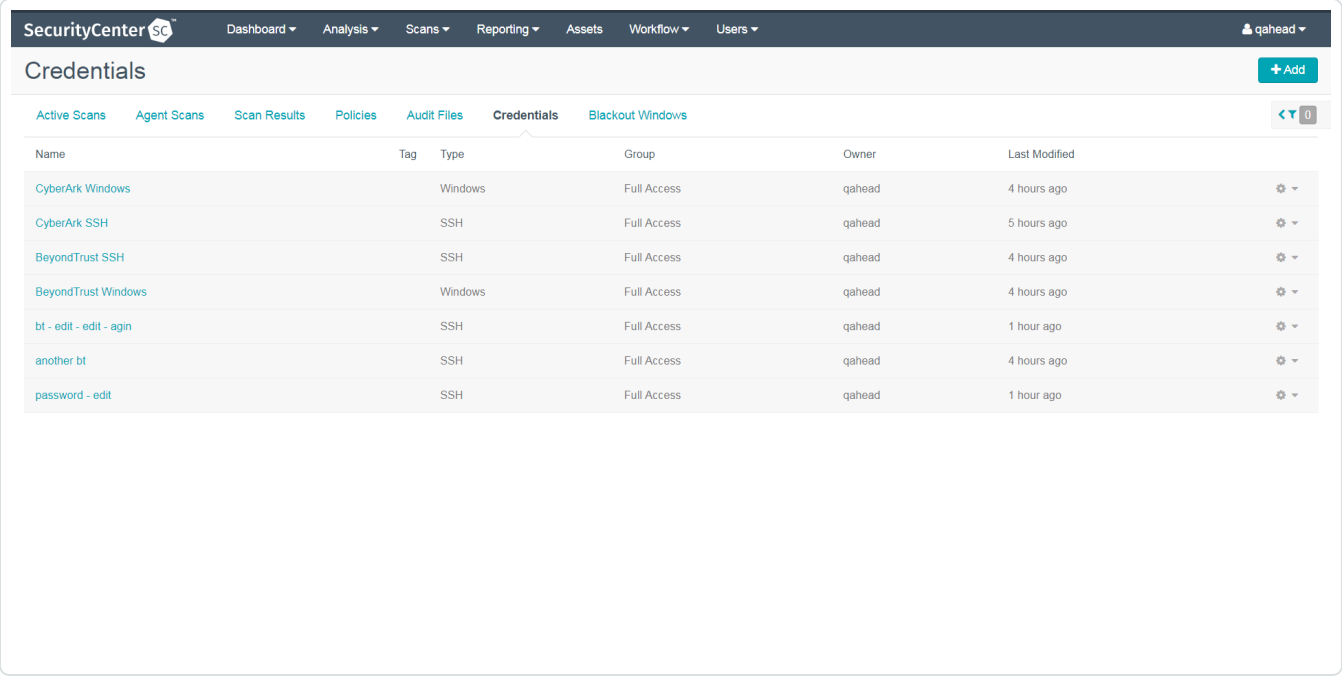
1. Log in to SecurityCenter.
2. In the top navigation bar, click **Scans**.

   A menu appears.

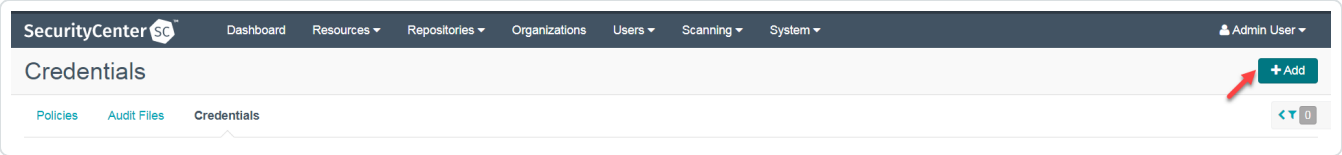


3. Click **Credentials**.

   The **Credentials** page appears.

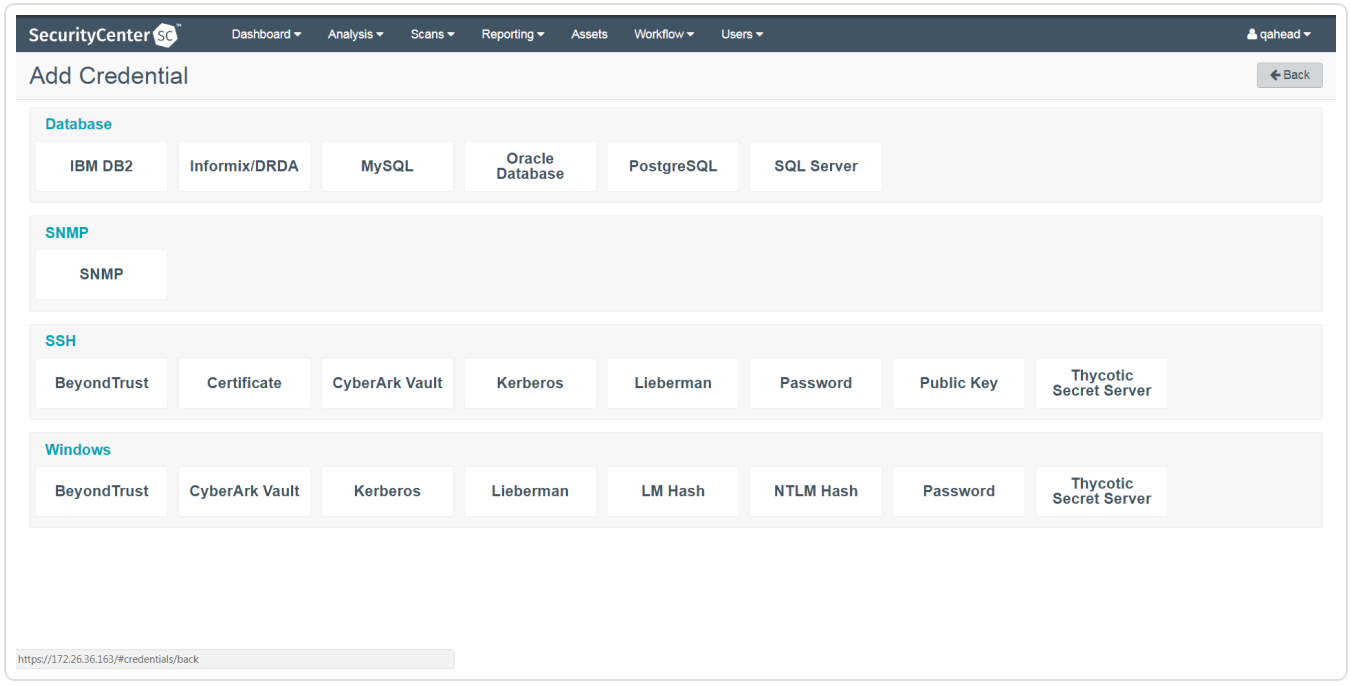


4. Click **+Add** at the top of the screen.



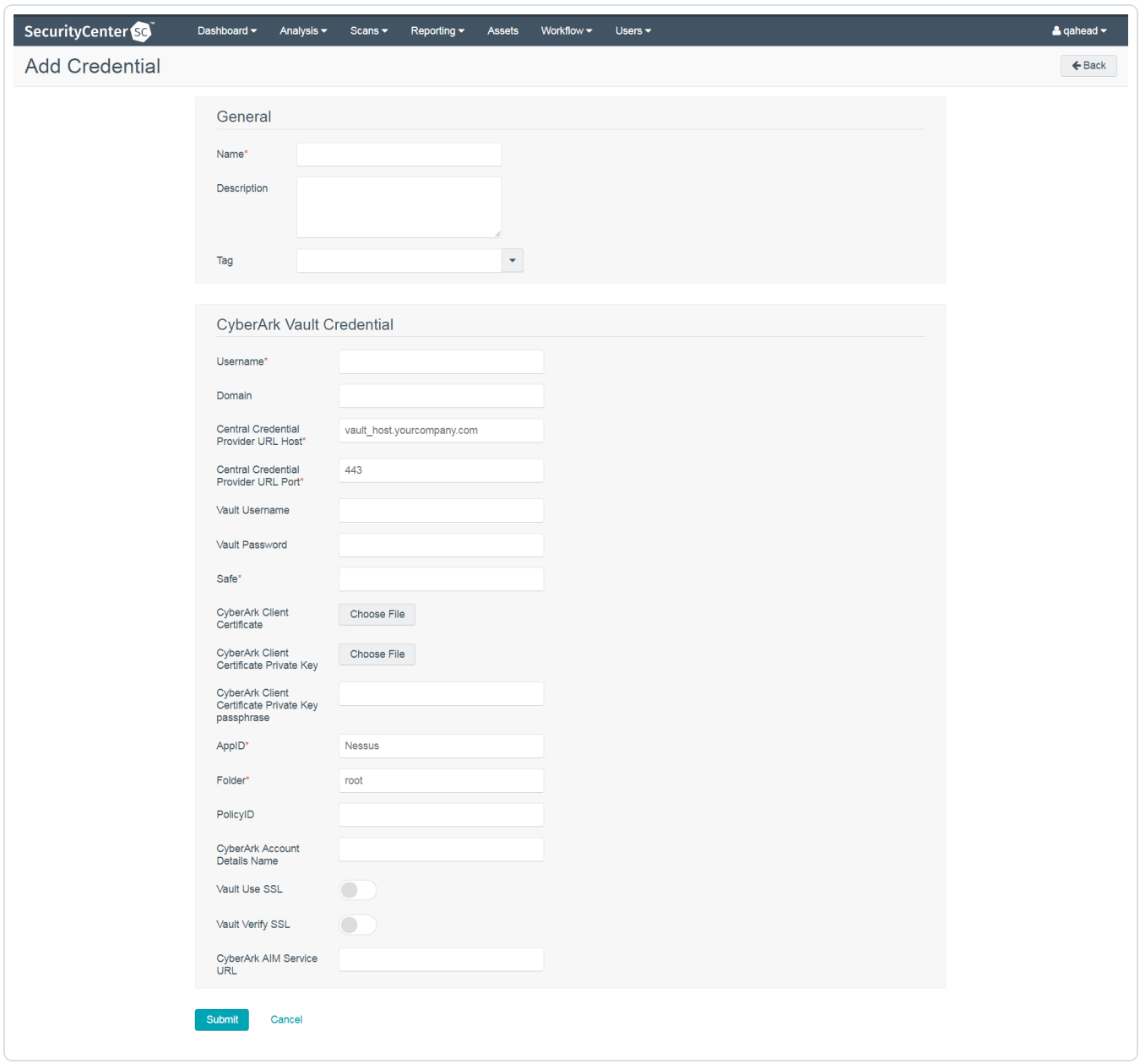
The **Add Credential** page appears.

5. In the **Windows** section, click **CyberArk Vault**.



The **Add Credential** page appears.

6. Configure each field for **Windows** authentication. See the SecurityCenter User Guide to get detailed descriptions for each option.



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

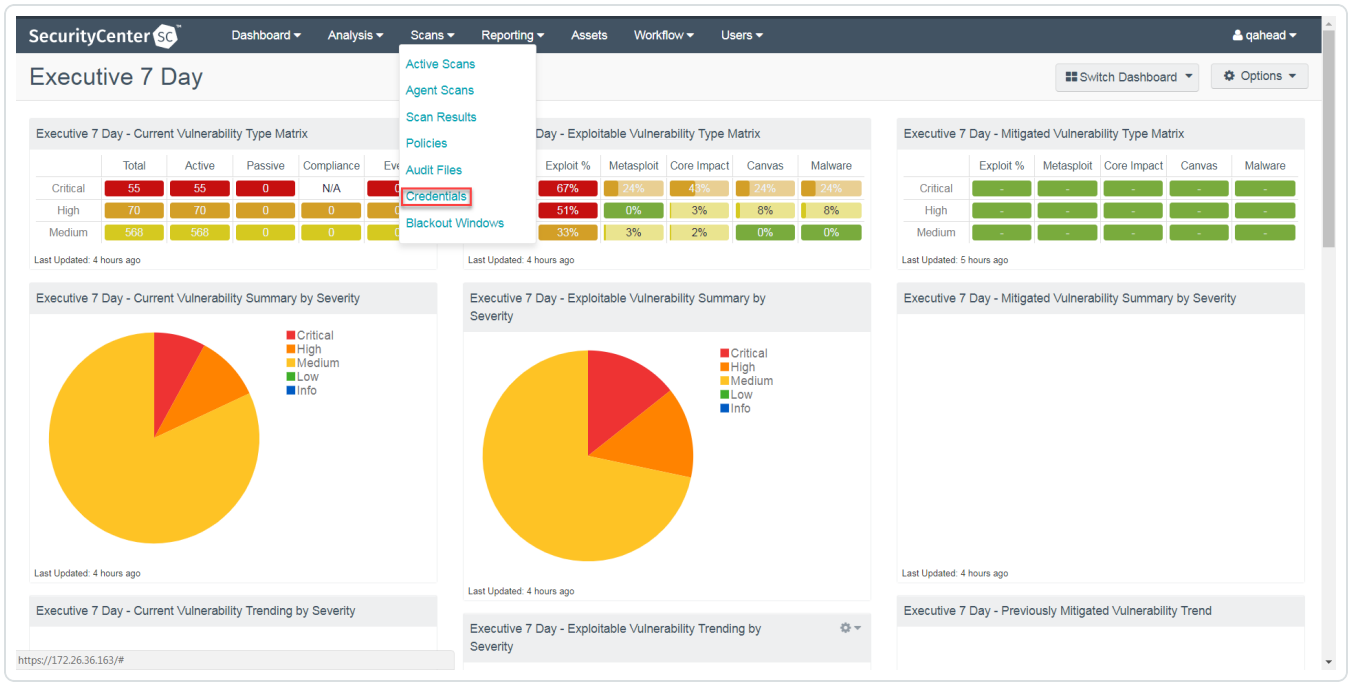
7. Click **Submit**.
8. Next, follow the steps for adding the credential to a scan.

SSH (Privilege Escalation) Integration

To configure SSH integration:

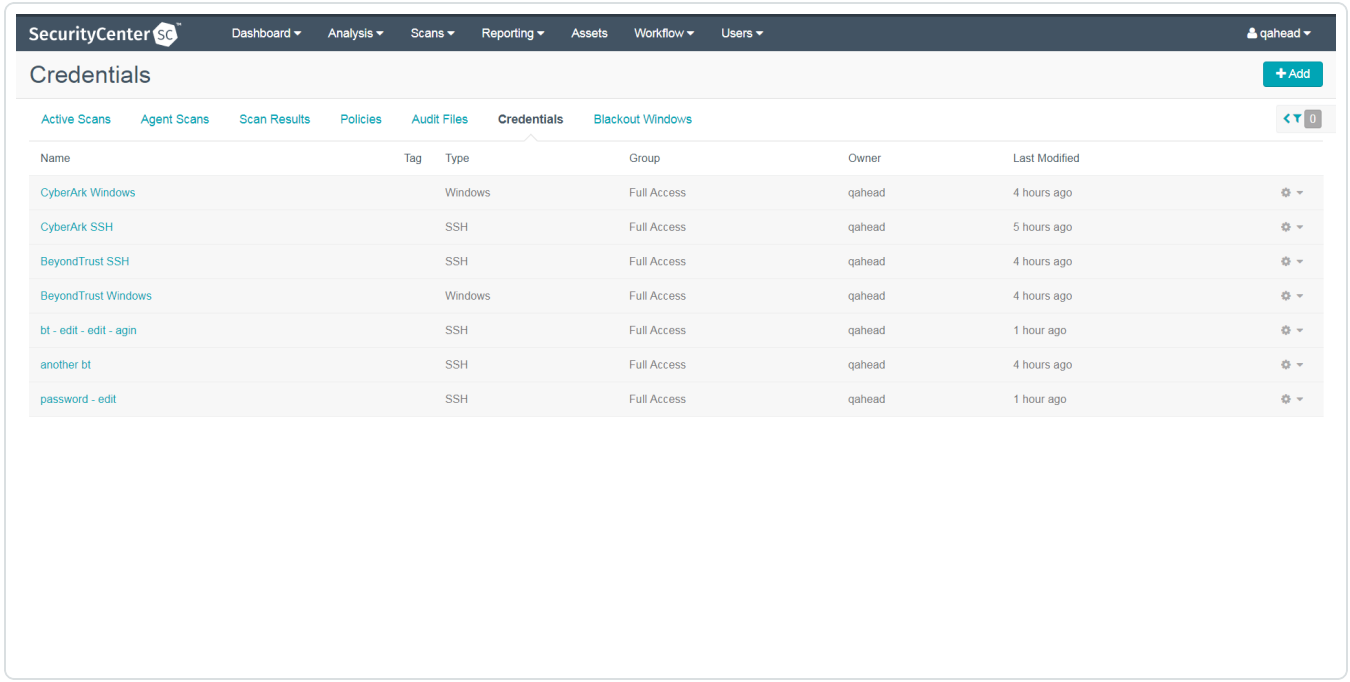
1. Log in to SecurityCenter.
2. In the top navigation bar, click **Scans**.

   A menu appears.

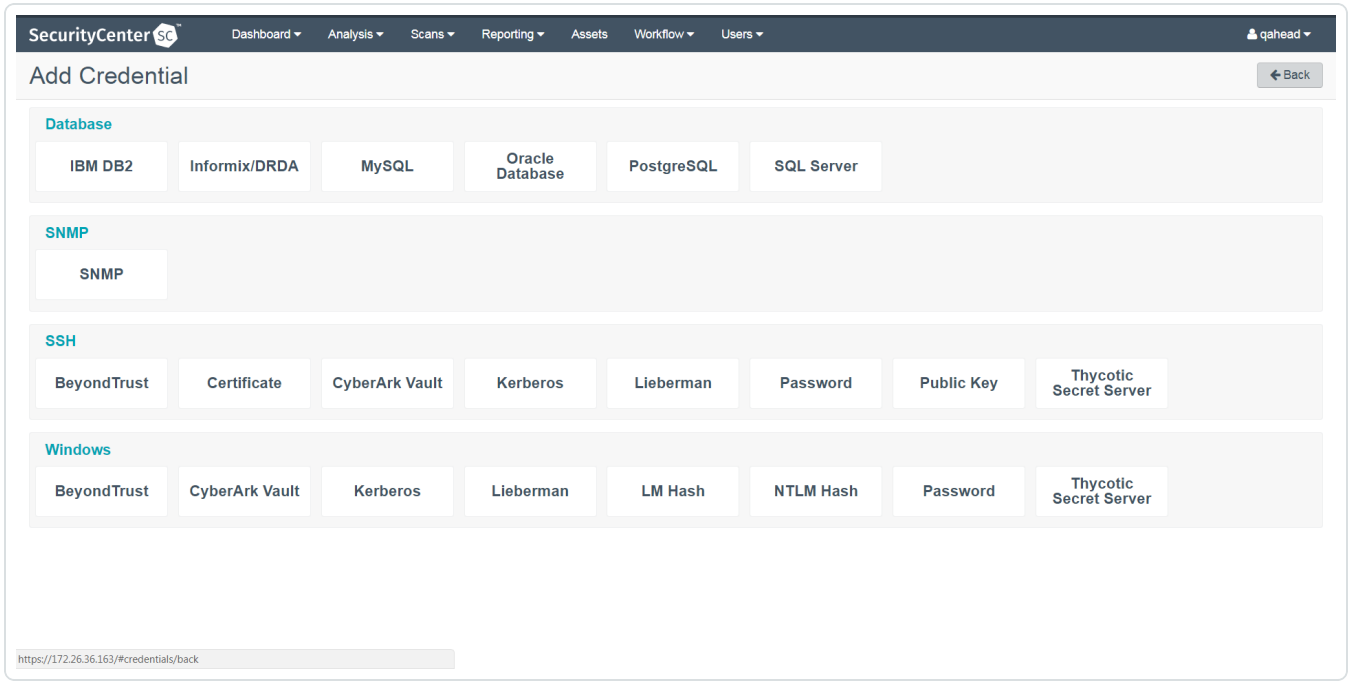


3. Click **Credentials**.

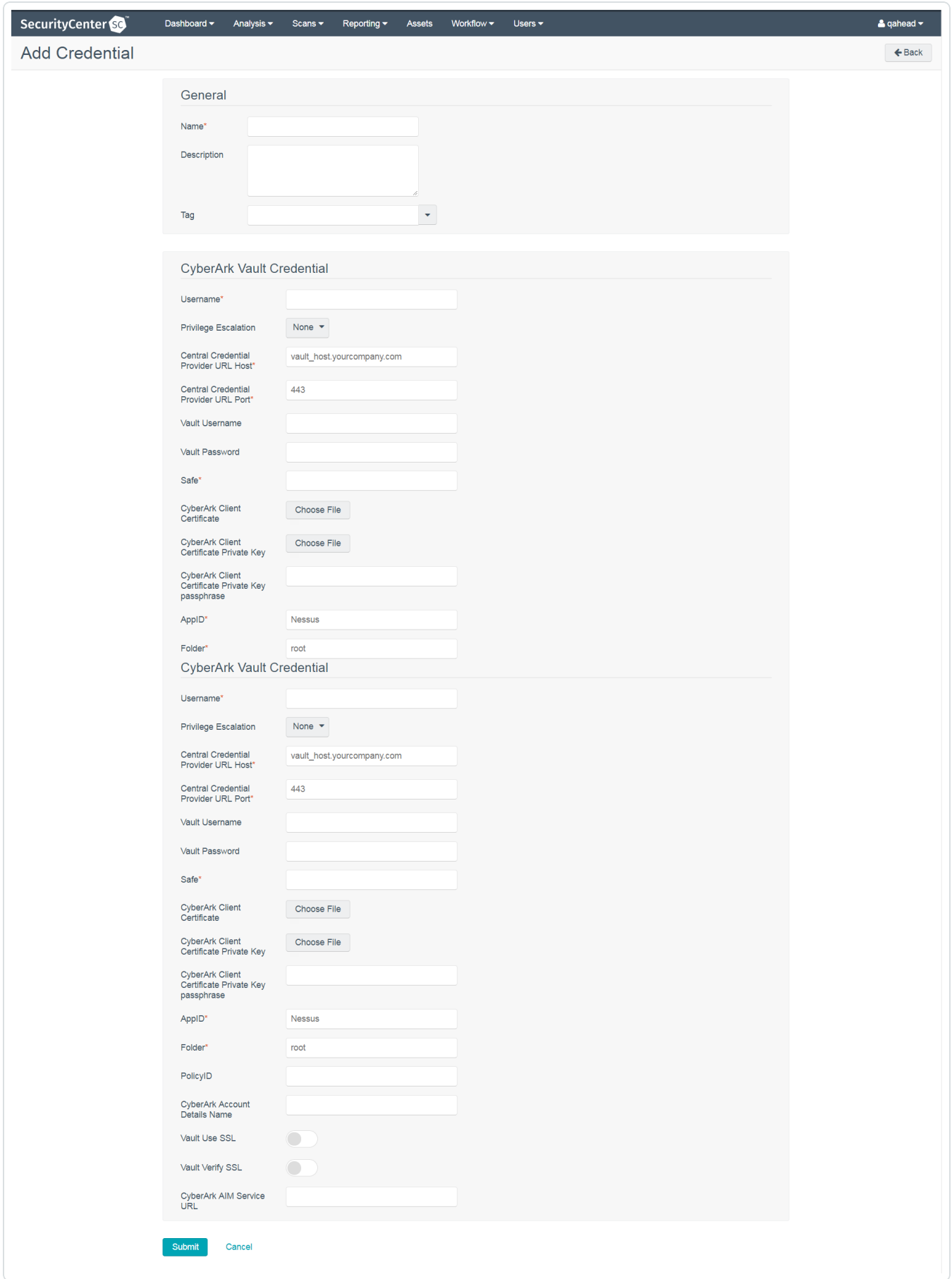
   The **Credentials** page appears.



4. In the SSH section, click **CyberArk Vault**.



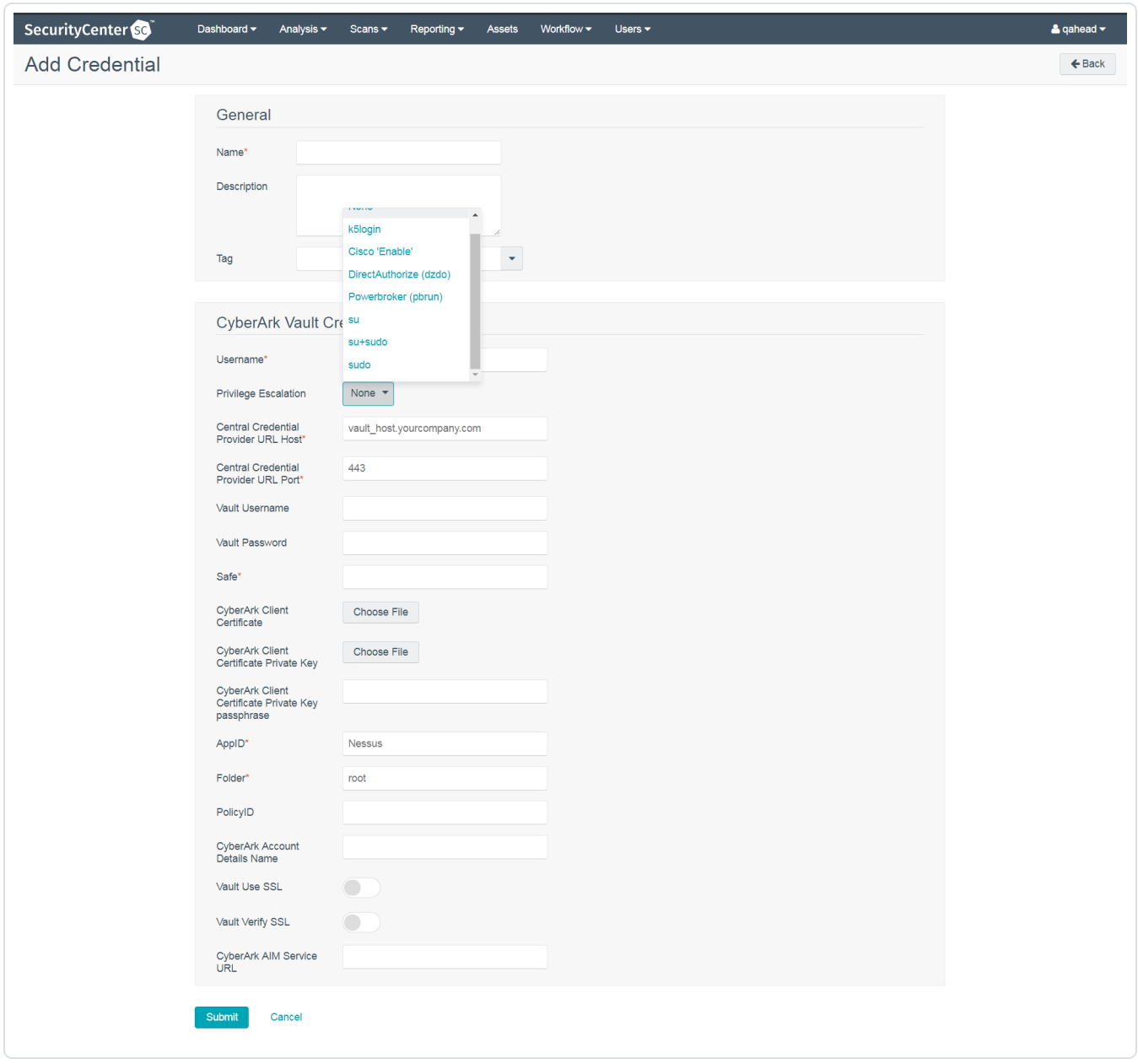
The **Add Credential** page appears.



5. In the **CyberArk Vault Credentials** section, click **Privilege Escalation**.

   The **Privilege Escalation** options appear.

> **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 SecurityCenter User Guide for additional information about the supported privilege escalation types and their accompanying fields.



6. Configure each field for **SSH** authentication. See the SecurityCenter User Guide to get detailed descriptions for each option.
7. Click **Submit**.
8. Next, follow the steps for adding the credential to a scan.

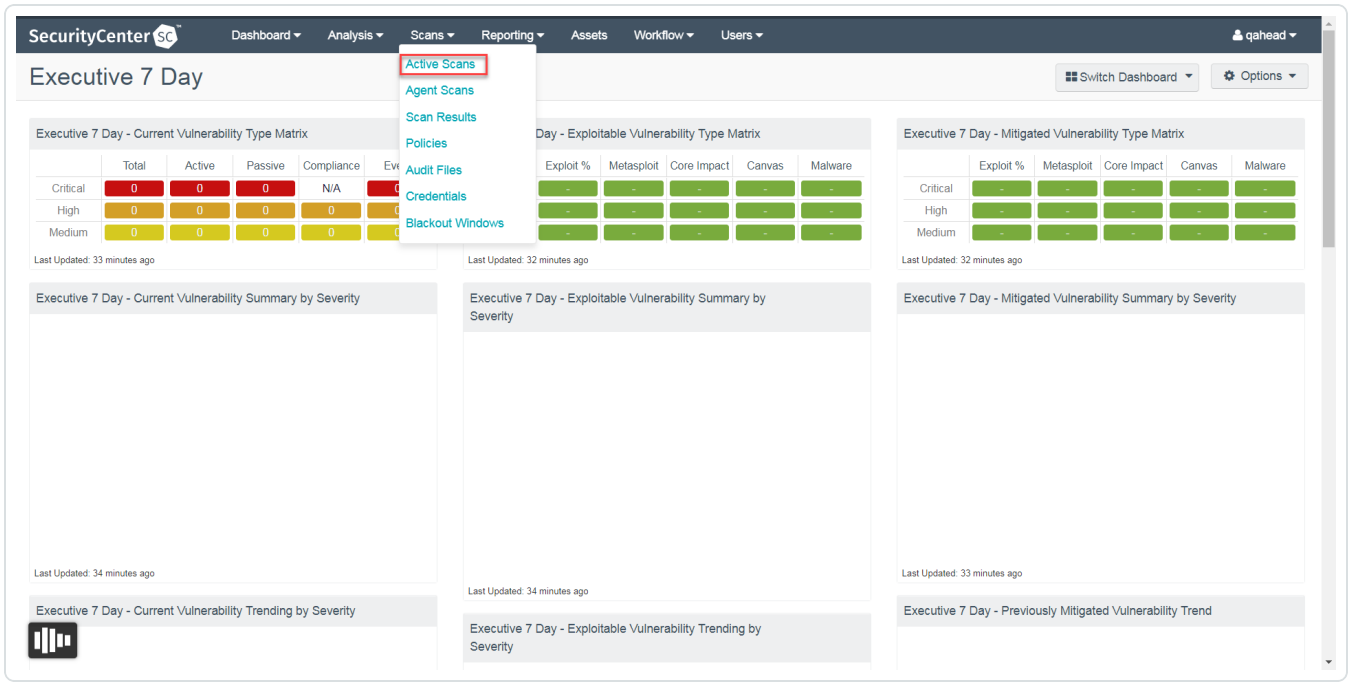
Add the CyberArk Credential to the Scan

To add the CyberArk credential to the scan:

1. In the top navigation bar, click **Scans**.

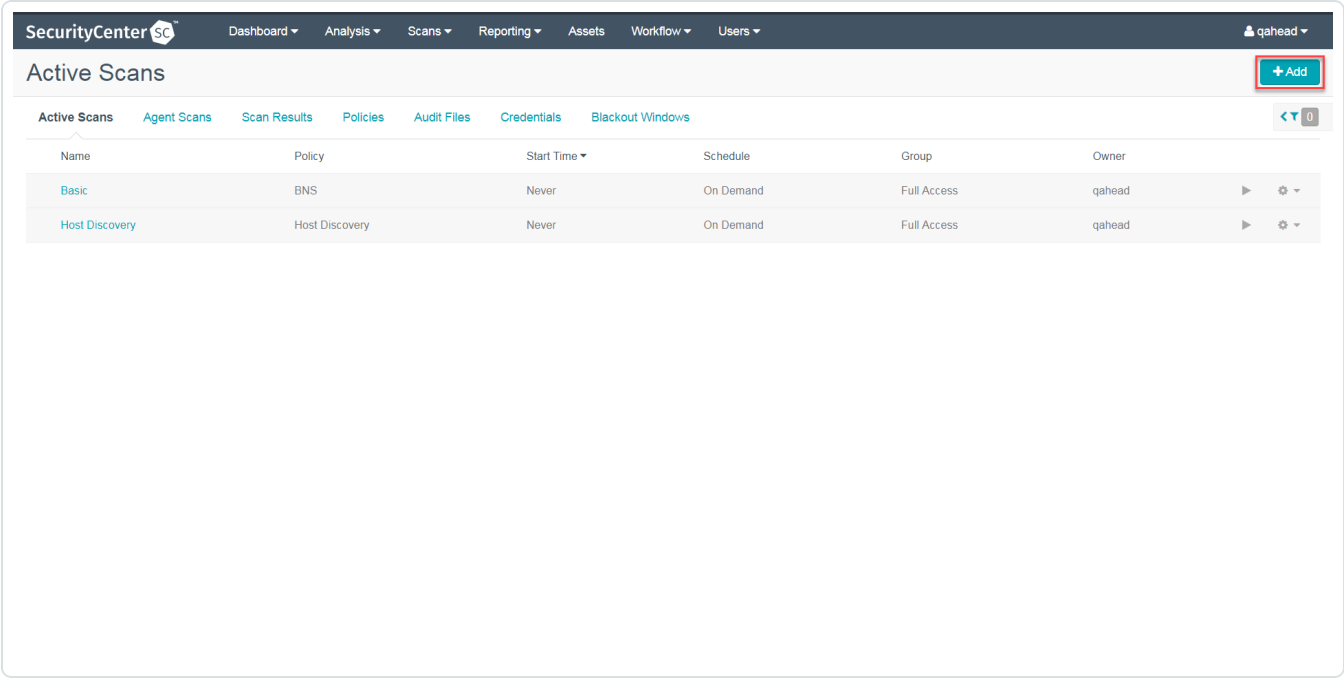
   A drop-down menu appears.

2. Select **Active Scans**.



   The **Active Scans** window opens.

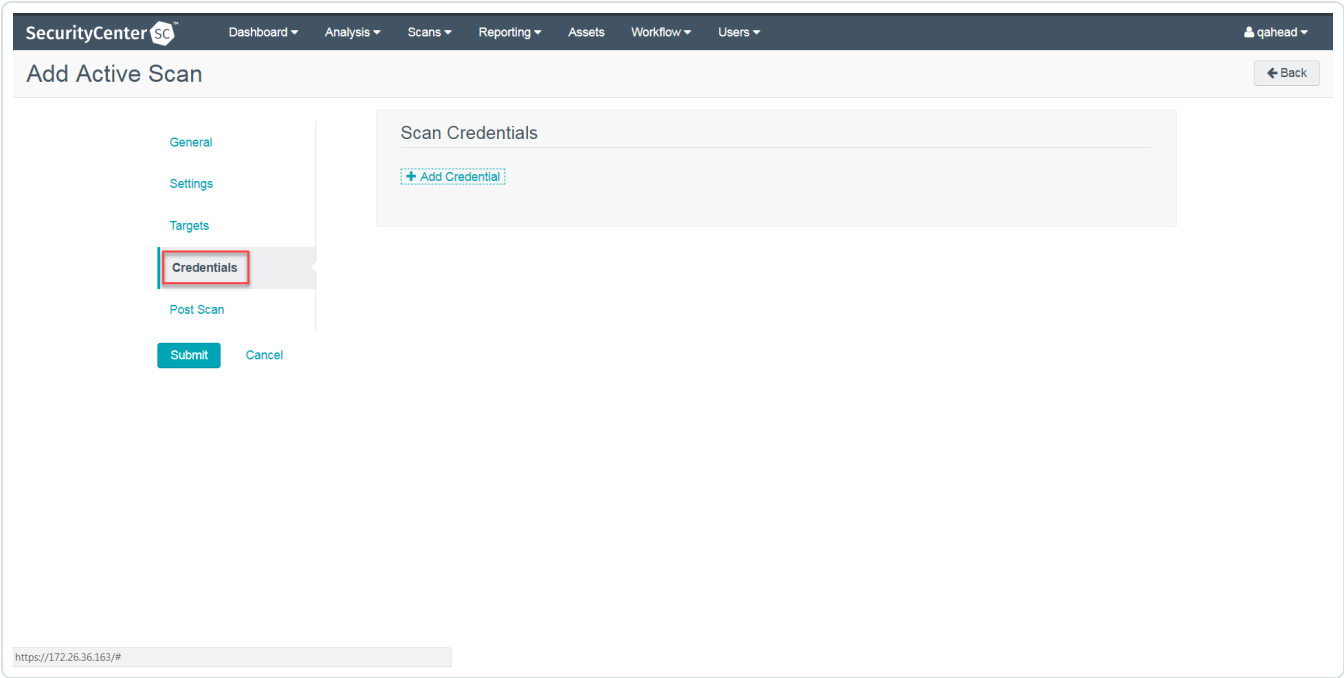
3. In the top right corner, click **+Add**.



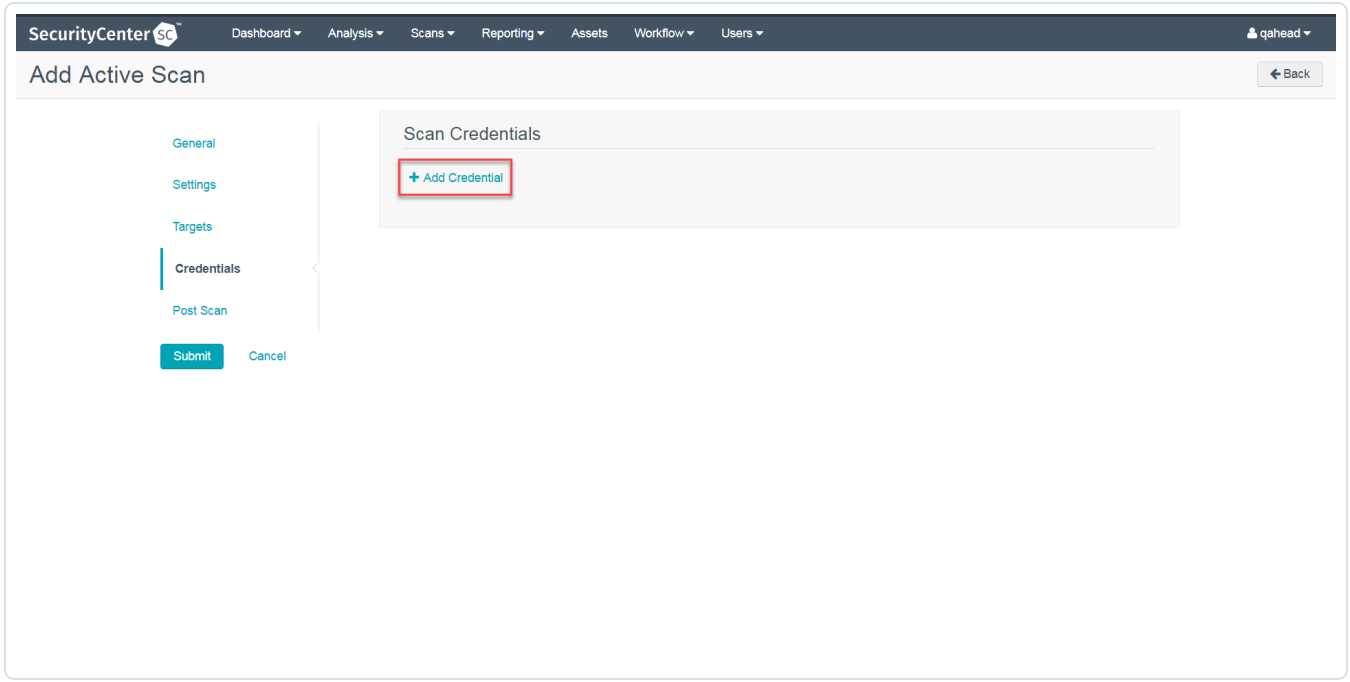
The **Add Active Scan** window opens.

4. In the left column, click **Credentials**.

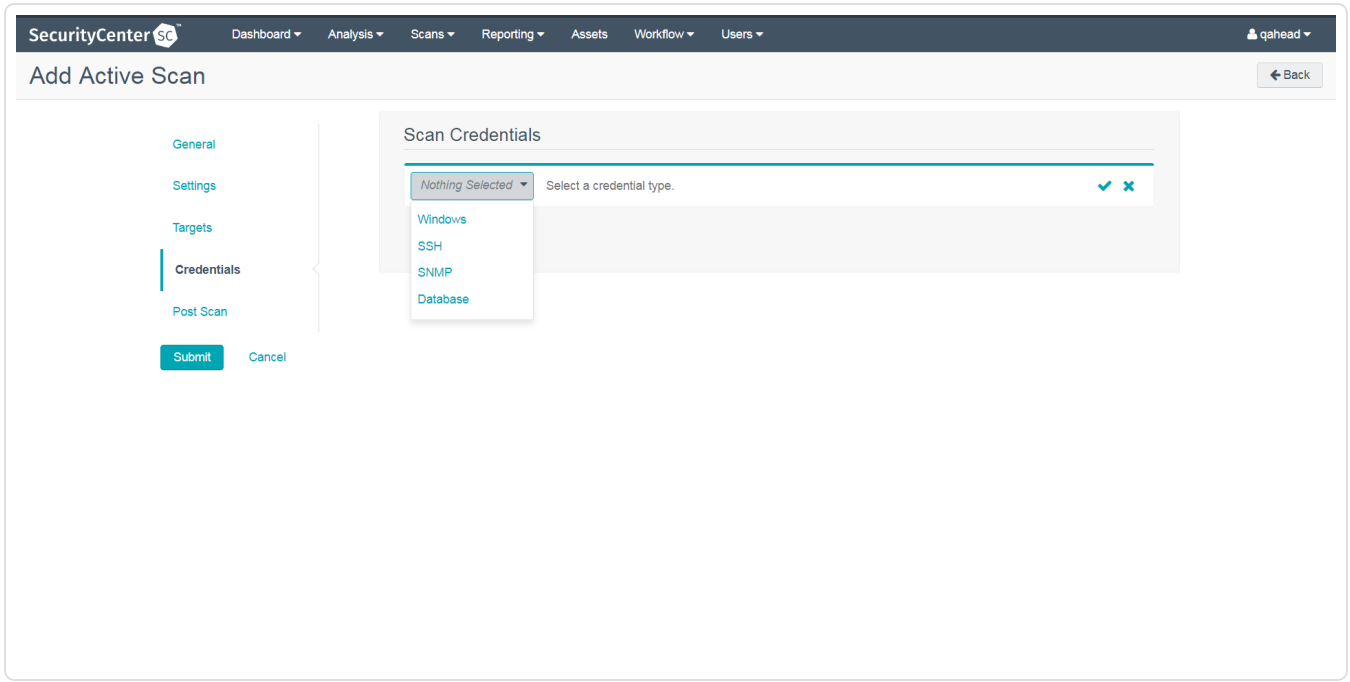
   The **Scan Credentials** section appears.



5. In the **Scan Credentials** section, click **+Add Credential**.



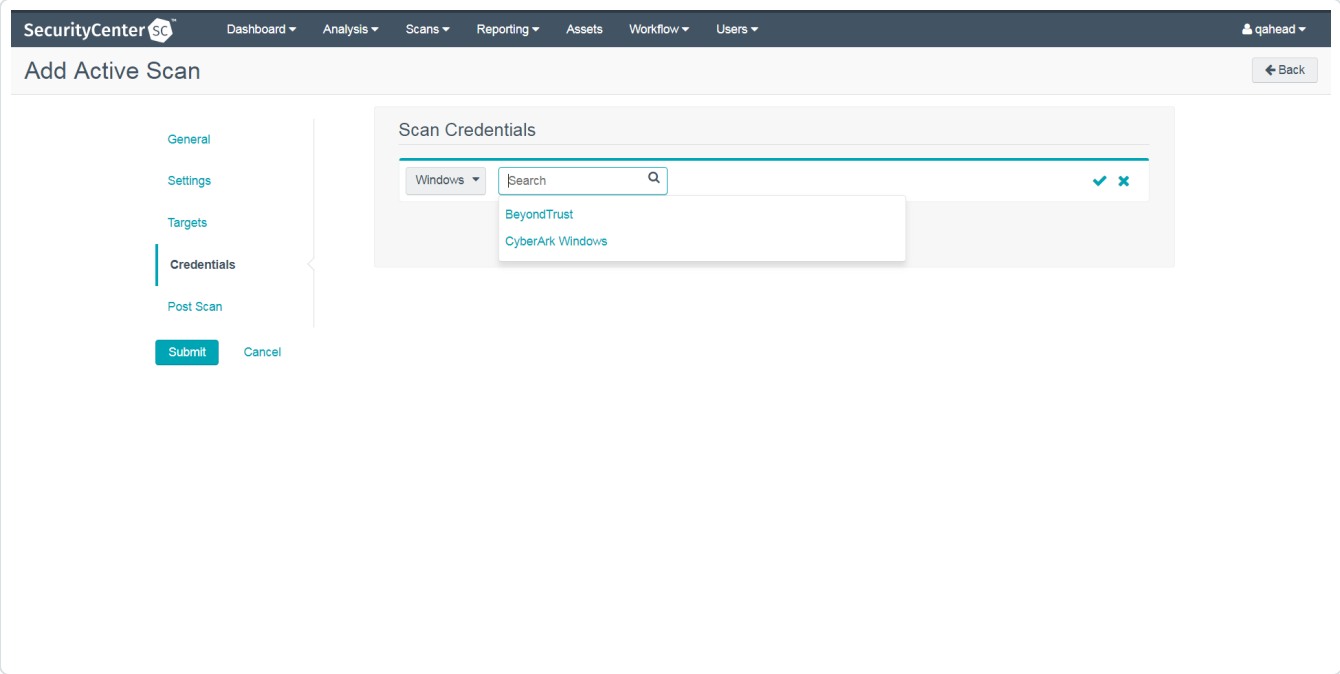
A drop-down appears.



6. Select the system type.

   The **Select Credential** option appears.

7. Click **Select Credential**.



A drop-down appears.

8. Select the previously created credential.
9. Enter information for the **General**, **Settings**, **Targets**, and **Post Scan** sections.
10. Click **Submit**.

Additional Information

CyberArk Domain and DNS Support

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

SecurtiyCenter Priority Scanning for CyberArk

SecurityCenter sets a priority system that allows for flexible querying. The following describes the order SecurityCenter tries values and the logic behind it.

1. SecurityCenter queries CyberArk with the target value entered into the SecurityCenter **Targets** configuration field. For example, if you put a FQDN in the target list, SecurityCenter 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, SecurityCenter 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 is contacted.
2. If the target value fails, SecurityCenter looks to see if there is a domain value (for a Windows system). If a domain value is present, SecurityCenter 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, SecurityCenter pulls the IP address of the system. If the IP address does not match one of the IP addresses supplied in the target list, SecurityCenter 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.

Retrieving Addresses to Scan from CyberArk

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

Debugging CyberArk

To enable debugging when you configure a scan in SecurityCenter, go to active scans > settings > diagnostic scan > plugin 84239. If a debug output for the system exists in the debug log, one or more of the following files will be present:

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

About Tenable

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