Tenable Nessus and Lieberman RED Integration Guide

Last Revised: April 09, 2025

Table of Contents

Welcome to Tenable 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 applications with Lieberman.

Note: Lieberman is only compatible with Nessus Manager. It is not compatible with Nessus Professional.

Integrating Tenable applications with Lieberman provides security administrators with the assistance they need to access and navigate the ever-changing sea of usernames, passwords, and privileges. By integrating your Tenable applications with Lieberman, you have more choice and flexibility.

You can integrate Lieberman with Tenable Vulnerability Management, Tenable Nessus, or Tenable Security Center.

The benefits of integrating Tenable applications with Lieberman include:

- Credential updates directly in your Tenable Application, 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.

Nessus Supported Credentials

You can configure the Lieberman system with Windows or SSH. Full database support is also provided. Click the corresponding link to view the configuration steps.

Configure Tenable Nessus for Lieberman Windows

Configure Tenable Nessus for Lieberman SSH

Configure Tenable Nessus for Lieberman Database

Configure Tenable Nessus for Lieberman Database

Tenable Nessus provides full database support for Lieberman. Enable Database Plugins in Nessus in the scanner to display them in the output.

To configure Nessus for Lieberman database:

1. Log in to your Tenable user interface.
2. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.
3. In the left navigation plane, click **Scans**.

   The **Scans** page appears.
4. In the upper-right corner of the page, click the **Create a Scan** button.

   The **Select a Scan Template** page appears.
5. Select a scan template.

   The scan configuration page appears.
6. In the **Name** box, type a name for the scan.
7. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
8. (Optional) Add a description, folder location, scanner location, and specify target groups.
9. Click the **Credentials** tab.

   The **Settings** pane appears.

10. Click the **Database** option.

    The **Database** options appear.

11. In the **Database Type** drop-down box, select **Oracle**.

12. In the **Auth Type** drop-down box, click **Tenable Nessus for Lieberman RED**.

    The Tenable Nessus for Lieberman RED options appear.

13. Configure each option for the **Database** authentication.

Option	Database Type	Description	Required
Username	All	The target system's username.	yes
Lieberman host	All	The Lieberman IP/DNS address. **Note:** If your Lieberman installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname / subdirectory path*.	yes
Lieberman port	All	The port on which Lieberman listens.	yes
Lieberman API URL	All	The URL Tenable Nessus for Lieberman REDTenable Security Center uses to access Lieberman.	no
Lieberman user	All	The Lieberman explicit user for authenticating to the Lieberman API.	yes
Lieberman password	All	The password for the Lieberman explicit user.	yes
Lieberman	All	The alias used for the	no

Option	Database Type	Description	Required
Authenticator		authenticator in Lieberman. The name should match the name used in Lieberman. **Note:** If you use this option, append a domain to the **Lieberman user** option, i.e., *domain\user*.	
Lieberman Client Certificate	All	The file that contains the PEM certificate used to communicate with the Lieberman host. **Note:** If you use this option, you do not have to enter information in the **Lieberman user**, **Lieberman password**, and **Lieberman Authenticator** fields.	no
Lieberman Client Certificate Private Key	All	The file that contains the PEM private key for the client certificate.	no
Lieberman Client Certificate Private Key Passphrase	All	The passphrase for the private key, if required.	no
Use SSL	All	If Lieberman is configured to support SSL through IIS, check for secure communication.	no
Verify SSL Certificate	All	If Lieberman is configured to support SSL through IIS and you want to validate the certificate,	no

Option	Database Type	Description	Required
		check this option. Refer to Custom CA documentation for how to use self-signed certificates.	
System Name	All	In the rare case your organization uses one default Lieberman entry for all managed systems, enter the default entry name.	no
Database Port	All	The port on which Tenable Nessus for Lieberman REDTenable Security Center communicates with the database.	yes
Database Name	DB2 PostgreSQL	(PostgreSQL and DB2 databases only) The name of the database.	no
Auth type	Oracle SQL Server Sybase ASE	(SQL Server, Oracle. and Sybase ASE databases only) SQL Server values include: • Windows • SQL Oracle values include: • SYSDBA • SYSOPER • NORMAL	yes

Option	Database Type	Description	Required
		Sybase ASE values include: • RSA • Plain Text	
Instance Name	SQL Server	The name for your database instance.	no
Service type	Oracle	Valid values include: • SID • SERVICE_NAME	no
Service	Oracle	The SID value for your database instance or a SERVICE_NAME value. The **Service** value you enter must match your parameter selection for the **Service Type** option.	yes

14. Do one of the following:

    - If you want to save without launching the scan, click **Save**.
    - If you want to save and launch the scan immediately, click **Save & Launch**.

    > **Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

Enable Database Plugins in Nessus

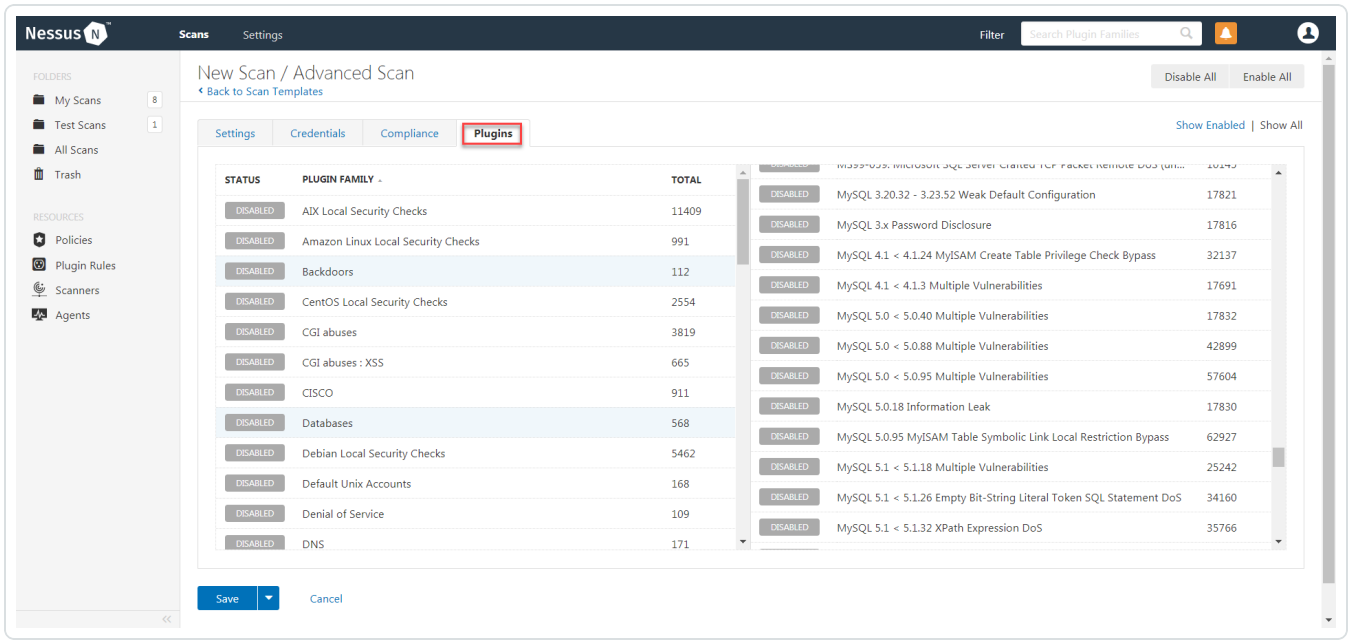
You can enable database plugins in your Tenable Application for your configured Lieberman Database account.

To enable database plugins:

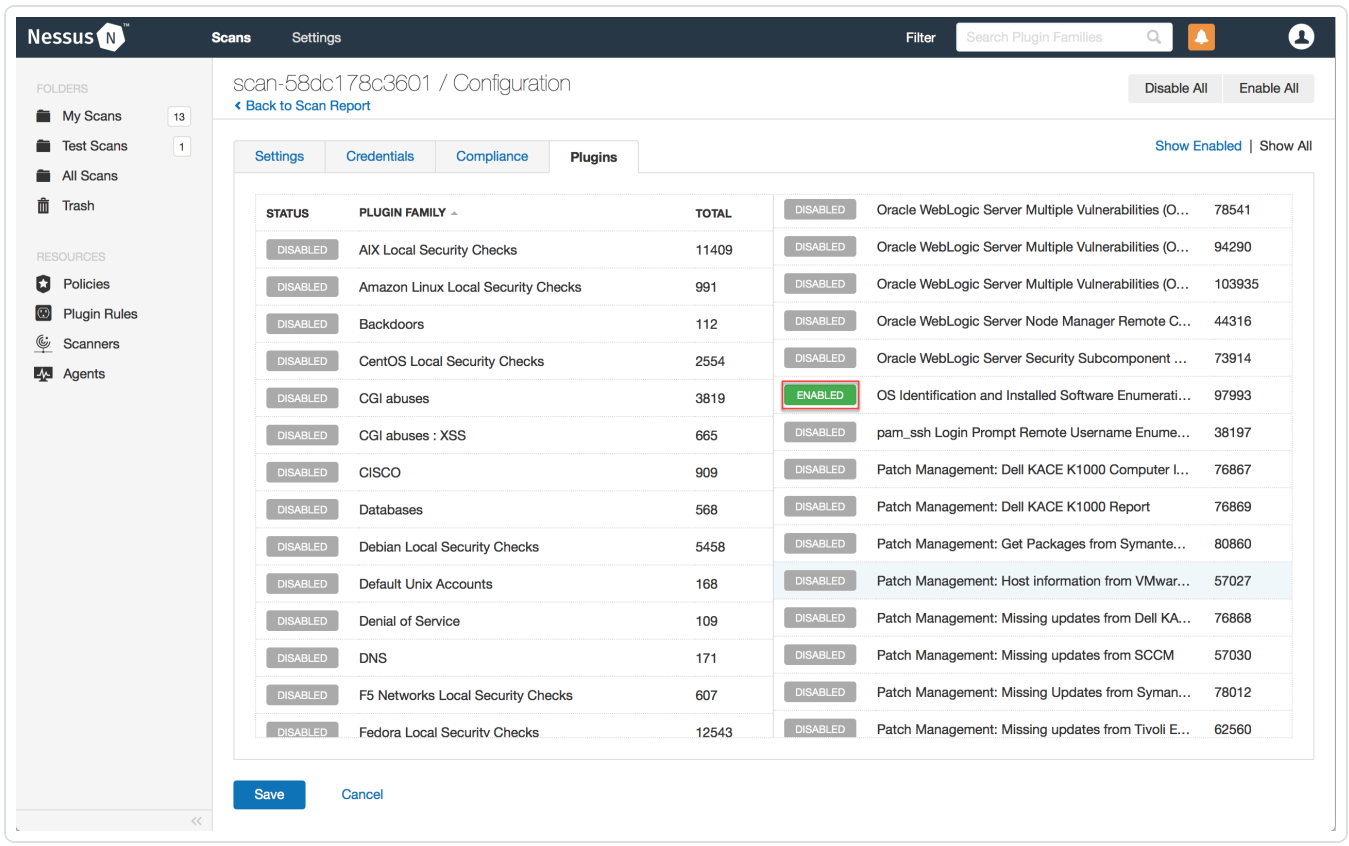
1. In the scan where you configured the Lieberman credentials, click the **Plugins** tab.

   The **Plugins** section appears.

   .



2. Click the **Status** button.



3. Click **Save**.

   See the chart for database plugin types and corresponding IDs.

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

Configure Tenable Nessus for Lieberman SSH

Tenable Nessus provides an option for Lieberman SSH integration. Complete the following steps to configure Nessus with Lieberman SSH.

To configure Nessus for Lieberman SSH:

1. Log in to your Tenable user interface.
2. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.
3. In the left navigation plane, click **Scans**.

   The **Scans** page appears.
4. In the upper-right corner of the page, click the **Create a Scan** button.

   The **Select a Scan Template** page appears.
5. Select a scan template.

   The scan configuration page appears.
6. In the **Name** box, type a name for the scan.
7. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
8. (Optional) Add a description, folder location, scanner location, and specify target groups.
9. Click the **Credentials** tab.

   The **Credentials** pane appears.
10. In the **Select a Credential** menu, select the **Host** drop-down.
11. Select **SSH**.

    The **Settings** pane appears.
12. In the **Auth Type** drop-down box, click **Tenable Nessus for Lieberman RED**.

    The Tenable Nessus for Lieberman RED options appear.
13. Configure each option for the **SSH** authentication.

Option	Description	Required
Username	The target system's username.	yes
Lieberman host	The Lieberman IP/DNS address.	yes

Option	Description	Required
	Note: If your Lieberman installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname / subdirectory path*.	
Lieberman port	The port on which Lieberman listens.	yes
Lieberman API URL	The URL Tenable Vulnerability ManagementTenable Nessus uses to access Lieberman.	no
Lieberman user	The Lieberman explicit user for authenticating to the Lieberman RED API.	yes
Lieberman password	The password for the Lieberman explicit user.	yes
Lieberman Authenticator	The alias used for the authenticator in Lieberman. The name should match the name used in Lieberman. **Note:** If you use this option, append a domain to the **Lieberman user** option, i.e., *domain\user*.	no
Lieberman Client Certificate	The file that contains the PEM certificate used to communicate with the Lieberman host. **Note:** If you use this option, you do not have to enter information in the **Lieberman user**, **Lieberman password**, and **Lieberman Authenticator** fields.	no
Lieberman Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	no
Lieberman Client Certificate	The passphrase for the private key, if required.	no

Option	Description	Required
Private Key Passphrase		
Use SSL	If Lieberman is configured to support SSL through IIS, check for secure communication.	no
Verify SSL Certificate	If Lieberman is configured to support SSL through IIS and you want to validate the certificate, check this option. Refer to Custom CA documentation for how to use self-signed certificates.	no
System Name	In the rare case your organization uses one default Lieberman entry for all managed systems, enter the default entry name.	no
Custom password prompt	The password prompt used by the target host. Only use this setting when an interactive SSH session fails due to Tenable Vulnerability ManagementTenable Nessus receiving an unrecognized password prompt on the target host's interactive SSH shell.	no
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To**	no

Option	Description	Required
	Prioritize Credentials, you configure the scan to use the successful credential first, which allows the scan to access the target faster.	

14. Do one of the following:

    - If you want to save without launching the scan, click **Save**.
    - If you want to save and launch the scan immediately, click **Save & Launch**.

    > **Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

What to do next:

1. To verify the integration is working, click the **Launch** button to initiate an on-demand scan.
2. Once the scan has completed, select the completed scan and look for **Plugin ID 97993** and the corresponding message - *It was possible to log into the remote host via SSH using 'password' authentication*. This validates that authentication was successful.

Configure Tenable Nessus for Lieberman Windows

To integrate with Windows:

1. Log in to your Tenable user interface.
2. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.
3. In the left navigation plane, click **Scans**.

   The **Scans** page appears.
4. In the upper-right corner of the page, click the **Create a Scan** button.

   The **Select a Scan Template** page appears.
5. Select a scan template.

The scan configuration page appears.

6. In the **Name** box, type a name for the scan.
7. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
8. (Optional) Add a description, folder location, scanner location, and specify target groups.
9. Click the **Credentials** tab.

   The **Credentials** pane appears.
10. In the **Select a Credential** menu, select the **Host** drop-down.
11. Select **Windows**.

    The **Settings** pane appears.
12. In the **Auth Type** drop-down box, click **Tenable Nessus for Lieberman RED**.

    The Tenable Nessus for Lieberman RED options appear.
13. Configure each option for the **Windows** authentication.

Option	Description	Required
Username	The target system's username.	yes
Domain	The domain, if the username is part of a domain.	no
Lieberman host	The Lieberman IP/DNS address. **Note:** If your Lieberman installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname / subdirectory path*.	yes
Lieberman port	The port on which Lieberman listens.	yes
Lieberman API URL	The URL Tenable Vulnerability ManagementTenable Nessus uses to access Lieberman.	no
Lieberman user	The Lieberman explicit user for authenticating to	yes

Option	Description	Required
	the Lieberman RED API.	
Lieberman password	The password for the Lieberman explicit user.	yes
Lieberman Authenticator	The alias used for the authenticator in Lieberman. The name should match the name used in Lieberman. **Note:** If you use this option, append a domain to the **Lieberman user** option, i.e., *domain\user*.	no
Lieberman Client Certificate	The file that contains the PEM certificate used to communicate with the Lieberman host. **Note:** If you use this option, you do not have to enter information in the **Lieberman user**, **Lieberman password**, and **Lieberman Authenticator** fields.	no
Lieberman Client Certificate Private Key	The file that contains the PEM private key for the client certificate.	no
Lieberman Client Certificate Private Key Passphrase	The passphrase for the private key, if required.	no
Use SSL	If Lieberman is configured to support SSL through IIS, check for secure communication.	no
Verify SSL Certificate	If Lieberman is configured to support SSL through IIS and you want to validate the certificate, check this. Refer to custom_CA.inc documentation for how to use self-signed certificates.	no

Option	Description	Required
System Name	In the rare case your organization uses one default Lieberman entry for all managed systems, enter the default entry name.	no

14. Do one of the following:
    - If you want to save without launching the scan, click **Save**.
    - If you want to save and launch the scan immediately, click **Save & Launch**.

    > **Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

Allow Shared Accounts

You can use the shared accounts option to manage multiple targets using the same credentials.

Before you begin:

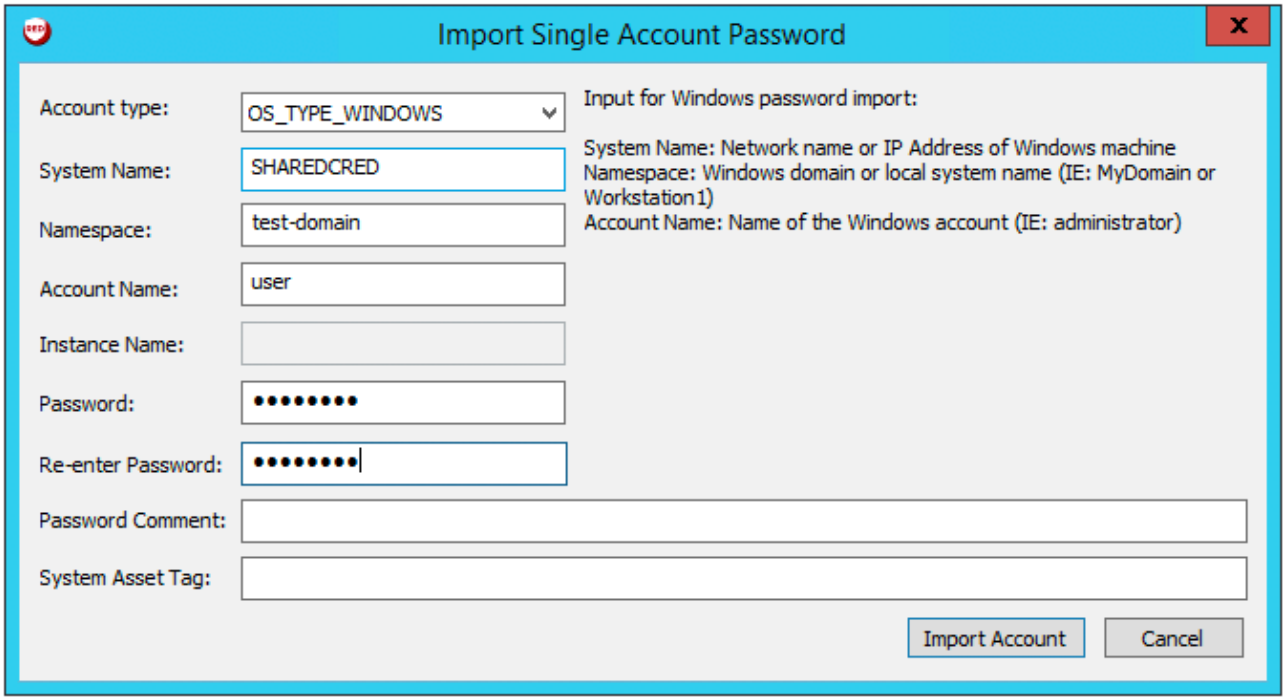
You must have the following permissions selected in Lieberman:

- log in
- ignore password checkout
- recover password
- the management sets you want the account to have access to

To allow shared accounts in Lieberman:

1. Choose an account or import one into the Lieberman password store.
2. In the Lieberman UI, specify the credential and enter a name in the **System Name** field.

   For this example, we created: user - *test-domain/user* and machine - *sharedcred*.



Note: If you enter a specific machine in the **System Name**, you can pull back a synced password.

Note: The machine in the **System Name** field uses the same username and password combo for all targets.

3. Click **Import Account**.

Additional Information

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.