Tenable Security Center and Lieberman RED Integration Guide

Last Revised: June 26, 2024
Table of Contents

Welcome to Tenable Security Center for Lieberman ......................................................... 3

Integrations ......................................................................................................................... 4
  Configure Database Integration ....................................................................................... 4
  Enable Database Plugins ............................................................................................... 6
  SSH Integration ............................................................................................................... 6
  Windows Integration ....................................................................................................... 8
  Add a Credential to a Scan ............................................................................................ 9

Additional Information ...................................................................................................... 14
  Lieberman System ......................................................................................................... 14
  About Tenable .............................................................................................................. 14
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

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 (administrator users) or Scans > Credentials (organizational users).

   The Credentials page appears.

3. Click Add.

   The Credential Templates page appears.

4. In the Miscellaneous, API Gateway, Database, SNMP, SSH, or Windows, or Web Authentication sections, click the tile for the specific method you want to configure.

   The Add Credentials configuration page appears.

5. In the Name box, type a name for the credentials.

6. In the Description box, type a description for the credentials.

7. (Optional) Type or select a Tag. For more information, see Tags in the Tenable Security Center User Guide.

8. Configure each option for the Database authentication.
The following table describes the additional options to configure when using Lieberman as the Authentication Method for Apache Cassandra, IBM DB2, SQL Server, MySQL, Oracle Database, PostgreSQL, or Sybase ASE database credentials.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delinea Secret Name</td>
<td>The value of the secret on the Delinea server. The secret is labeled Secret Name on the Delinea server.</td>
<td>yes</td>
</tr>
<tr>
<td>Delinea Host</td>
<td>The Delinea Secret Server IP address or DNS address.</td>
<td>yes</td>
</tr>
<tr>
<td>Delinea Port</td>
<td>The port on which Delinea Secret Server listens.</td>
<td>yes</td>
</tr>
<tr>
<td>Delinea Authentication Method</td>
<td>Indicates whether to use credentials or an API key for authentication. By default, credentials are selected.</td>
<td>yes</td>
</tr>
<tr>
<td>Delinea Login Name</td>
<td>The username to authenticate to the Delinea server.</td>
<td>yes</td>
</tr>
<tr>
<td>Delinea Password</td>
<td>The password to authenticate to the Delinea server. This is associated with the Delinea Login Name you provided.</td>
<td>yes</td>
</tr>
<tr>
<td>Delinea API key</td>
<td>The API key provided by Delinea Secret Server.</td>
<td>yes</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Enable if the Delinea Secret Server is configured to support SSL.</td>
<td>no</td>
</tr>
<tr>
<td>Verify SSL certificate</td>
<td>If enabled, verifies the SSL Certificate on the Delinea server.</td>
<td>no</td>
</tr>
</tbody>
</table>

9. Click **Submit**.

Tenable Security Center saves your configuration.

What to do next:
• Next, follow the steps to Add a Credential to a Scan.

Enable Database Plugins

To enable database plugins:


See the chart for database plugin types and corresponding IDs.

<table>
<thead>
<tr>
<th>Plugin Type</th>
<th>Plugin ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSSQL</td>
<td>91827</td>
</tr>
<tr>
<td>Oracle</td>
<td>91825</td>
</tr>
<tr>
<td>MySQL</td>
<td>91823</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>91826</td>
</tr>
</tbody>
</table>

2. Click Save.

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 configure a SSH credentialed network scan with Lieberman:

1. Log in to Tenable Security Center.

2. Click Scanning > Credentials (administrator users) or Scans > Credentials (organizational users).

   The Credentials page appears.

3. Click Add.

   The Credential Templates page appears.
4. In the **Miscellaneous, API Gateway, Database, SNMP, SSH, or Windows, or Web Authentication** sections, click the tile for the specific method you want to configure.

   The **Add Credentials** configuration page appears.

5. In the **Name** box, type a name for the credentials.

6. In the **Description** box, type a description for the credentials.

7. (Optional) Type or select a **Tag**. For more information, see [Tags](#) in the *Tenable Security Center User Guide*.

8. Configure each option for the **SSH** authentication.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Username</strong></td>
<td>The username for a user on the database.</td>
</tr>
<tr>
<td><strong>Lieberman Host</strong></td>
<td>The Lieberman IP address or DNS address.</td>
</tr>
<tr>
<td><strong>Note:</strong> If your Lieberman installation is in a subdirectory, you must include the subdirectory path. For example, type <em>IP address or hostname/subdirectory path</em>.</td>
<td></td>
</tr>
<tr>
<td><strong>Lieberman Port</strong></td>
<td>The port Lieberman is listening on.</td>
</tr>
<tr>
<td><strong>Lieberman User</strong></td>
<td>The username for the Lieberman explicit user you want Security Center for Lieberman to use for authentication to the Lieberman Rapid Enterprise Defense (RED) API.</td>
</tr>
<tr>
<td><strong>Lieberman Password</strong></td>
<td>The password for the Lieberman explicit user.</td>
</tr>
<tr>
<td><strong>Use SSL</strong></td>
<td>When enabled, Security Center for Lieberman uses SSL through IIS for secure communications. You must configure SSL through IIS in Lieberman before enabling this option.</td>
</tr>
<tr>
<td><strong>Verify SSL Certificate</strong></td>
<td>When enabled, Security Center for Lieberman validates the SSL certificate. You must configure SSL through IIS in Lieberman before enabling this option.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>System Name</td>
<td>The name for the database credentials in Lieberman.</td>
</tr>
</tbody>
</table>

9. Click **Submit**.

Tenable Security Center saves your configuration.

**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. Click **Scanning > Credentials** (administrator users) or **Scans > Credentials** (organizational users).

   The **Credentials** page appears.

3. Click **Add**.

   The **Credential Templates** page appears.

4. In the **Miscellaneous, API Gateway, Database, SNMP, SSH, or Windows, or Web Authentication** sections, click the tile for the specific method you want to configure.

   The **Add Credentials** configuration page appears.

5. In the **Name** box, type a name for the credentials.

6. In the **Description** box, type a description for the credentials.

7. (Optional) Type or select a **Tag**. For more information, see **Tags** in the **Tenable Security Center User Guide**.

8. Configure each option for the **Windows** authentication.
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The username for a user on the database.</td>
</tr>
<tr>
<td>Domain</td>
<td>The domain of the username, if required by Lieberman.</td>
</tr>
<tr>
<td>Lieberman Host</td>
<td>The Lieberman IP address or DNS address.</td>
</tr>
<tr>
<td>Note</td>
<td>If your Lieberman installation is in a subdirectory, you must include the subdirectory path. For example, type IP address or hostname/subdirectory path.</td>
</tr>
<tr>
<td>Lieberman Port</td>
<td>The port Lieberman is listening on.</td>
</tr>
<tr>
<td>Lieberman User</td>
<td>The username for the Lieberman explicit user you want Tenable Security Center to use for authentication to the Lieberman Rapid Enterprise Defense (RED) API.</td>
</tr>
<tr>
<td>Lieberman Password</td>
<td>The password for the Lieberman explicit user.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>When enabled, Tenable Security Center uses SSL through IIS for secure communications. Configure SSL through IIS in Lieberman before enabling this option.</td>
</tr>
<tr>
<td>Verify SSL Certificate</td>
<td>When enabled, Tenable Security Center validates the SSL certificate. Configure SSL through IIS in Lieberman before enabling this option.</td>
</tr>
<tr>
<td>System Name</td>
<td>The name for the database credentials in Lieberman.</td>
</tr>
</tbody>
</table>

9. Click **Submit**.  
Tenable Security Center saves your configuration.

10. Next, follow the steps for **adding the credential to a scan**.

**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**.

   ![Tenable Security Center screenshot](image)

   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://www.beyondtrust.com/docs/index.htm.

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.