Tenable Security Center and Lieberman RED Integration Guide

Last Revised: August 31, 2023

Table of Contents

Welcome to Tenable Security Center for Lieberman

> **Caution:** Tenable's integration app for Lieberman is deprecated and is not supported beyond version 7.0. Contact BeyondTrust for the available alternatives or look towards another Tenable-supported PAM solution integration. For a list of supported integrations, see Tenable's [Partner Page](#) and [Integrations documentation page.](#)

This document provides information and steps for integrating Tenable Security Center 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 Tenable Security Center with Lieberman, customers have more choice and flexibility.

The benefits of integrating Tenable Security Center with Lieberman include:

- Credentials update directly in Tenable Security Center, 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](#).
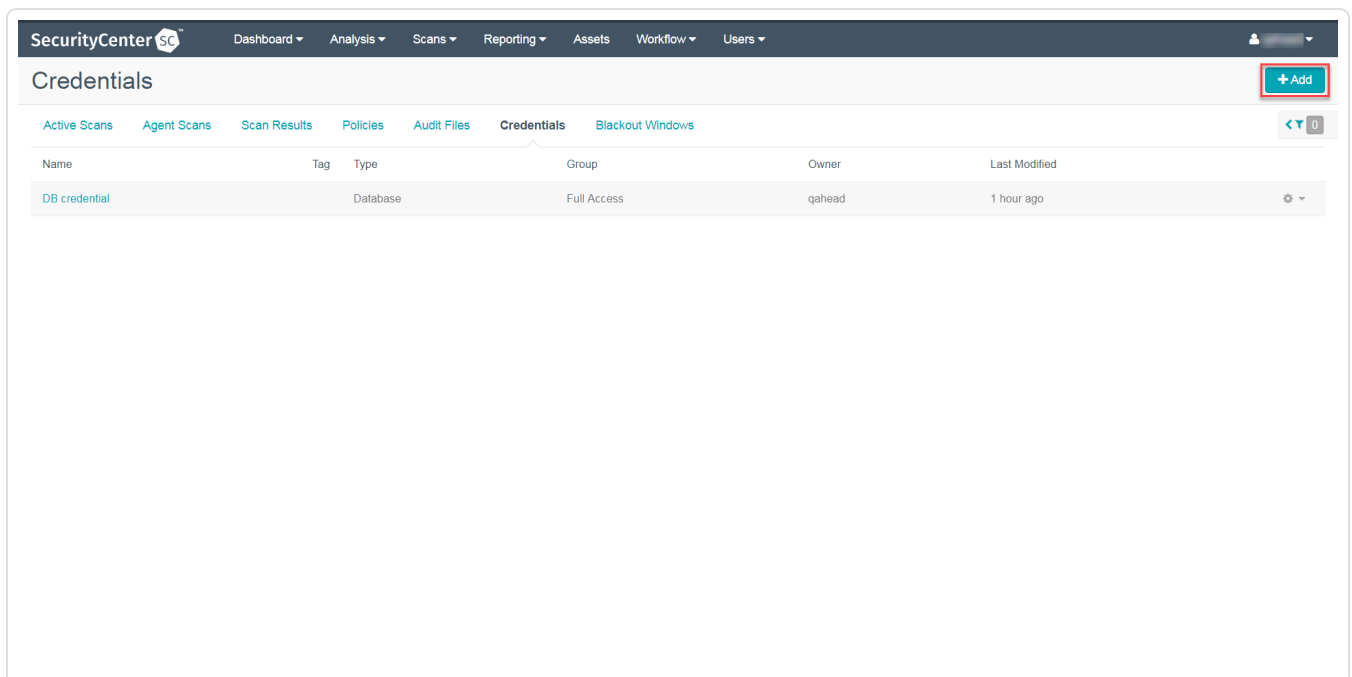
To integrate with Windows:

1. Log in to Tenable Security Center.

2. In the top navigation bar, click **Scanning**.

   A drop-down appears.
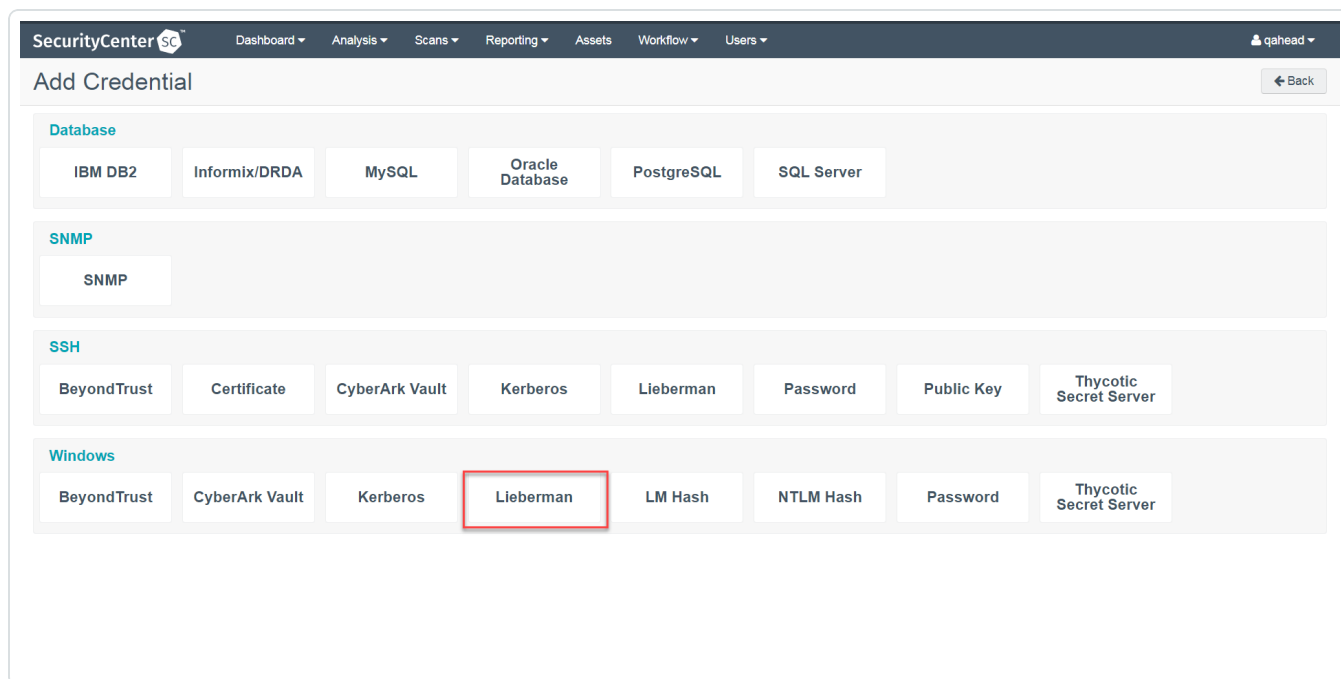
3. Click **Credentials**.

   The **Credentials** window opens.
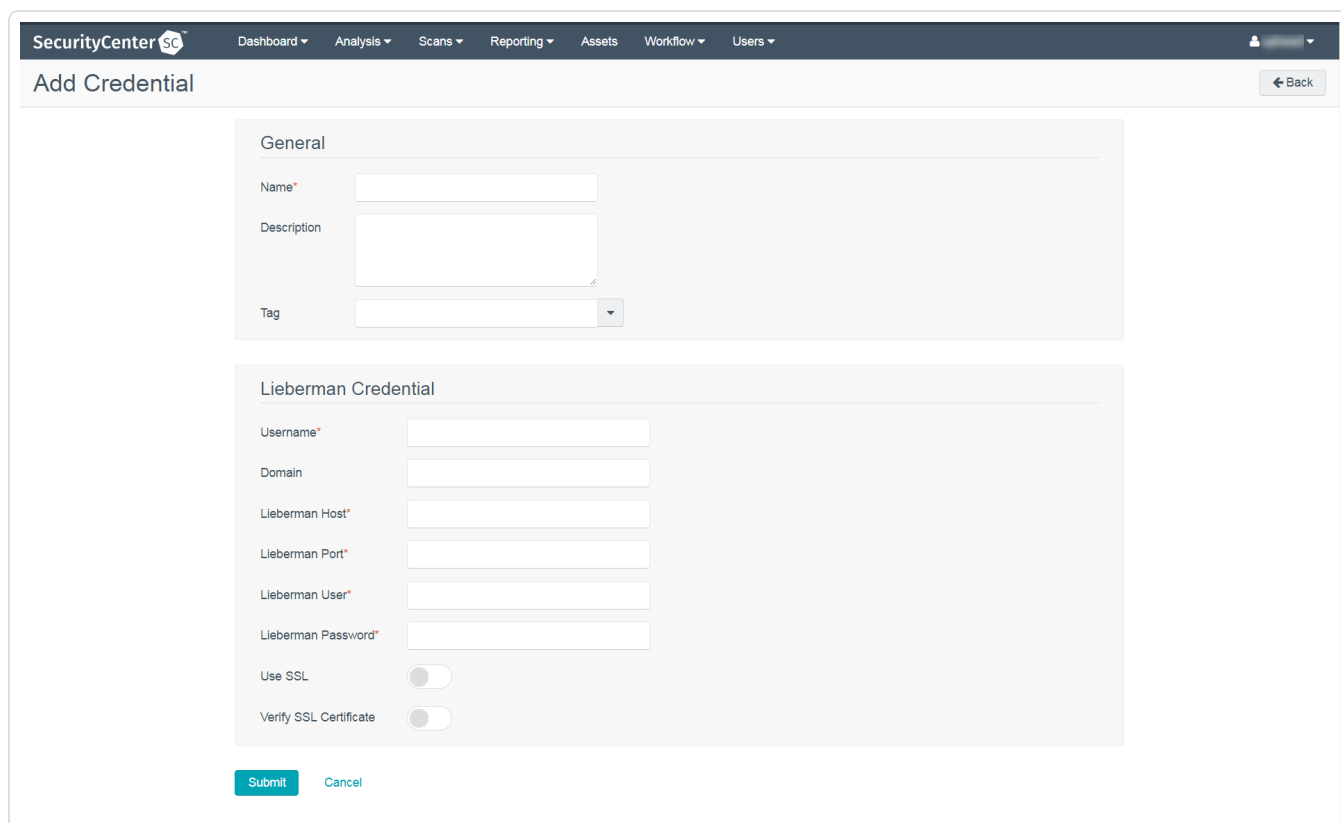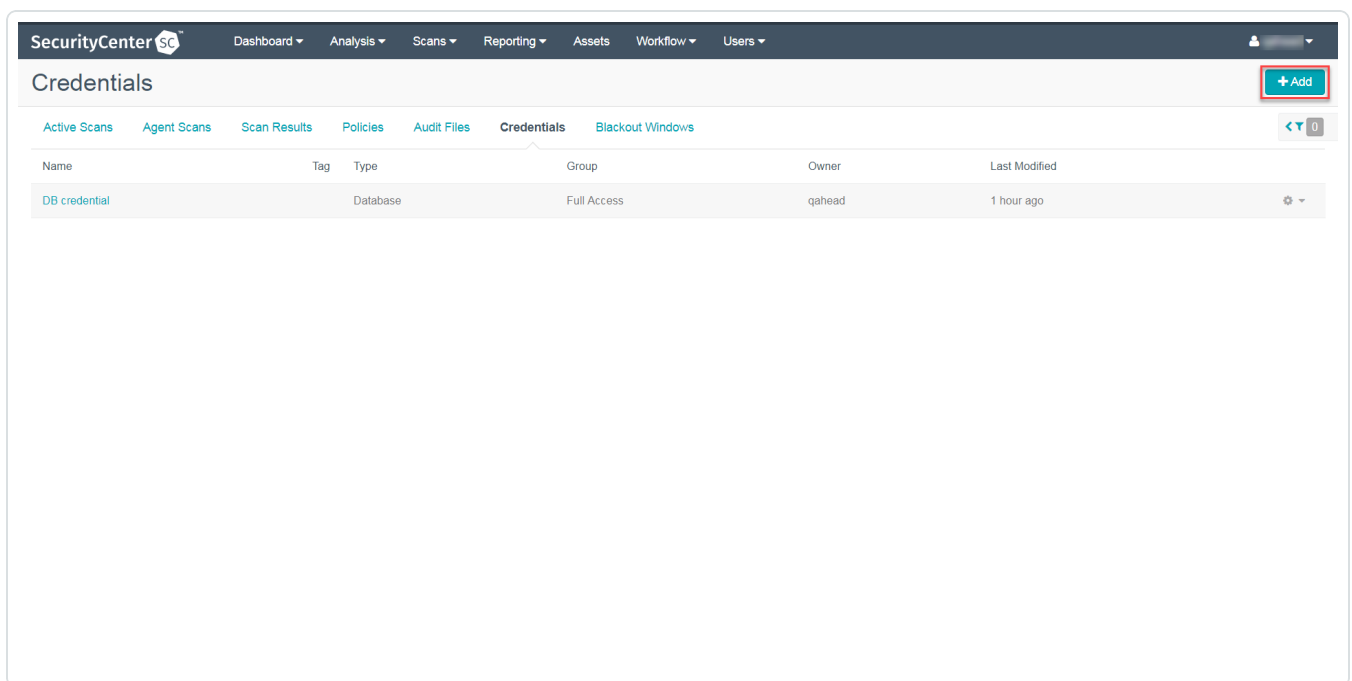
4. Click the **+ Add** button.

   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 [Tenable Security Center 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 Tenable Security Center.

2. In the top navigation bar, click **Scanning**.

   A drop-down appears.
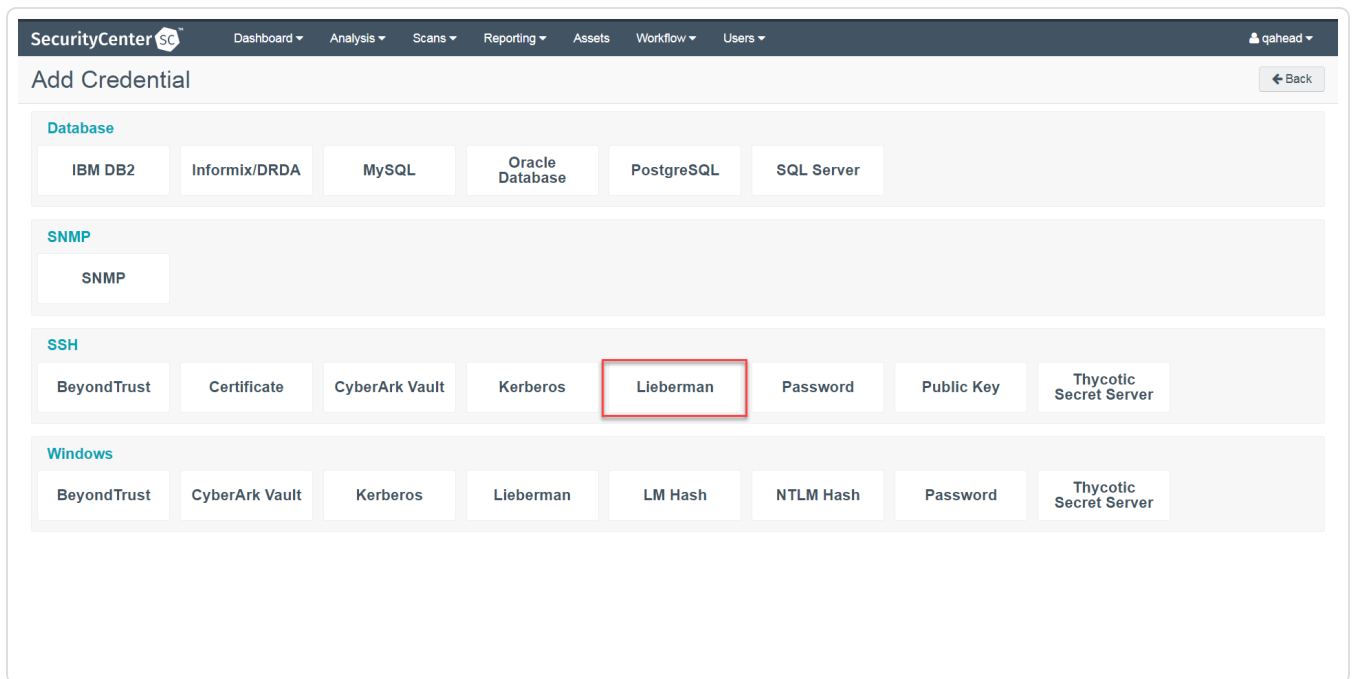
3. Click **Credentials**.

   The **Credentials** window opens.
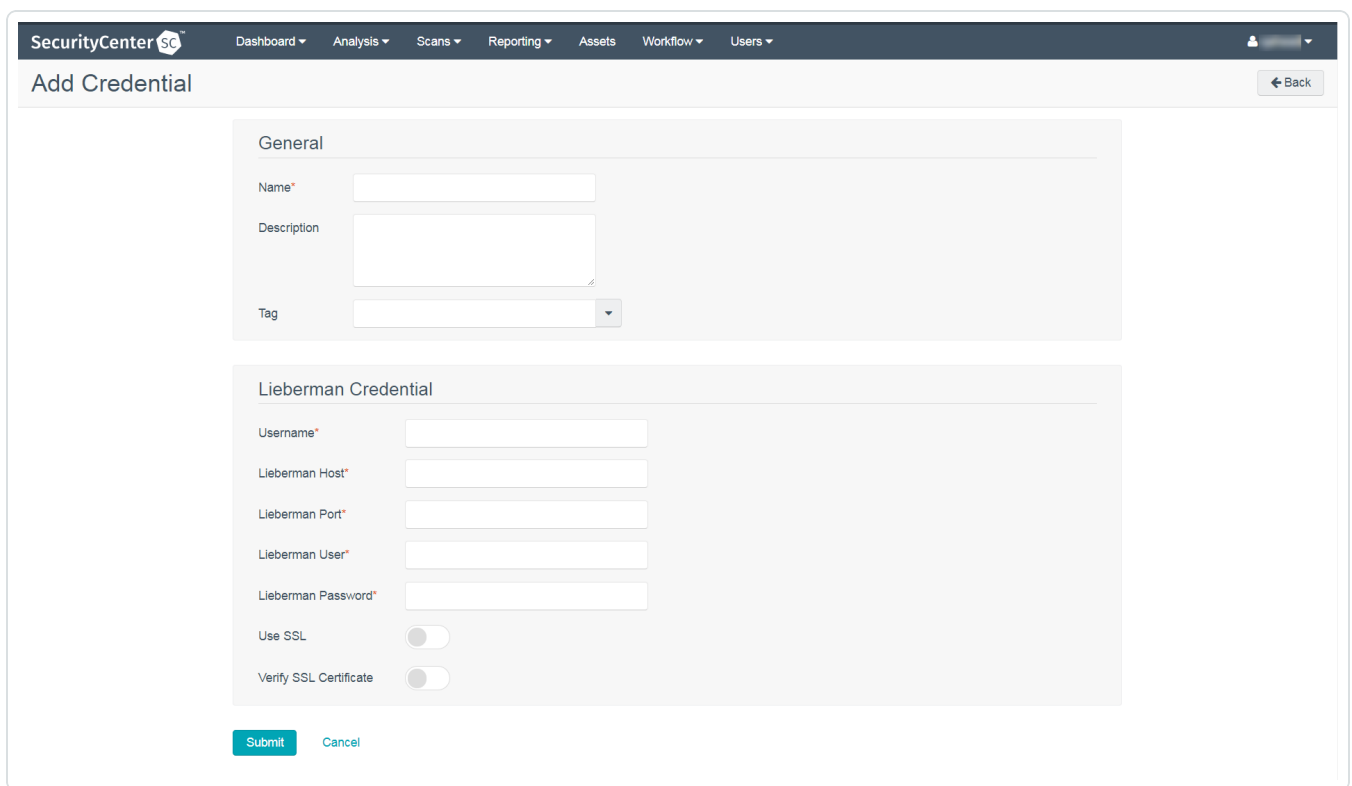
4. Click the **+ Add** button.

   The **Add Credential** window opens.

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

The **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 **SSH** authentication. See the [Tenable Security Center User Guide](#) to get detailed descriptions for each option.

8. Click **Save**.

9. Next, follow the steps for [adding the credential to a scan](#).

Configure Database Integration

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

To configure database integration:

1. Log in to Tenable Security Center.

2. Click **Scanning** > **Credentials**.

   The **Credentials** page appears.

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

   The **Add Credential** page appears.

4. In the **Database** section, click **Oracle Database**.
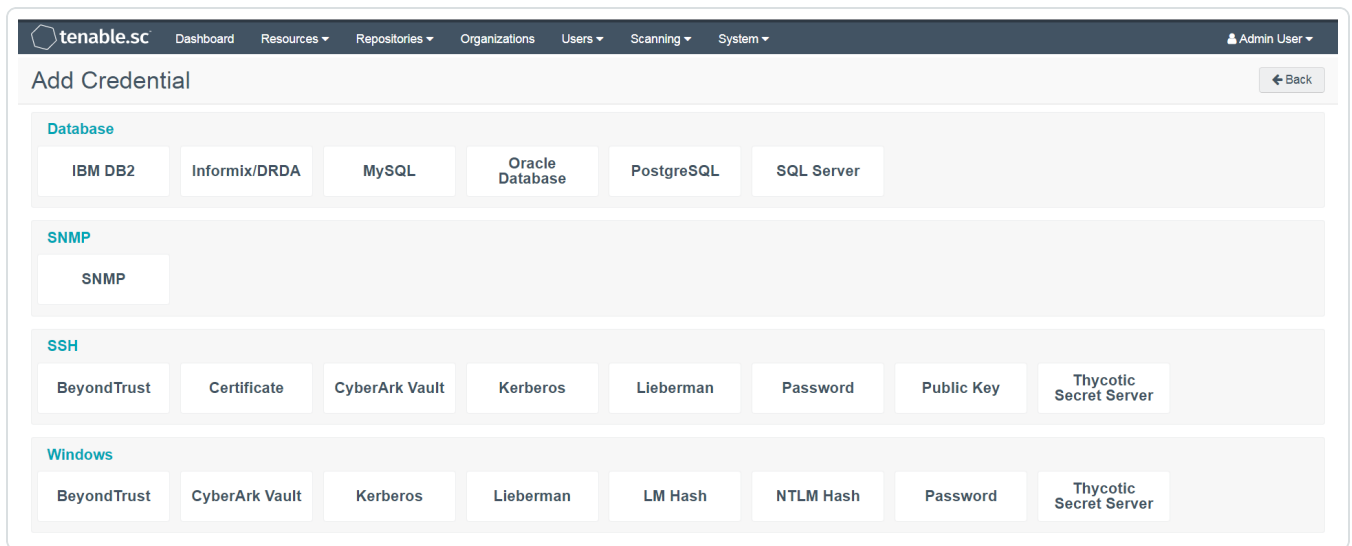
   The **Add Credential** page appears.

5. In the **Name** field, type a descriptive name.

6. (Optional) In the **Description**n field, type a description.

7. (Optional) In the **Tag** drop-down, select a tag.

8. In the **Authentication Method** drop-down, select **Lieberman**.

The **Lieberman** options appear.

9. Configure each option for the **Oracle Database** authentication. See the [Database Credentials](#) section in the Tenable Security Center User Guide to get detailed descriptions for each option.

10. Click **Submit**.

What to do next:

- Next, follow the steps to [Add a Credential to a Scan](#).

Enable Database Plugins

To enable database plugins:

1. Complete the steps on the [Configure Options Plugin](#) page in the Tenable Security Center User Guide.

   See the chart for database plugin types and corresponding IDs.

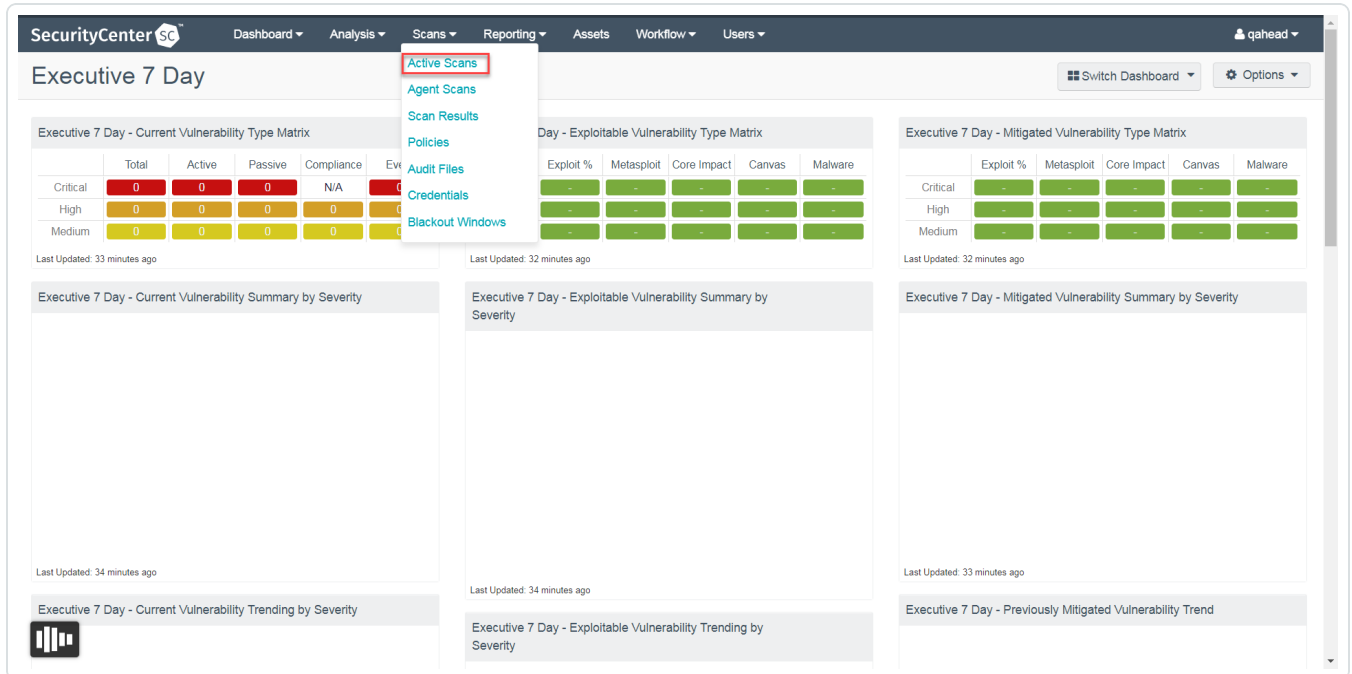 | Plugin Type | Plugin ID |
   | --- | --- |
   | MSSQL | 91827 |
   | Oracle | 91825 |
   | MySQL | 91823 |
   | PostgresSQL | 91826 |

2. Click **Save**.

Add a Credential to a Scan

To add a Lieberman credential to a scan:

1. In the top navigation bar in Tenable Security Center, click **Scans**.
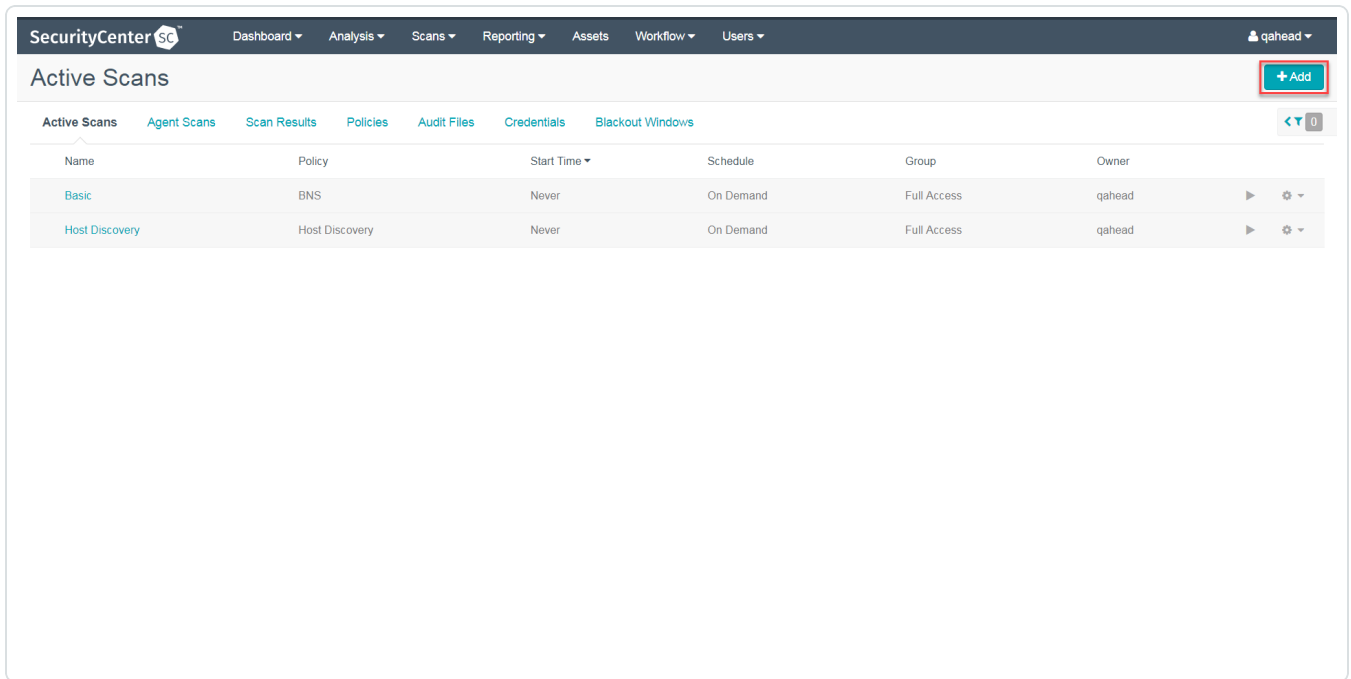
   A drop-down appears.

2. Select **Active Scans**.

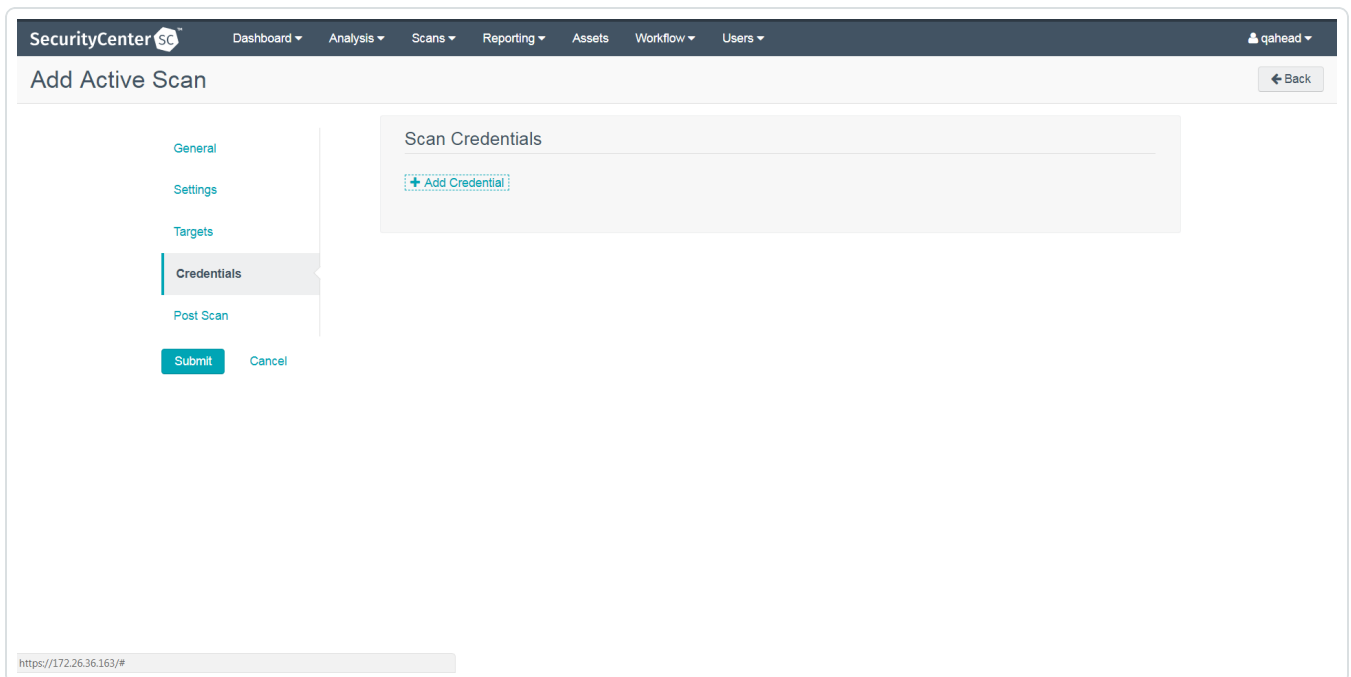

The **Active Scans** window appears.
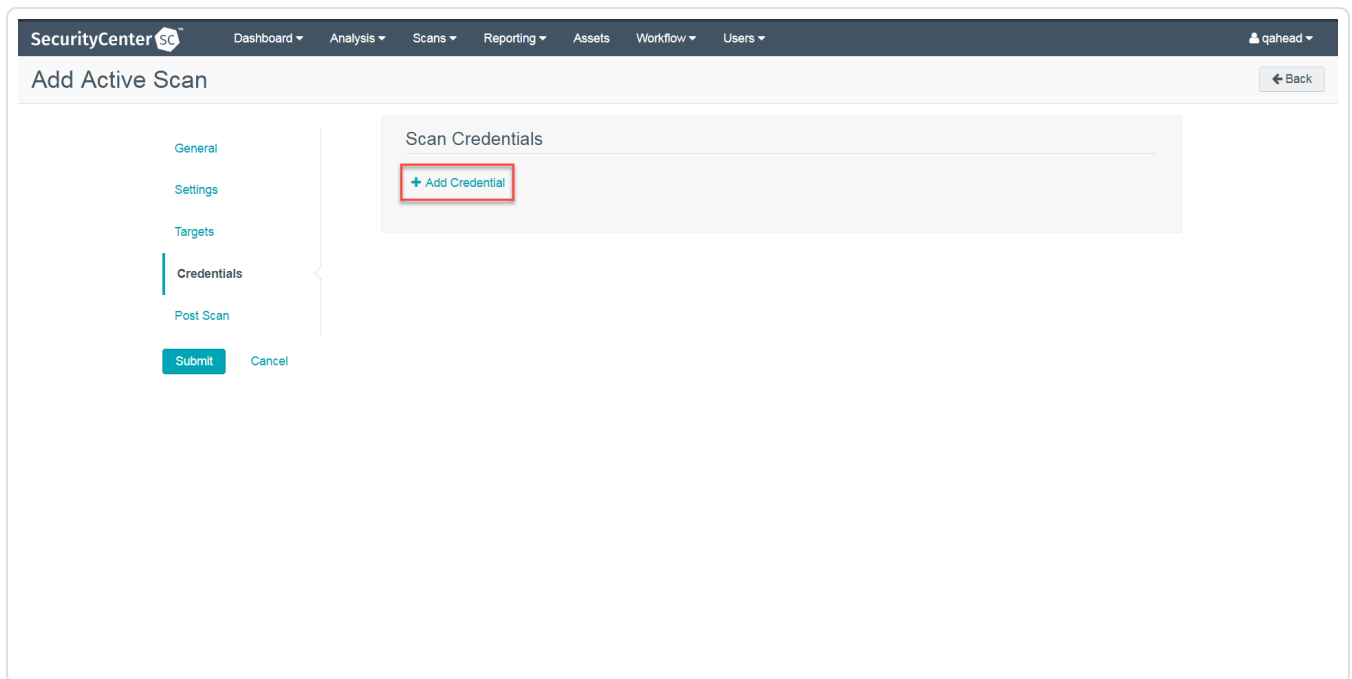
3. In the top right corner, click **+Add**.

The **Add Active Scan** window appears.

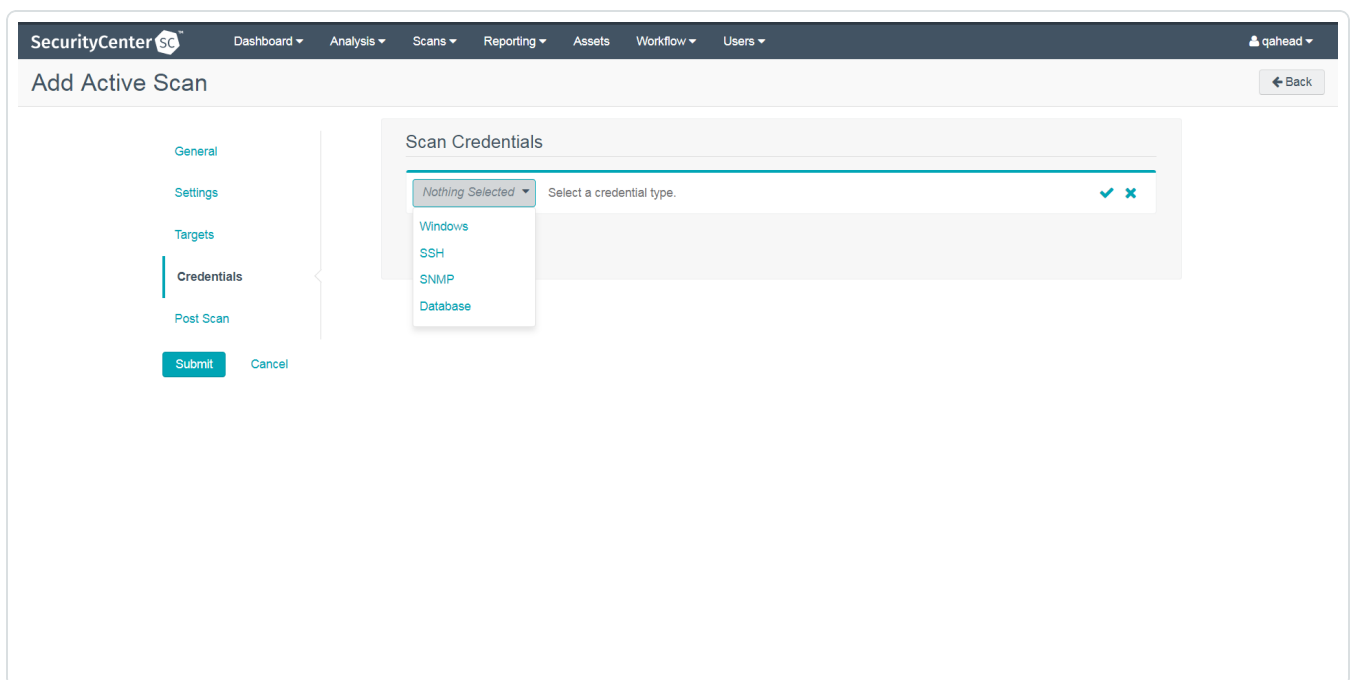4. In the left column, click **Credentials**.

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**.

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://lieb-soft.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.