



How-to Guide: Tenable SecurityCenter for Lieberman

Last Revised: November 16, 2018

Table of Contents

Welcome to SecurityCenter for Lieberman	3
Integrations	4
Windows Integration	5
SSH Integration	8
Database Integration	11
Add Credential to a Scan	12
Additional Information	16
Lieberman System	17
About Tenable	18

Welcome to SecurityCenter for Lieberman

This document provides information and steps for integrating SecurityCenter with Lieberman.

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 SecurityCenter with Lieberman, customers have more choice and flexibility.

The benefits of integrating SecurityCenter with Lieberman include:

- Credentials update directly in SecurityCenter, requiring less management.
- 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.

Integrations

The Lieberman system can be configured using either Windows or SSH. Full database support is also provided. Click the corresponding link to view the configuration steps.

[Windows Integration](#)

[SSH Integration](#)

[Database Integration](#)

[Add Credential to the Scan](#)

Windows Integration

Before you begin:

Caution: You must create an **Explicit Account** under **Delegation > Delegation Identities** in Lieberman. For additional information on how to create an Explicit Account, see the Explicit Accounts section in the [Lieberman RED Identity Management Administrator's Guide](#).

To integrate with Windows:

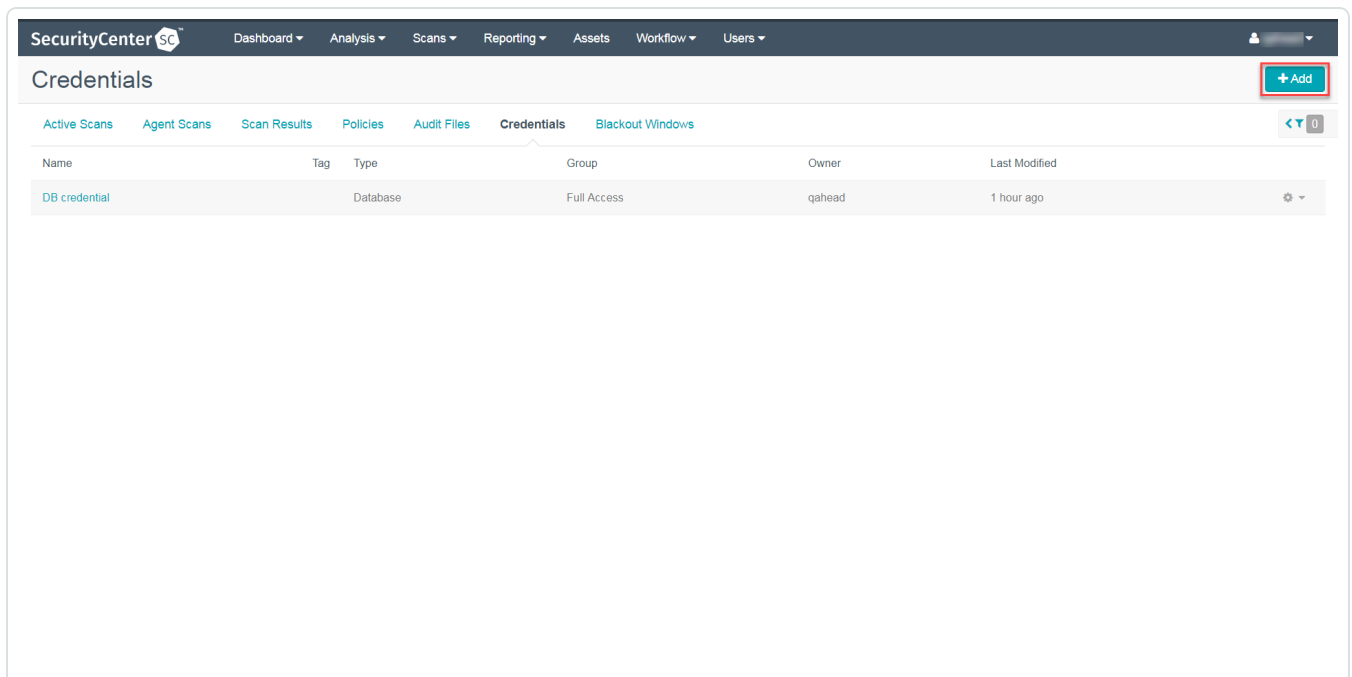
1. Log in to SecurityCenter.
2. In the top navigation bar, click **Scans**.

A drop-down appears.

3. Click **Credentials**.

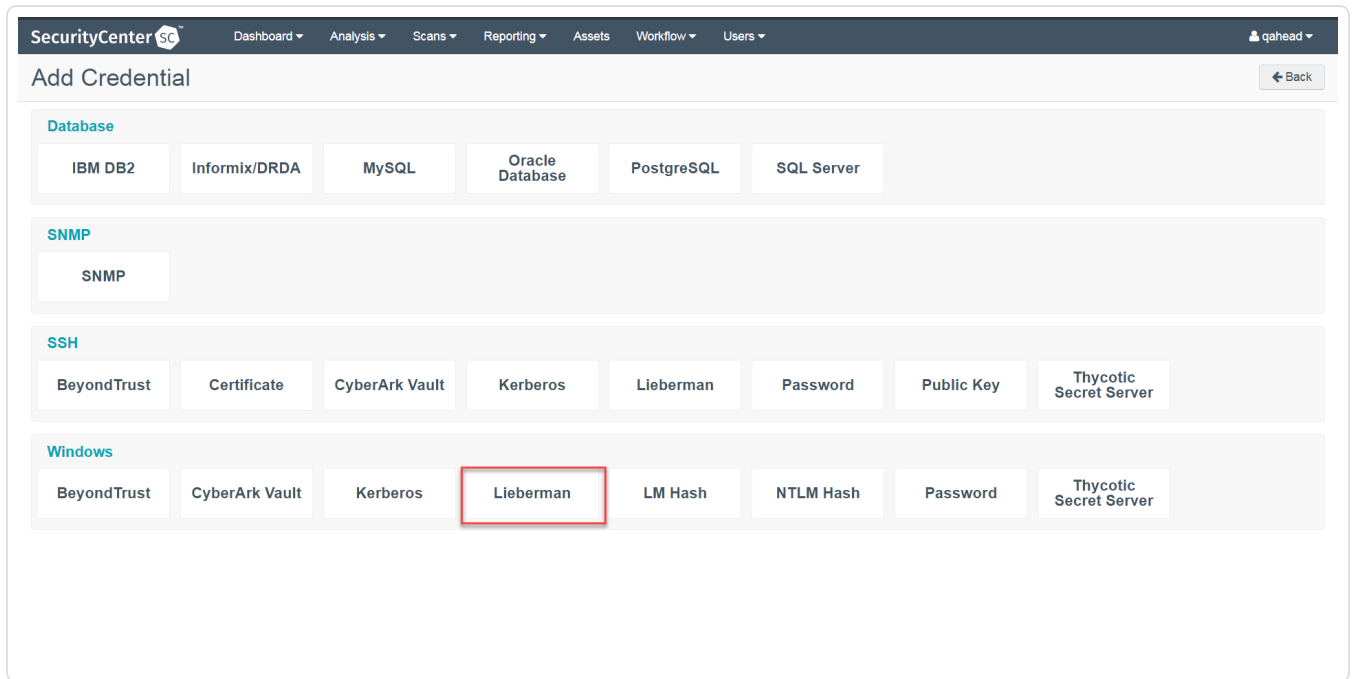
The **Credentials** window opens.

4. Click the **+ Add** button.

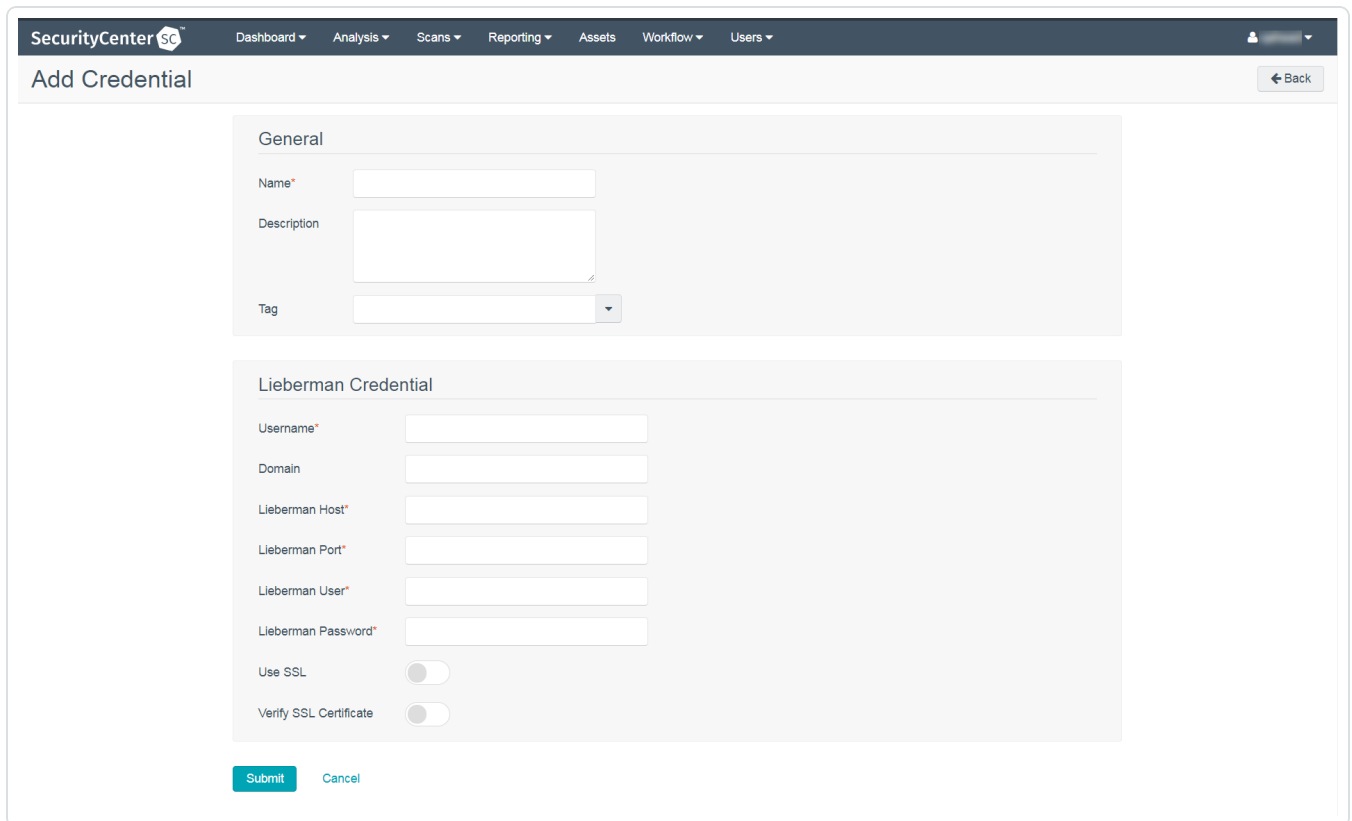


The **Add Credential** window opens.

5. In the **Windows** section, click **Lieberman**.



The **Add Credential** configuration page appears.



-
6. In the top section, enter a descriptive **Name** (required) , **Description** (optional), and **Tag** (optional).
7. Configure each field for **Windows** authentication. See the [SecurityCenter User Guide](#) to get detailed descriptions for each option.
8. Click **Save**.
9. Next, follow the steps for [adding the credential to a scan](#).

SSH Integration

Before you begin:

Caution: You must create an **Explicit Account** under **Delegation > Delegation Identities** in Lieberman. For additional information on how to create an Explicit Account, see the Explicit Accounts section in the [Lieberman RED Identity Management Administrator's Guide](#).

To integrate with SSH:

To configure a **SSH** credentialed network scan with Lieberman:

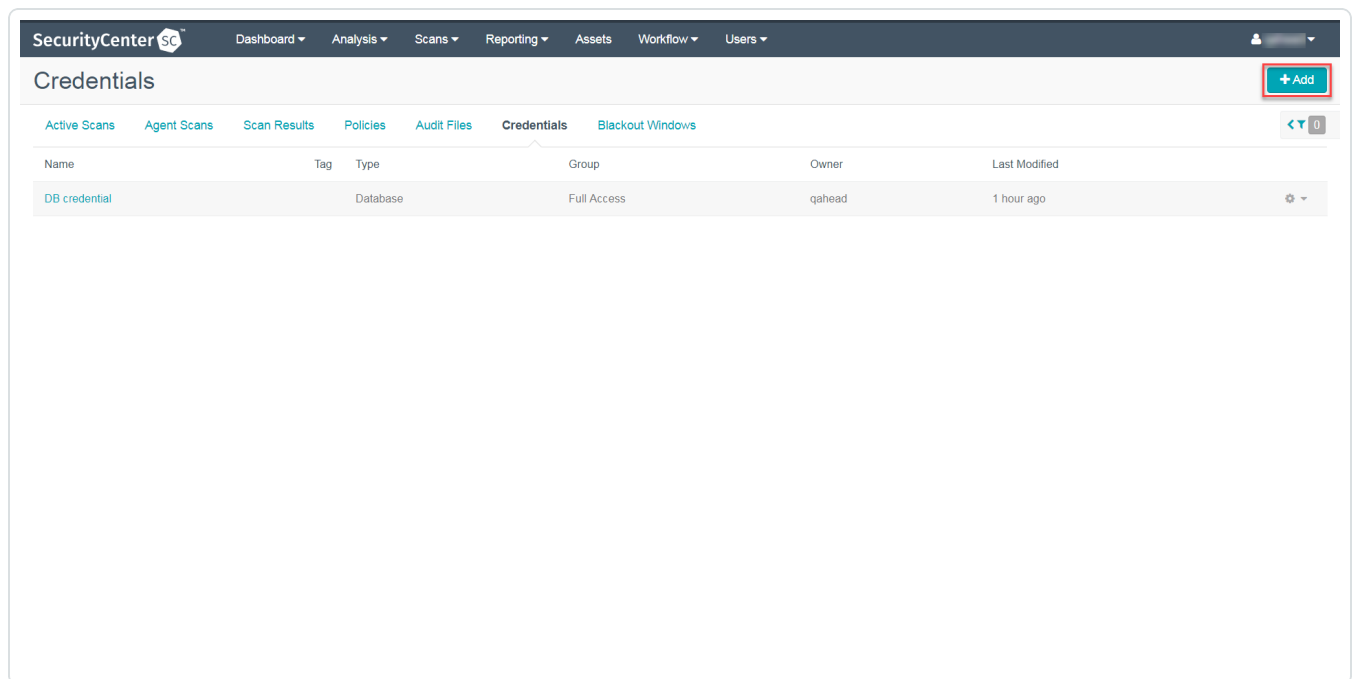
1. Log in to SecurityCenter.
2. In the top navigation bar, click **Scans**.

A drop-down appears.

3. Click **Credentials**.

The **Credentials** window opens.

4. Click the **+ Add** button.



The **Add Credential** window opens.

5. In the SSH section, click **Lieberman**.

The screenshot shows the 'Add Credential' page in the SecurityCenter interface. The page has a dark header with the SecurityCenter logo and navigation menus for Dashboard, Analysis, Scans, Reporting, Assets, Workflow, and Users. A user profile 'qahead' is visible in the top right. Below the header, the page title 'Add Credential' is displayed with a 'Back' button. The main content area is divided into four sections: Database, SNMP, SSH, and Windows. Each section contains a grid of buttons representing different credential types. In the SSH section, the 'Lieberman' button is highlighted with a red rectangular box. Other buttons in the SSH section include BeyondTrust, Certificate, CyberArk Vault, Kerberos, Password, Public Key, and Thycotic Secret Server. The Windows section also includes buttons for BeyondTrust, CyberArk Vault, Kerberos, Lieberman, LM Hash, NTLM Hash, Password, and Thycotic Secret Server.

The **Add Credential** configuration page appears.

The screenshot shows the configuration page for a Lieberman credential. The page title is 'Add Credential' with a 'Back' button. The configuration is organized into two main sections: 'General' and 'Lieberman Credential'. The 'General' section includes a 'Name*' text input field, a 'Description' text area, and a 'Tag' dropdown menu. The 'Lieberman Credential' section contains several required fields: 'Username*', 'Lieberman Host*', 'Lieberman Port*', 'Lieberman User*', and 'Lieberman Password*'. At the bottom of this section, there are two toggle switches: 'Use SSL' and 'Verify SSL Certificate'. At the very bottom of the page, there are 'Submit' and 'Cancel' buttons.

-
6. In the top section, enter a descriptive **Name** (required) , **Description** (optional), and **Tag** (optional).
7. Configure each field for **SSH** authentication. See the [SecurityCenter User Guide](#) to get detailed descriptions for each option.
8. Click **Save**.
9. Next, follow the steps for [adding the credential to a scan](#).

Database Integration

SecurityCenter provides full database support for Lieberman. Enable the plugins in the scanner to display them in the output.

To enable database plugins:

1. Go to the **Plugins** tab on the scan configurations page.
2. Click the **Status** button to enable the database plugin.
3. Click **Save**.

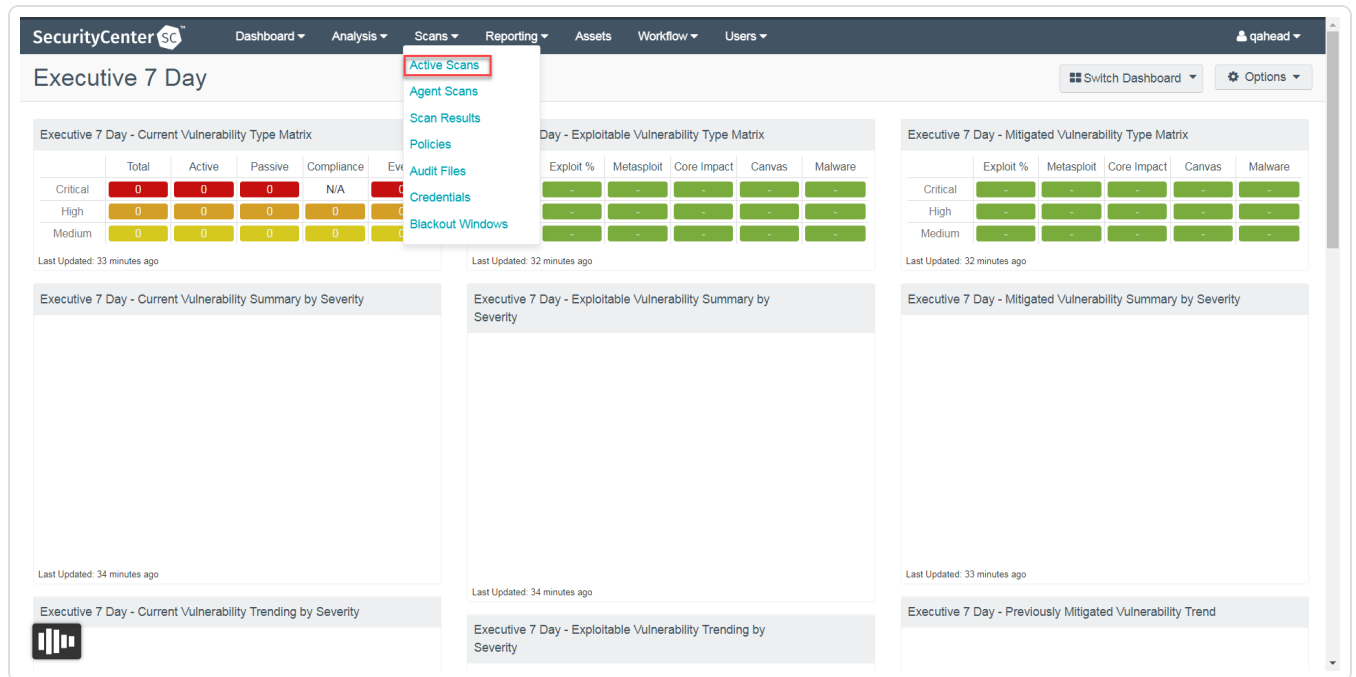
Note: See the chart for database plugin types and corresponding IDs.

Plugin Type	Plugin ID
MSSQL	91827
Oracle	91825
MySQL	91823
PostgreSQL	91826

Add Credential to a Scan

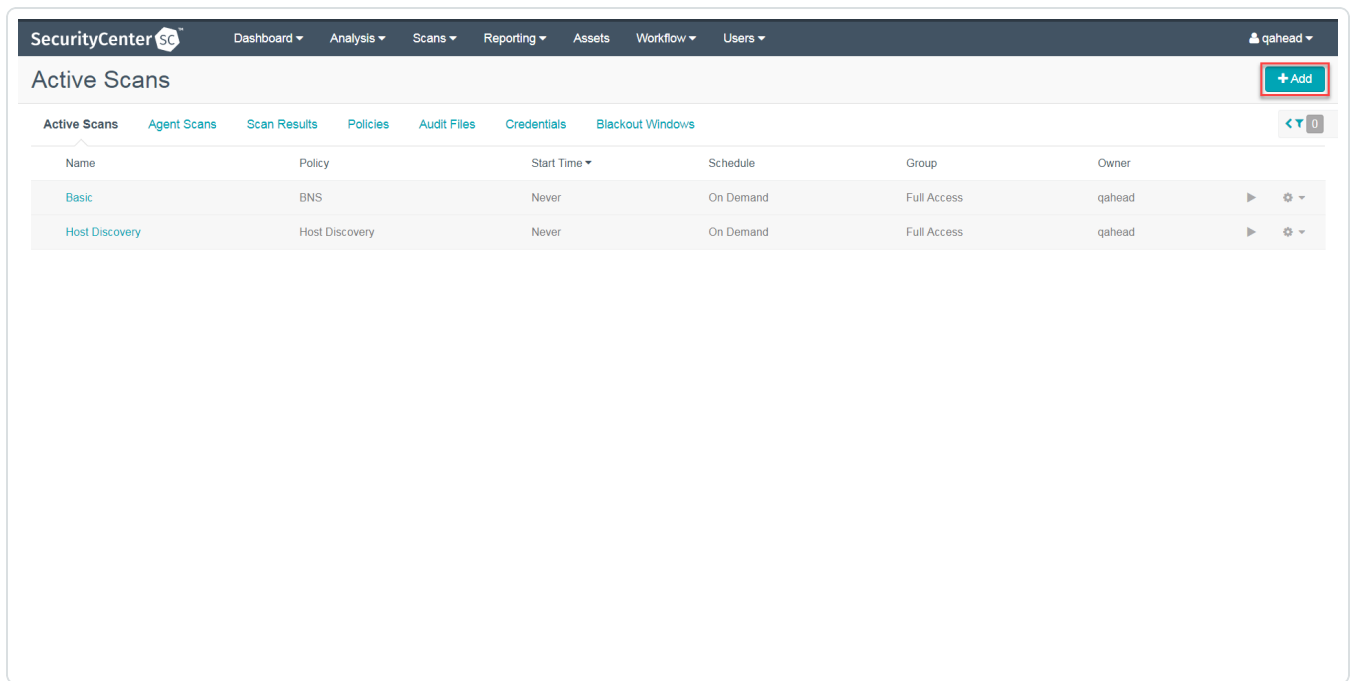
To add a Lieberman credential to a scan:

1. In the top navigation bar, click **Scans**.
A drop-down appears.
2. Select **Active Scans**.



The **Active Scans** window appears.

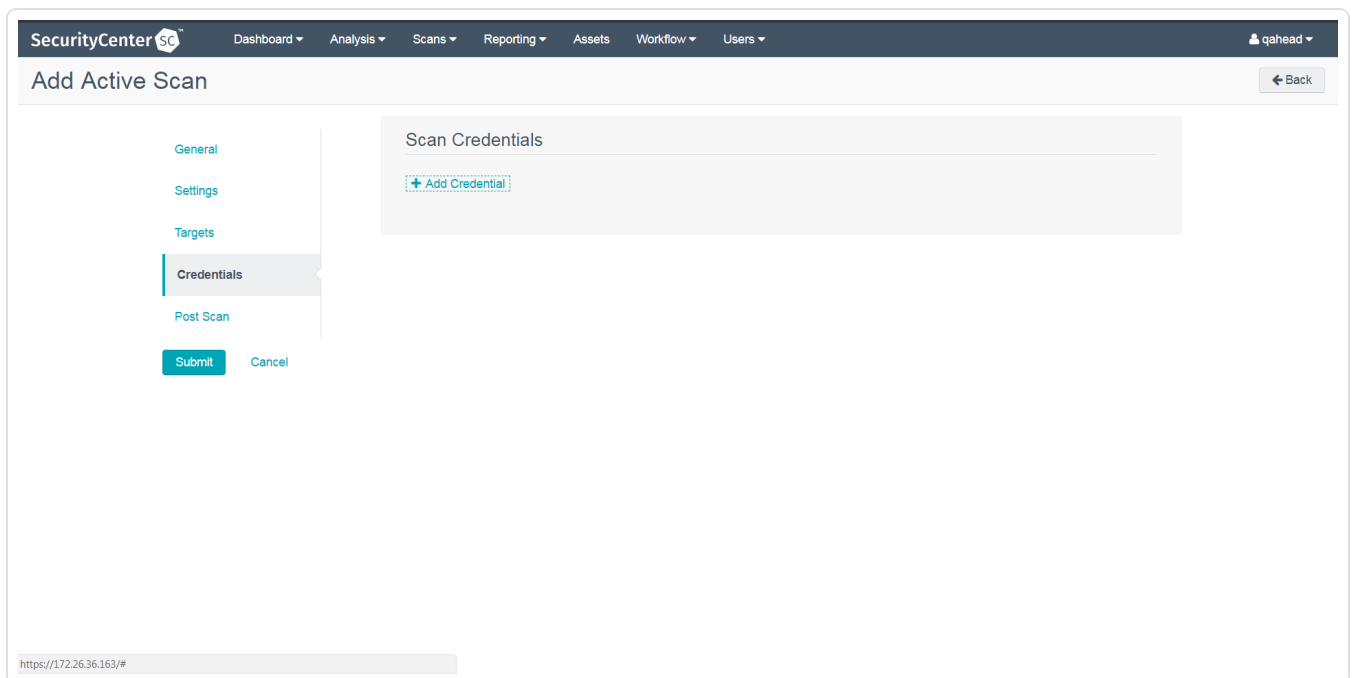
3. In the top right corner, click **+Add**.



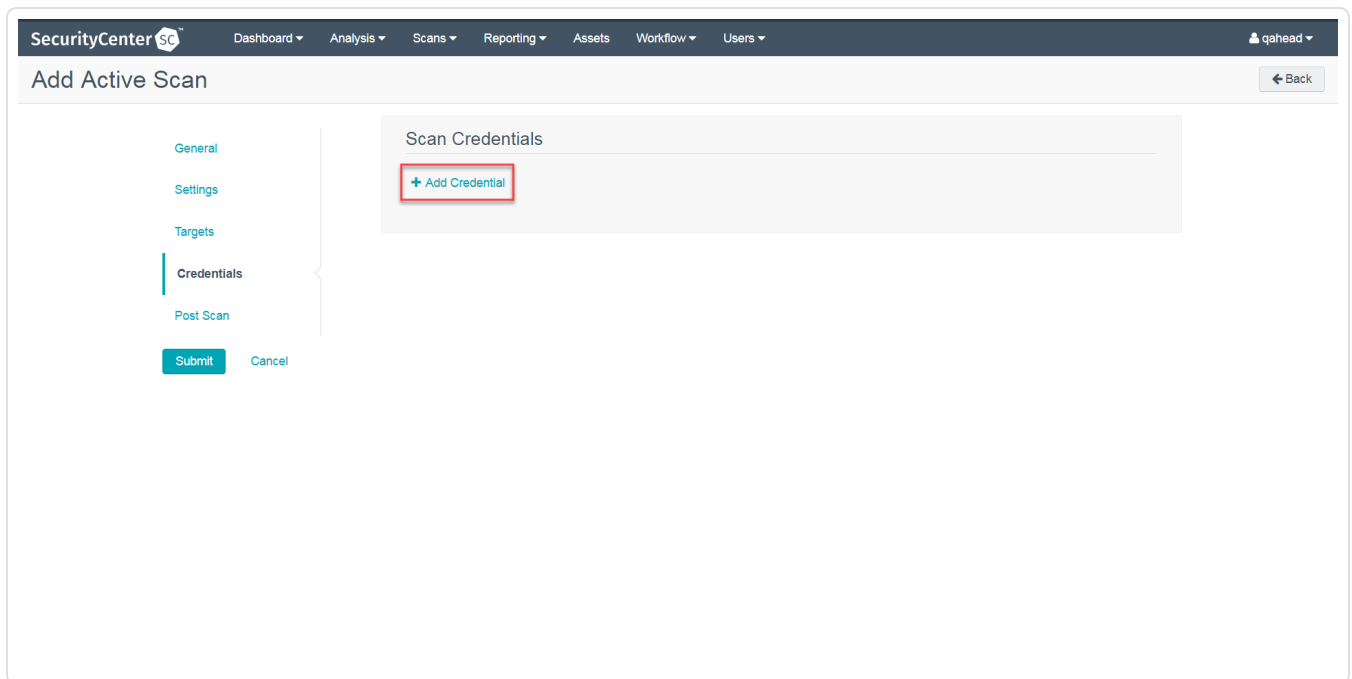
The **Add Active Scan** window appears.

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

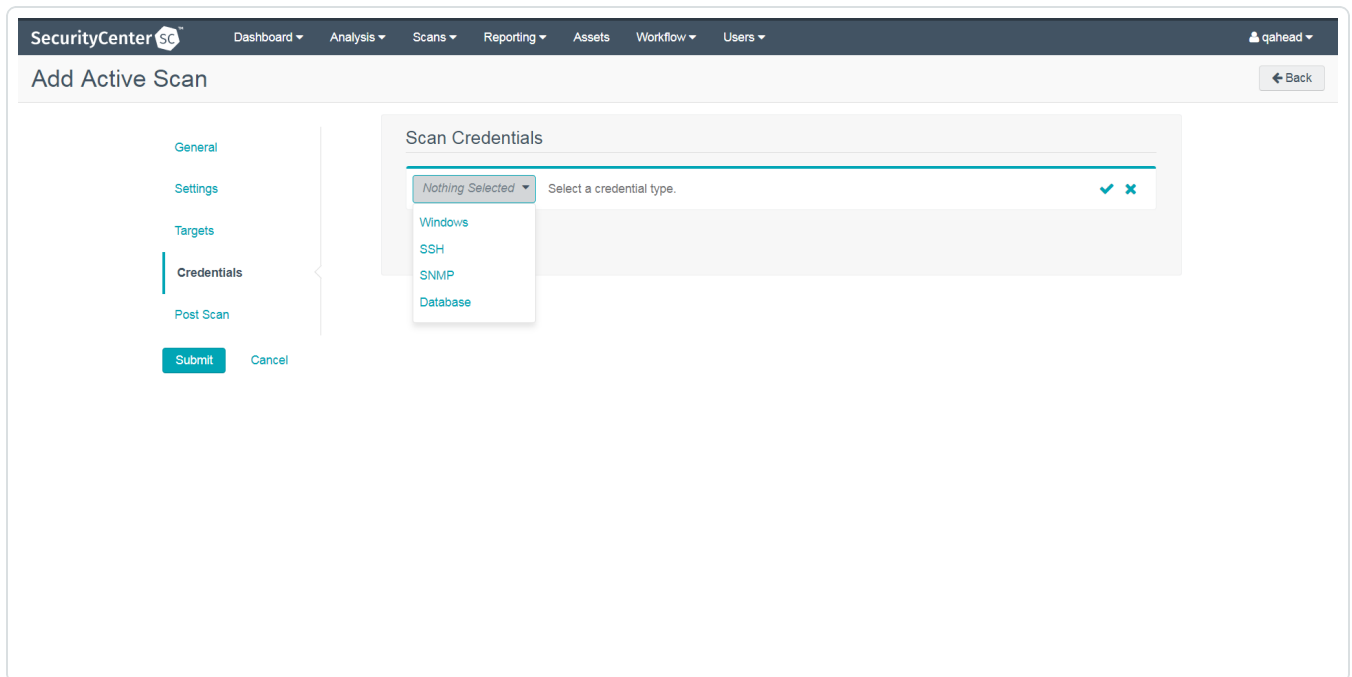
The **Scan Credentials** section appears.



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



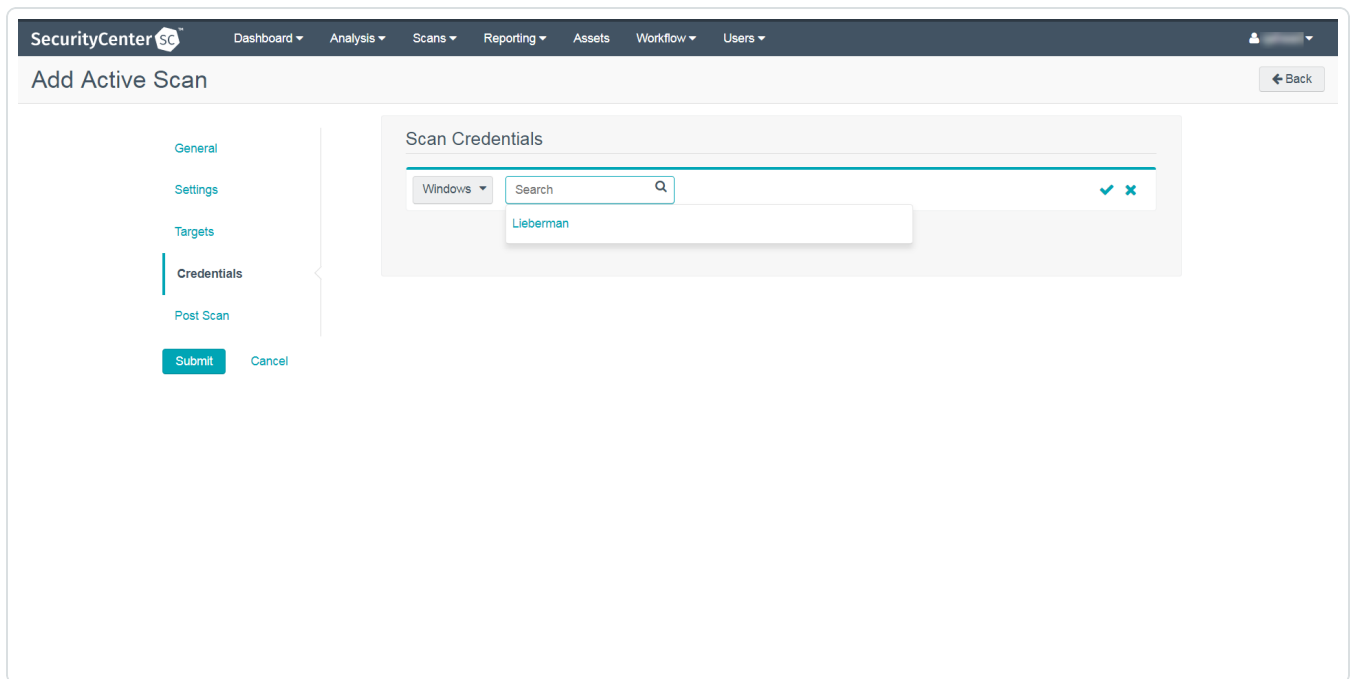
A drop-down appears.



6. Select the system type.

The **Select Credential** option appears.

7. Click **Select Credential**.



The screenshot shows the 'Add Active Scan' page in the SecurityCenter interface. The page has a dark header with the 'SecurityCenter' logo and navigation menus for Dashboard, Analysis, Scans, Reporting, Assets, Workflow, and Users. The main content area is titled 'Add Active Scan' and includes a 'Back' button. On the left, there is a sidebar with navigation options: General, Settings, Targets, Credentials (which is highlighted), and Post Scan. Below the sidebar are 'Submit' and 'Cancel' buttons. The main area displays a 'Scan Credentials' search box with a 'Windows' dropdown, a search input field containing 'Search', and a magnifying glass icon. A dropdown menu is open below the search box, showing a single result: 'Lieberman'. There are checkmark and close icons on the right side of the search box.

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

[Lieberman System](#)

[About Tenable](#)

Lieberman System

For additional information and documentation about the Lieberman system, go to <https://liebsoft.com/support/documentation/>.

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.