How-to Guide: SecurityCenter for CyberArk

Last Updated: March 27, 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.

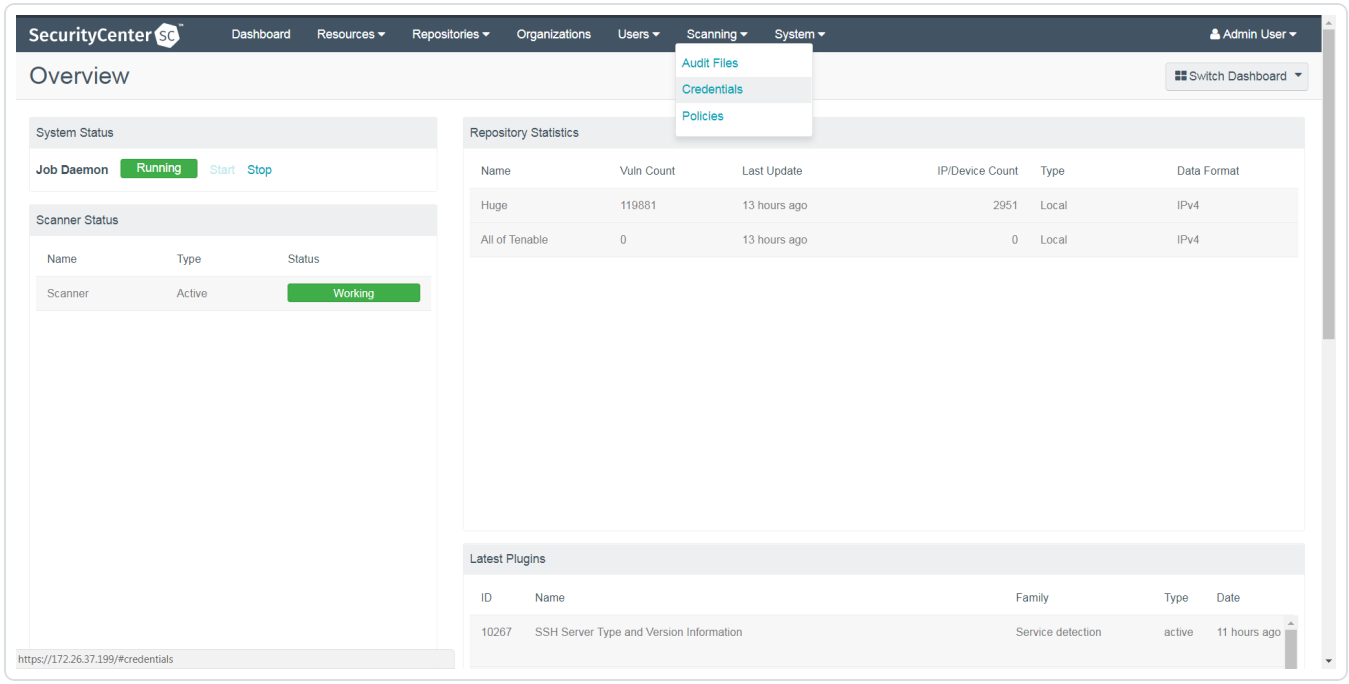
Benefits of integrating Tenable SecurityCenter with CyberArk Enterprise Password Vault include:

- 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

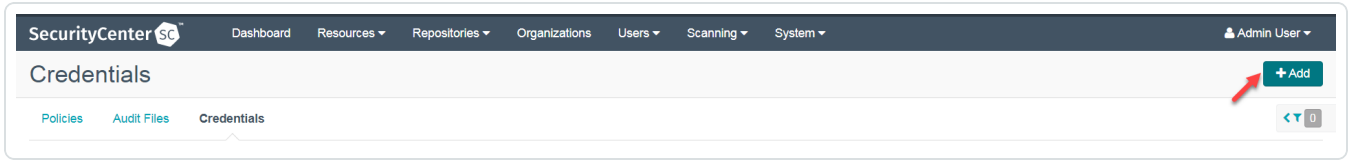
Integrating With CyberArk Enterprise Password Vault

Configuring credentialed network scans using CyberArk's password management solution is a simple process. CyberArk integration with SecurityCenter is seamless, so credentials are configured similarly to other credentialed network scans.

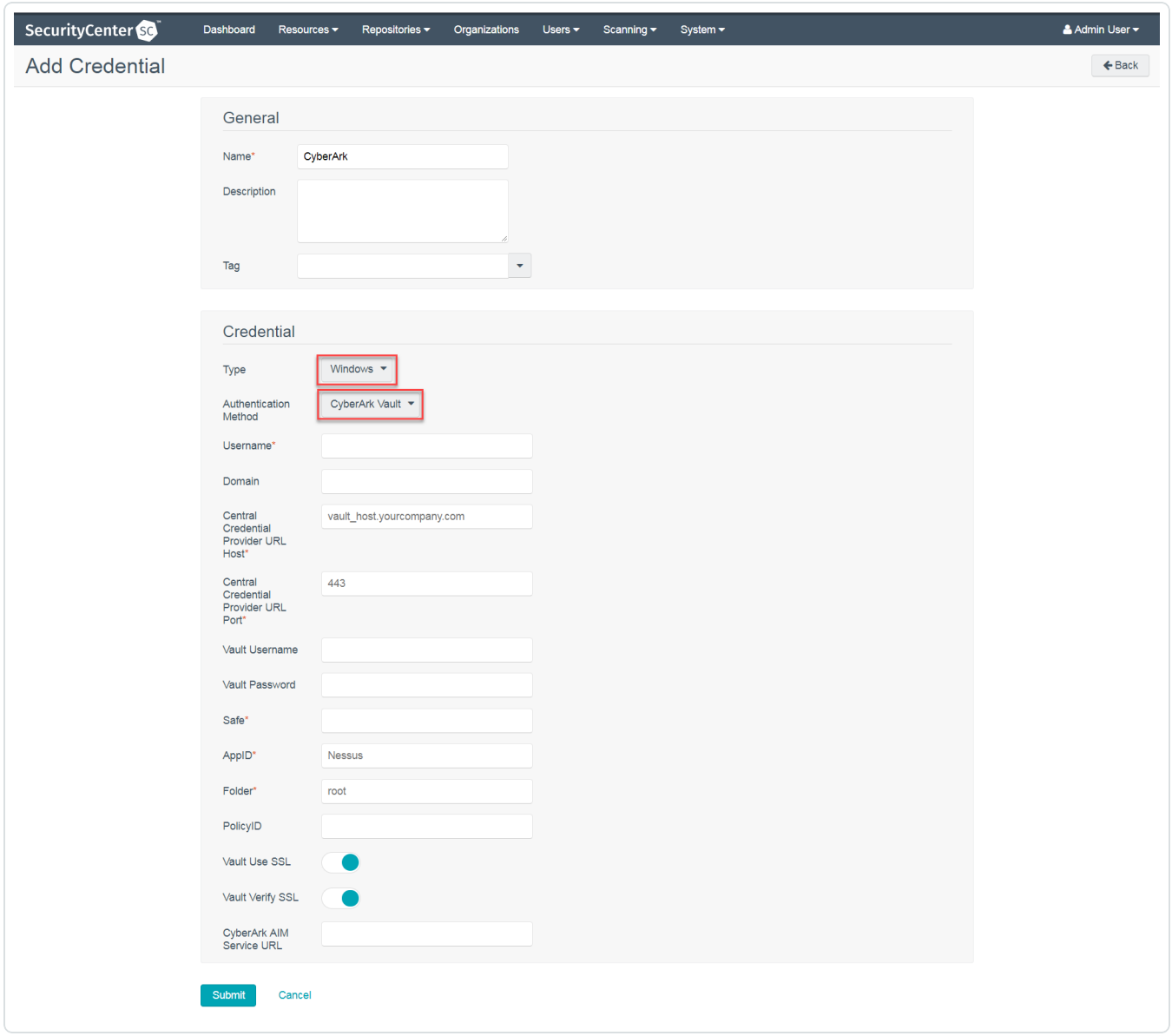
1. Log in to SecurityCener and click **Scanning** and select **Credentials** from the drop down menue to configure SecurityCenter for credentialed scans of Windows systems using CyberArk's password management solution.



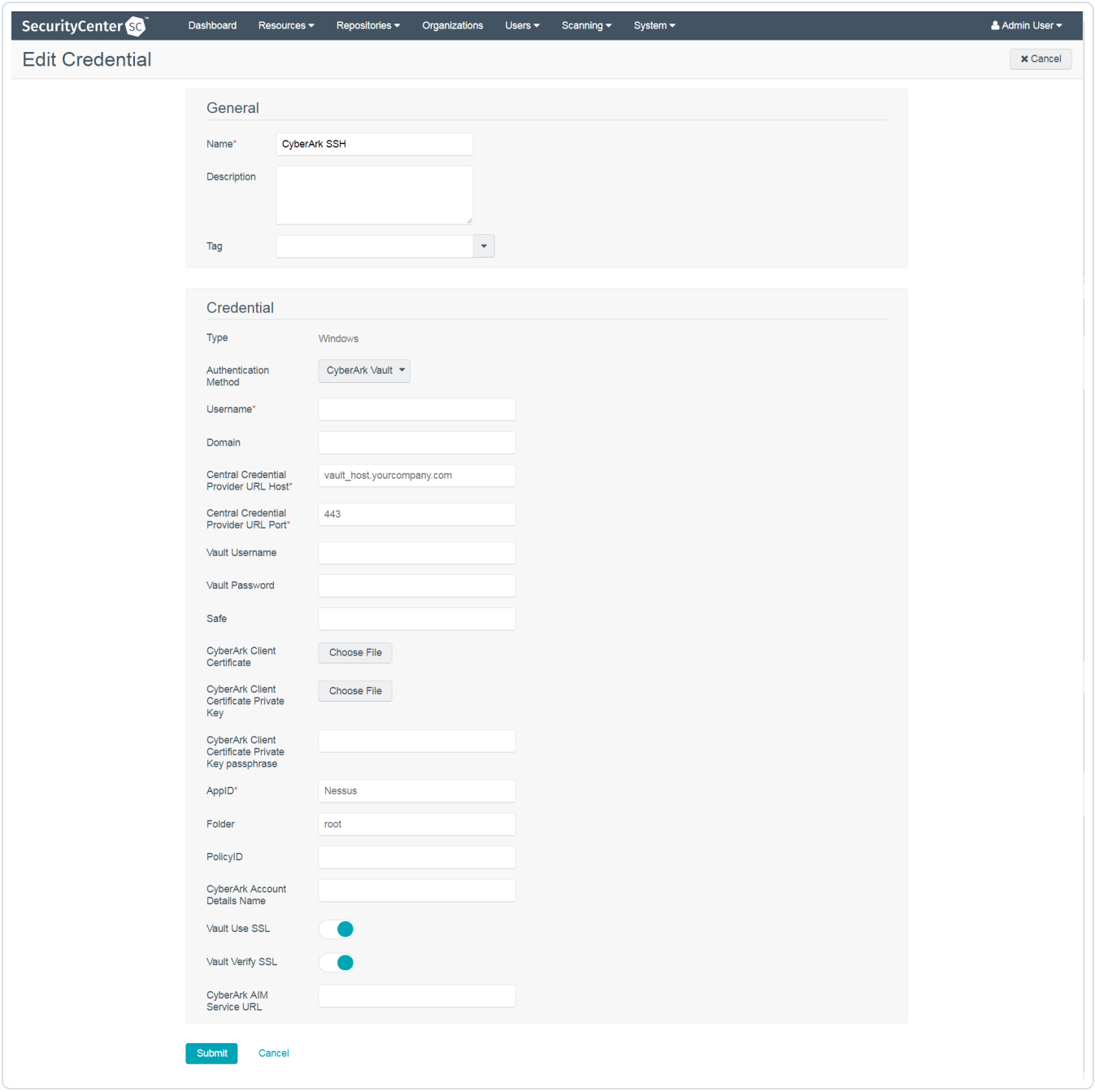
2. Click **+Add** at the top of the screen.



3. To configure a credentialed scan for Windows systems using CyberArk's password management solution, enter a descriptive **Name** and select **Windows** as the Type. For the **Authentication Method**, select **CyberArk Vault**.



4. After selecting the Authentication Method as **CyberArk Vault**, a new set of options will appear.



The table below contains a description of each option:

Option	Description
Username	The username for the target system.
Domain	The domain, if the username is part of a domain.
Central Credential Provider URL Host	The CyberArk Central Credential Provider IP/DNS

	address.
Central Credential Provider URL Port	The port the CyberArk Central Credential Provider is listening on.
Vault Username (optional)	The username for the vault, if the CyberArk Central Credential Provider is configured for basic authentication.
Vault Password (optional)	The password for the vault, if the CyberArk Central Credential Provider is configured for basic authentication.
Safe	The safe on the CyberArk Central Credential Provider server that contains the credentials you want to retrieve
CyberArk Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host.
CyberArk Client Certificate Private Key	The file that contains the PEM private key for the client certificate.
CyberArk Client Certificate Private Key Passphrase	The passphrase for the private key, if required.
AppID	The AppID with CyberArk Central Credential Provider permissions to retrieve the target password.
Folder	The folder on the CyberArk Central Credential Provider server that contains the credentials you want to retrieve.
PolicyID	The PolicyID assigned to the credentials you want to retrieve.
CyberArk Account Details Name	A unique string to identify the credential.
Vault Use SSL	When enabled, SecurityCenter uses SSL through IIS for secure communications. You must configure SSL through IIS in CyberArk Central Credential Provider before enabling this option.

Vault Verify SSL	When enabled, SecurityCenter validates the SSL certificate. You must configure SSL through IIS in CyberArk Central Credential Provider before enabling this option. For more information about using self-signed certificates, see the Nessus custom_CA.inc documentation.
CyberArk AIM Service URL	The URL for the CyberArk AIM web service. By default, SecurityCenter uses */AIMWebservice/v1.1/AIM.asmx*.

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).

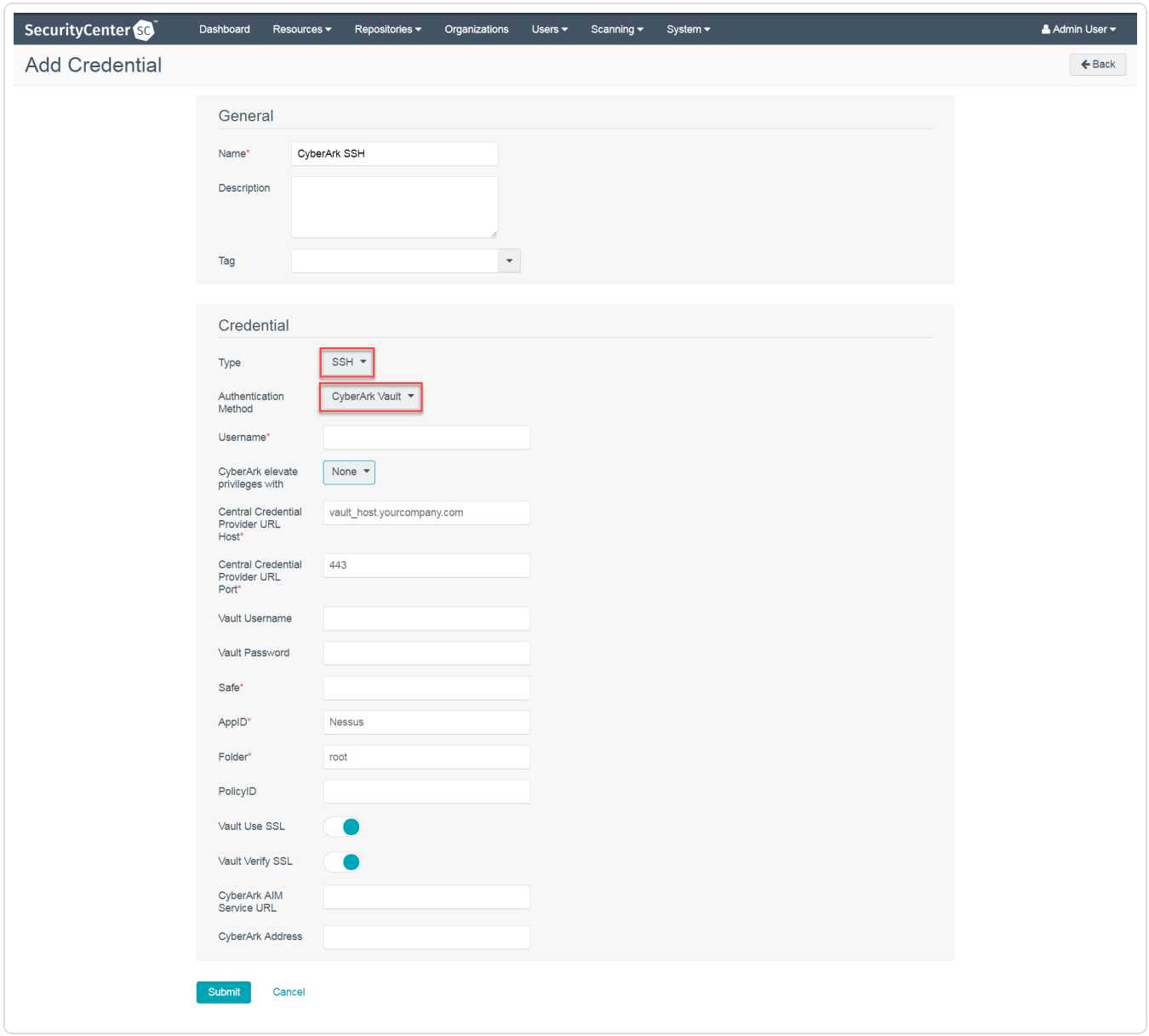
5. Once the options to reach the CyberArk Enterprise Password Vault are set, click **Submit** to save the changes.

Privilege Escalation With CyberArk Credentials

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

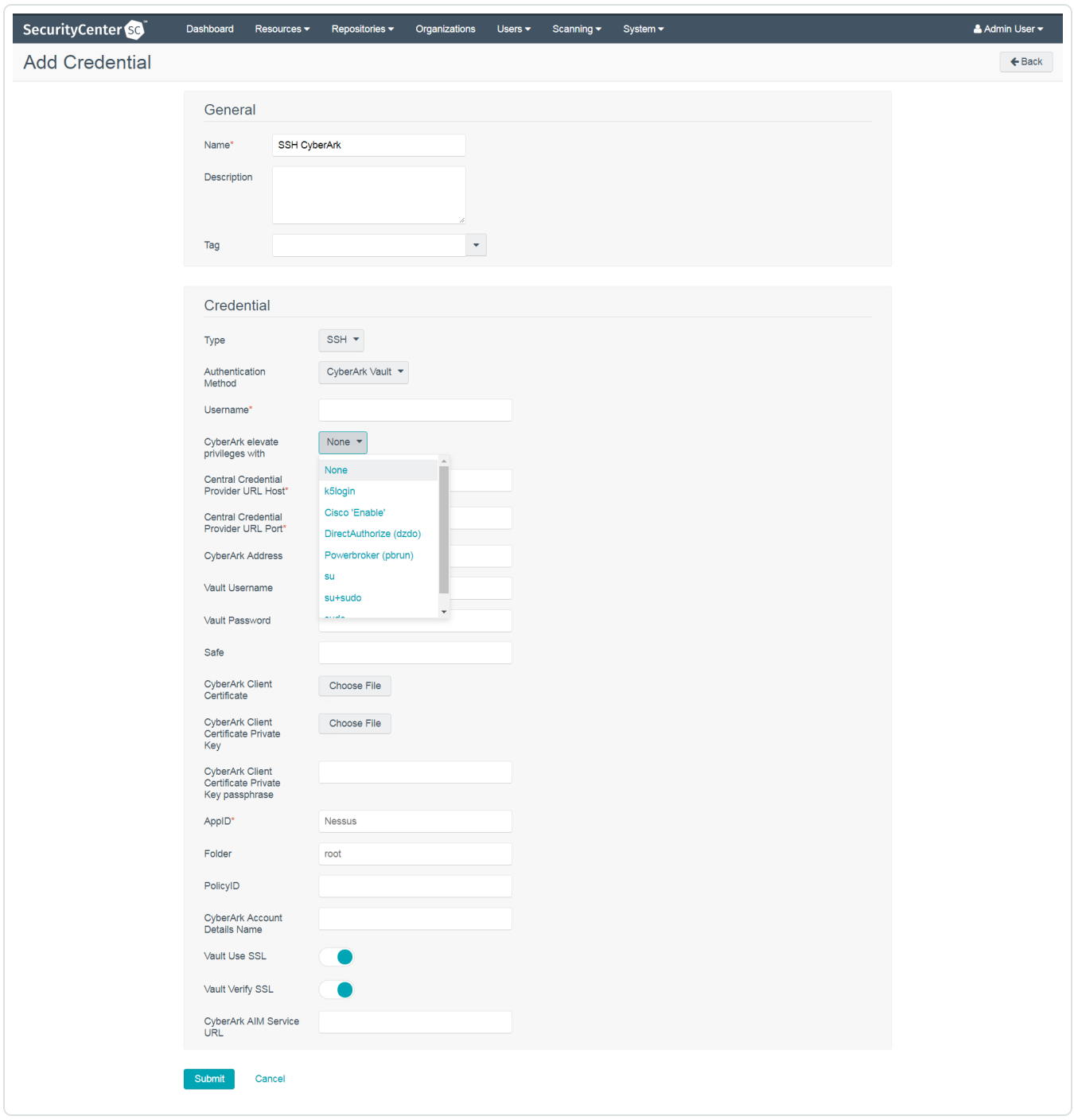
To add a CyberArk Password Vault credential set:

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

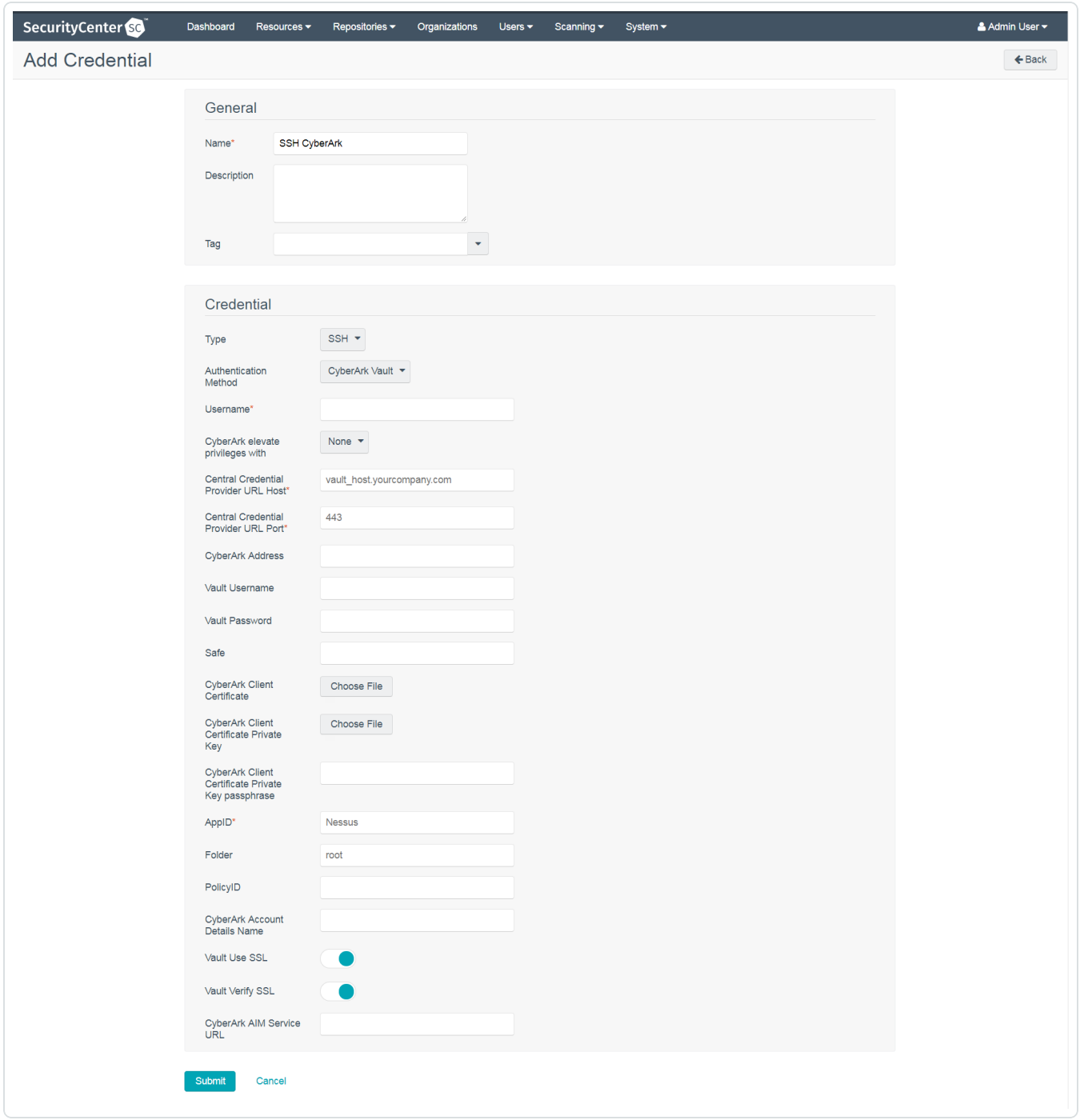


2. An option for **CyberArk elevate privileges with** appears near the bottom of the configuration

page. 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. Additional information about all of the supported privilege escalation types and their accompanying fields can be found in the SecurityCenter User Guide.



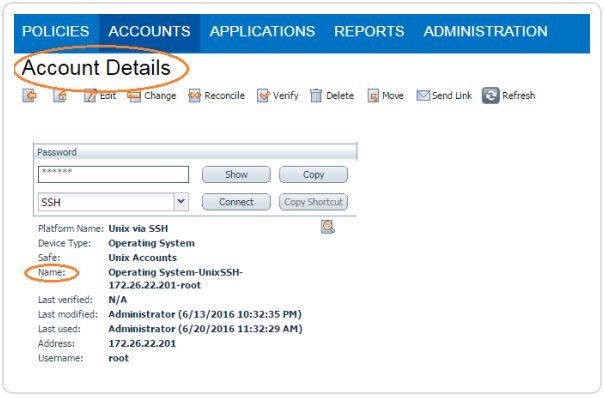
3. Configure each field for Windows authentication. Once the SSH credentials have been configured, click **Submit** to finalize the changes.



The table below contains a description of each option:

Option	Description
Username	The username for the target system.
CyberArk Elevate Privileges with	This item allows users to select or update

	options for SSH privilege escalation.
Central Credential Provider URL Host	The CyberArk Central Credential Provider IP/DNS address.
Central Credential Provider URL Port	The port the CyberArk Central Credential Provider is listening on.
CyberArk Address	The domain for the CyberArk account. You must configure SSL through IIS in CyberArk Central Credential Provider before configuring this option.
Vault Username (optional)	The username for the vault, if the CyberArk Central Credential Provider is configured for basic authentication.
Vault Password (optional)	The password for the vault, if the CyberArk Central Credential Provider is configured for basic authentication.
Safe	The safe on the CyberArk Central Credential Provider server that contains the credentials you want to retrieve
CyberArk Client Certificate	The file that contains the PEM certificate used to communicate with the CyberArk host.
CyberArk Client Certificate Private Key	The file that contains the PEM private key for the client certificate.
CyberArk Client Certificate Private Key Passphrase	The passphrase for the private key, if required.
AppID	The AppID with CyberArk Central Credential Provider permissions to retrieve the target password.
Folder	The folder on the CyberArk Central Credential Provider server that contains the credentials you want to retrieve.
PolicyID	The PolicyID assigned to the credentials you want to retrieve.

CyberArk Account Details Name	A unique string to identify the credential. **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. 
Vault Use SSL	When enabled, SecurityCenter uses SSL through IIS for secure communications. You must configure SSL through IIS in CyberArk Central Credential Provider before enabling this option.
Vault Verify SSL	When enabled, SecurityCenter validates the SSL certificate. You must configure SSL through IIS in CyberArk Central Credential Provider before enabling this option. For more information about using self-signed certificates, see the Nessus custom_CA.inc documentation.
CyberArk AIM Service URL	The URL for the CyberArk AIM web service. By default, SecurityCenter uses */AIMWebservice/v1.1/AIM.asmx*.

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 is set out to describe the order SecurityCenter tries values and the logic behind it.

1. SecurityCenter will query 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 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, SecurityCenter will then look to see if there is a domain value (for a Windows system). If a domain value is present, SecurityCenter 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, SecurityCenter 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, SecurityCenter 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

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 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

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.