Tenable.io and Lieberman RED Integration Guide

Last Revised: May 22, 2021

Table of Contents

Welcome to Tenable.io for Lieberman

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

The benefits of integrating Tenable.io with Lieberman include:

- Credentials update directly in Tenable.io, 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

Configure Windows Integration

To integrate with Windows:

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

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

   The **Settings** page appears.
4. Click the **Credentials** widget.

   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.
5. Click the ⊕ button next to the **Credentials** title.

   The credential form plane appears.
6. In the **Host** section, click **Windows**.

   The selected credential options appear.
7. In the **Authentication Method** drop-down, select **Lieberman**.

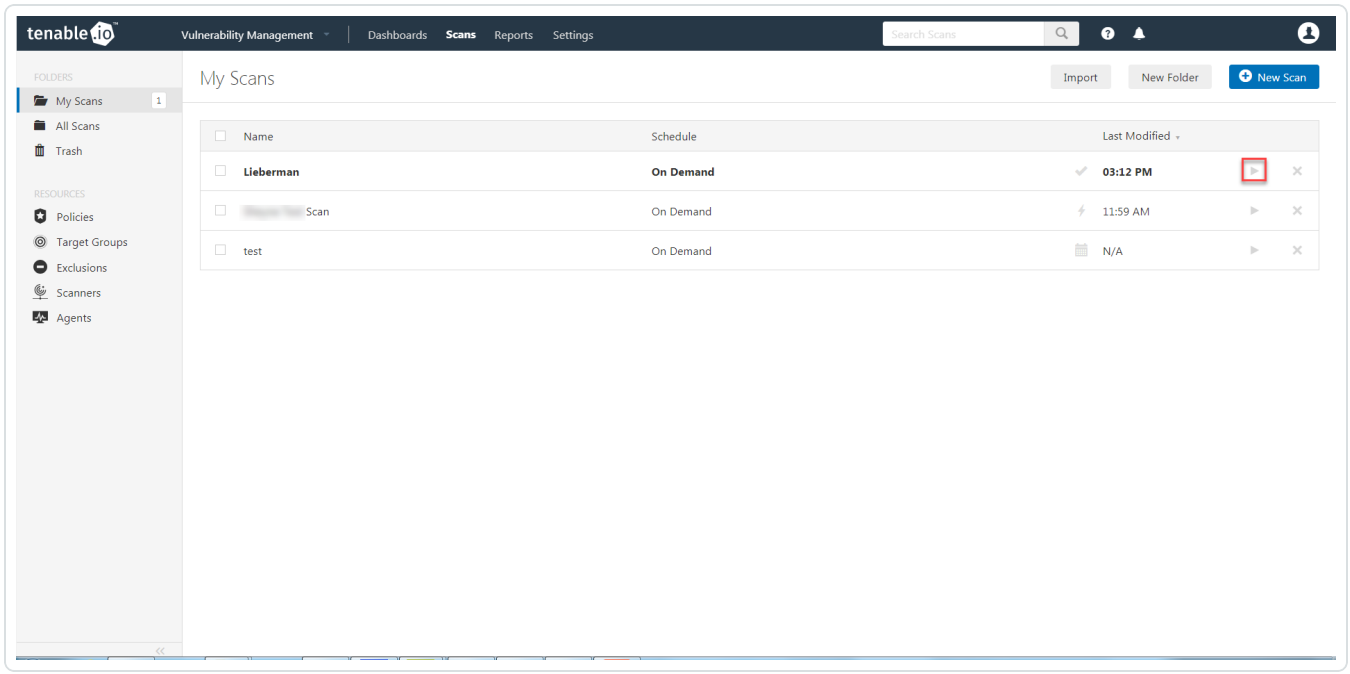
   The **Lieberman** options appear.
8. Configure the **Lieberman** credentials.

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	yes

Option	Description	Required
	subdirectory, you must include the sub-directory 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.io 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 Private Key Passphrase	The passphrase for the private key, if required.	no

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

9. Click **Save**.
10. To verify the integration works, click the **Launch** button to initiate an on-demand scan.



11. Once the scan has completed, select the completed scan and look for the corresponding message - *Microsoft Windows SMB Log In Possible: 10394*. This validates that authentication was successful.

Shared Accounts

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

Before you begin:

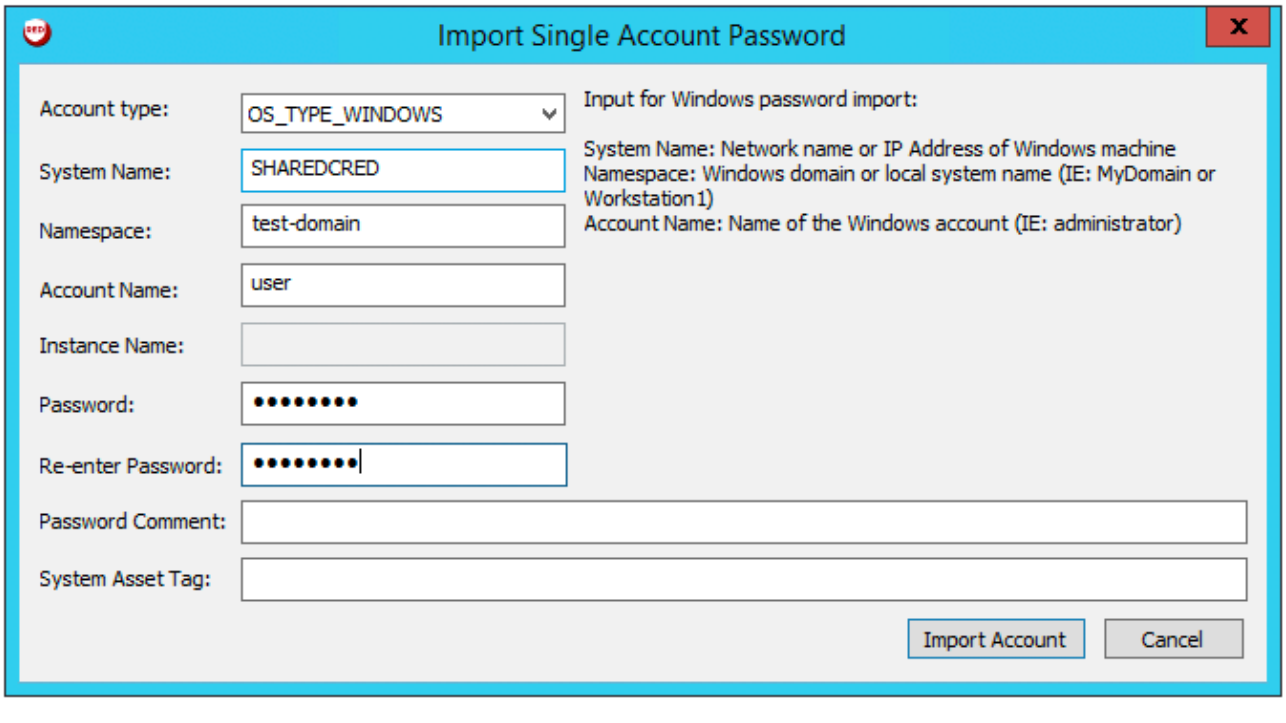
You must have the following permissions selected in Lieberman:

- 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**.

Configure SSH Integration

To integrate with SSH:

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

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

   The **Settings** page appears.
4. Click the **Credentials** widget.

   The **Credentials** page appears. The credentials table lists the managed credentials you have permission to view.
5. Click the ⊕ button next to the **Credentials** title.

   The credential form plane appears.
6. In the **Host** section, click **Windows**.

   The selected credential options appear.
7. In the **Authentication Method** drop-down, select **Lieberman**.

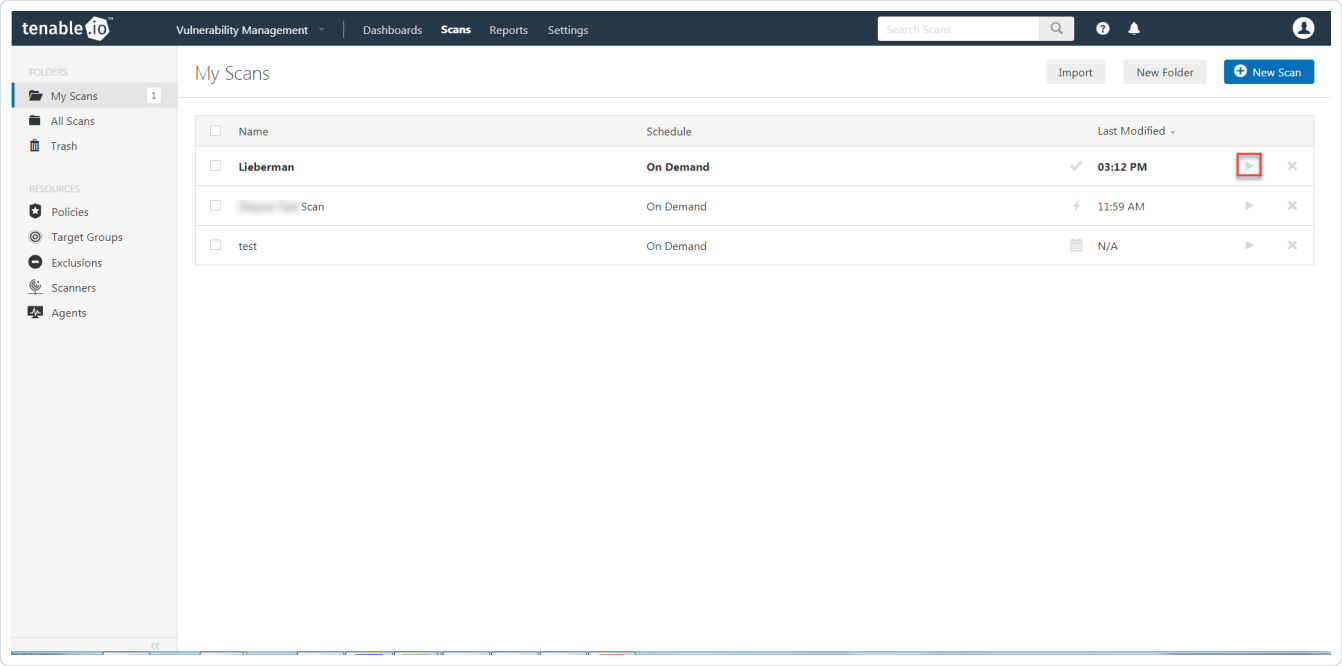
   The **Lieberman** options appear.
8. Configure the **Lieberman** credentials.

Option	Description	Required
Username	The target system's username.	yes
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

Option	Description	Required
Lieberman port	The port on which Lieberman listens.	yes
Lieberman API URL	The URL Tenable.io 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 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 Cer-	If Lieberman is configured to support SSL through IIS	no

Option	Description	Required
tificate	and you want to validate the certificate, check this option. Refer to Custom CA documentation for how to use self-signed certificates.	
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.io receiving an unrecognized password prompt on the target host's interactive SSH shell.	no

9. Click **Save**.
10. To verify the integration is working, click the **Launch** button to initiate an on-demand scan.



11. 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 Database Integration

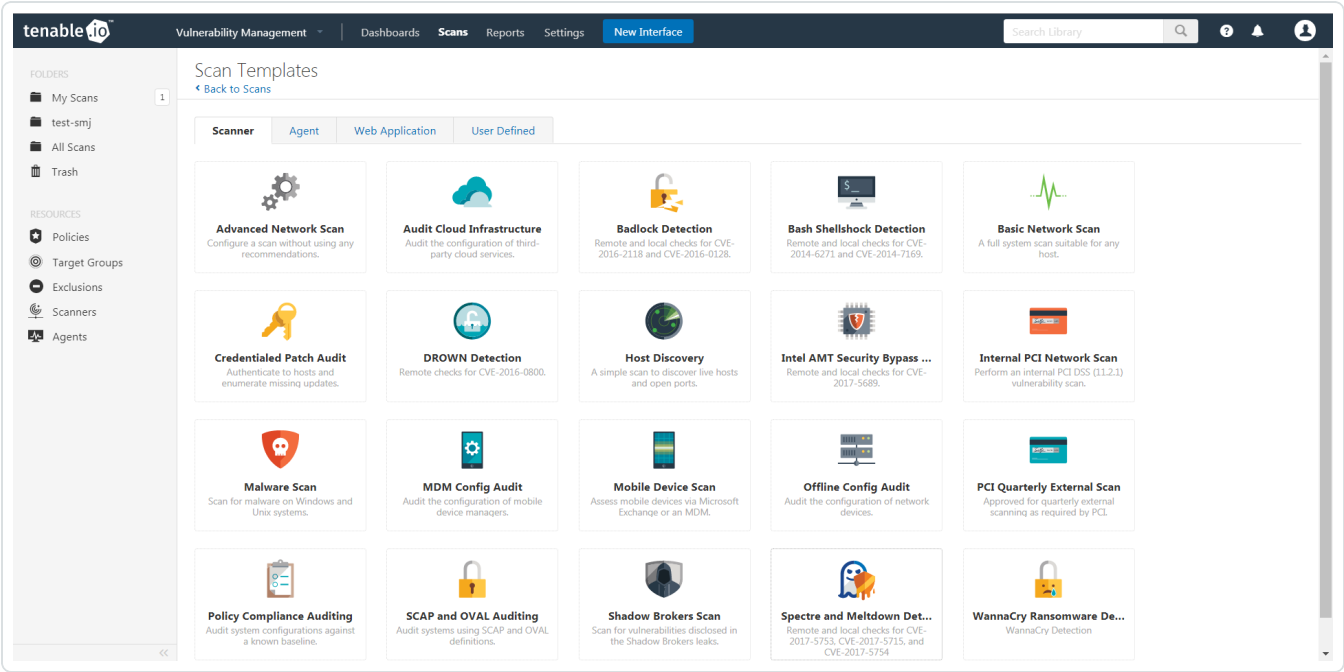
Tenable.io provides full database support for Lieberman. Enable the plugins in the scanner to display them in the output.

To configure Lieberman database integration:

1. Log in to Tenable.io.
2. Click **Scans**.

   The **My Scans** page appears.
3. Click **+ New Scan.**

   The **Scan Templates** page appears.



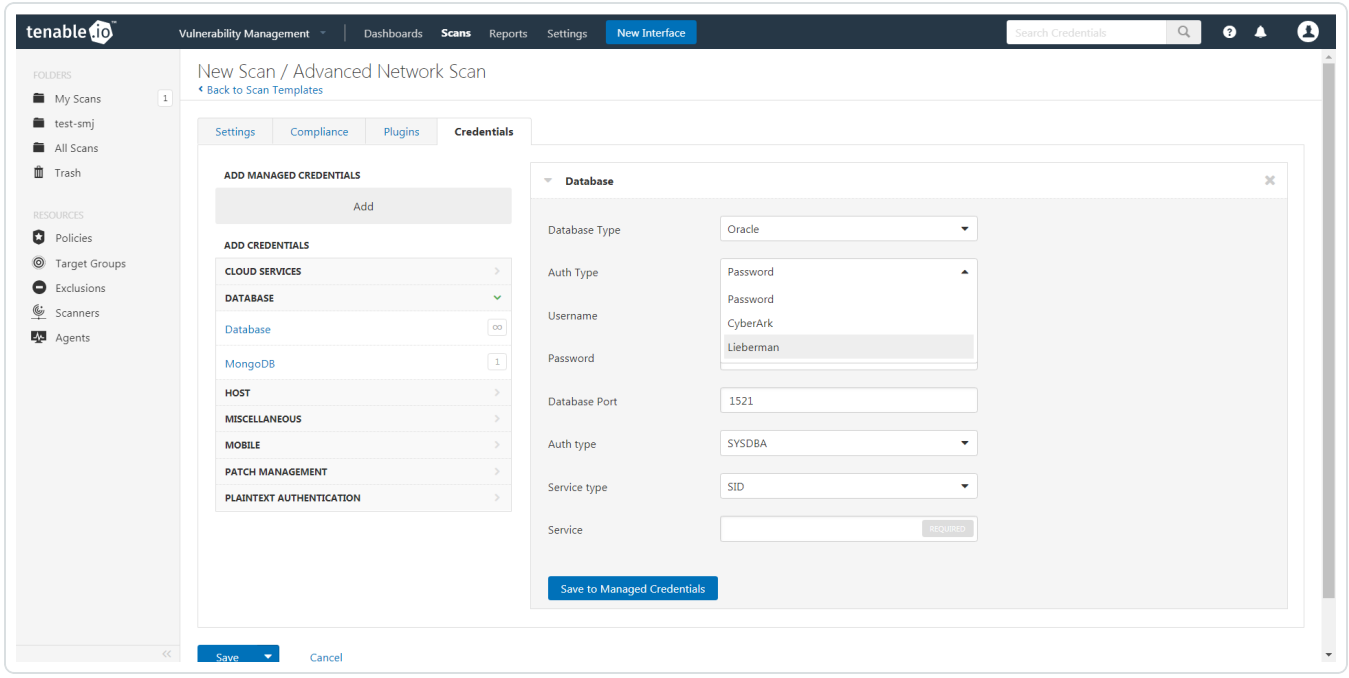
4. Click a **Scan Template**. For example, this procedure walks through the **Advanced Network Scan** template.

   The **Scan Configuration** page appears.
5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.

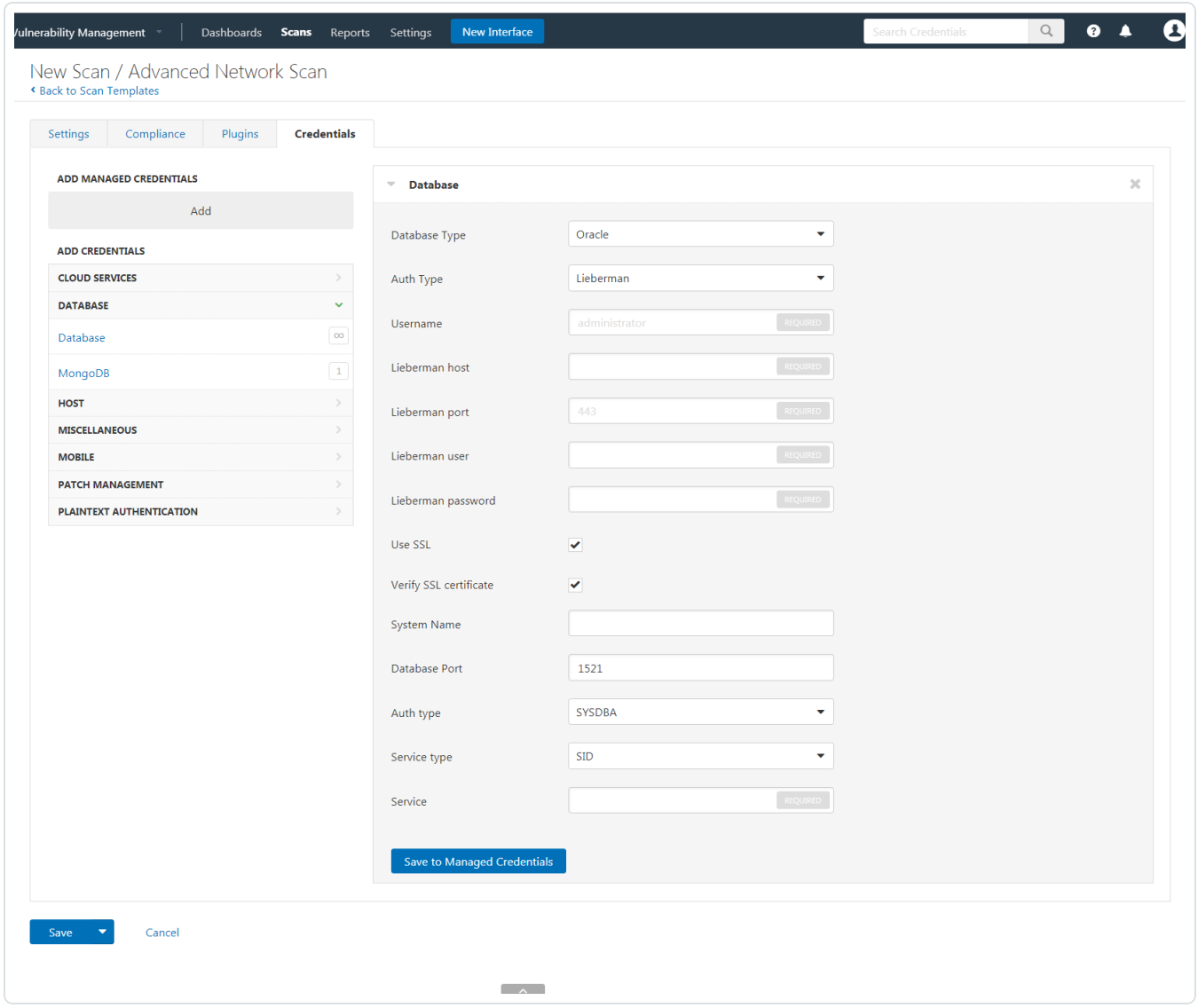
7. (Optional) You can add a description, folder location, scanner location, and specify target groups.
8. Click the **Credentials** tab.

   The **Credentials** options appear.
9. In the **Add Credentials** section, expand the **Database** section.
10. Click the **Database** option.

    The **Database** options appear.
11. Click the **Database Type** drop-down box.
12. Click **Oracle**
13. Click the **Auth Type** drop-down box.
14. Click **Lieberman**.



   The **Lieberman** options appear.
15. Configure each option for the **Database** authentication. See the Database section in the Tenable.io User Guide to get detailed descriptions for each option.



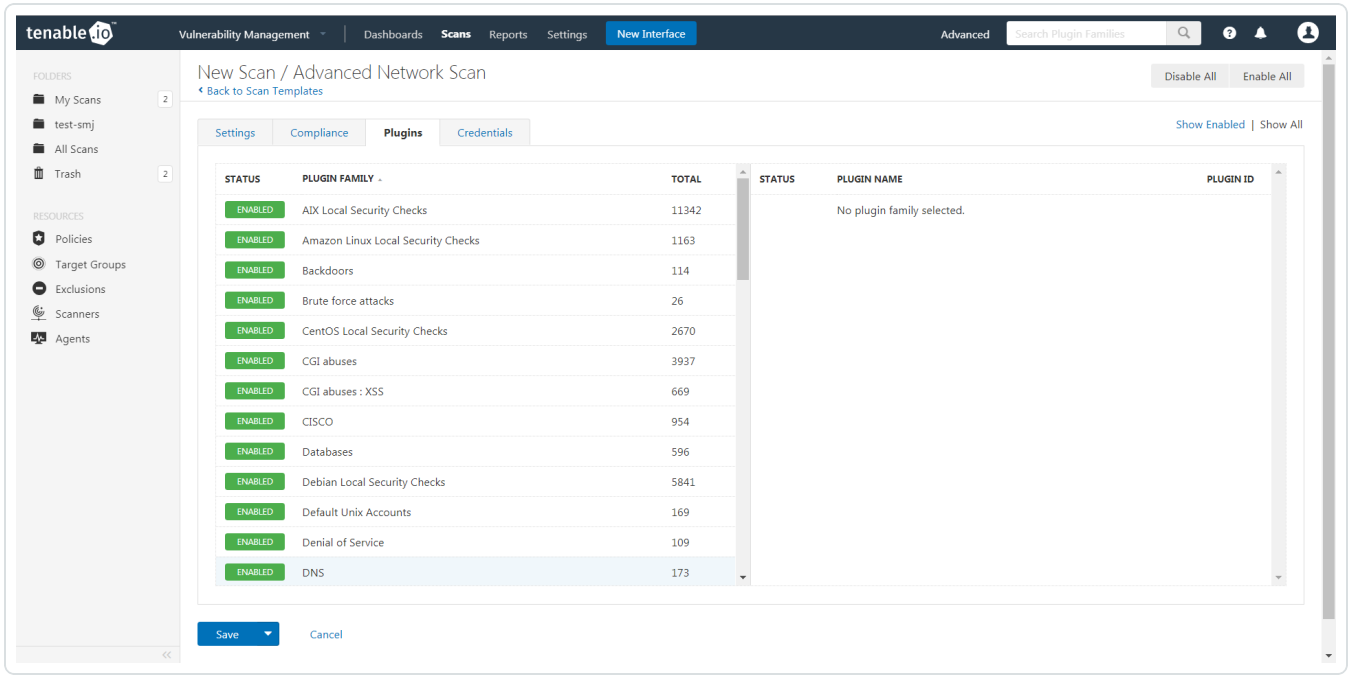
16. Click **Save**.

Enable Database Plugins

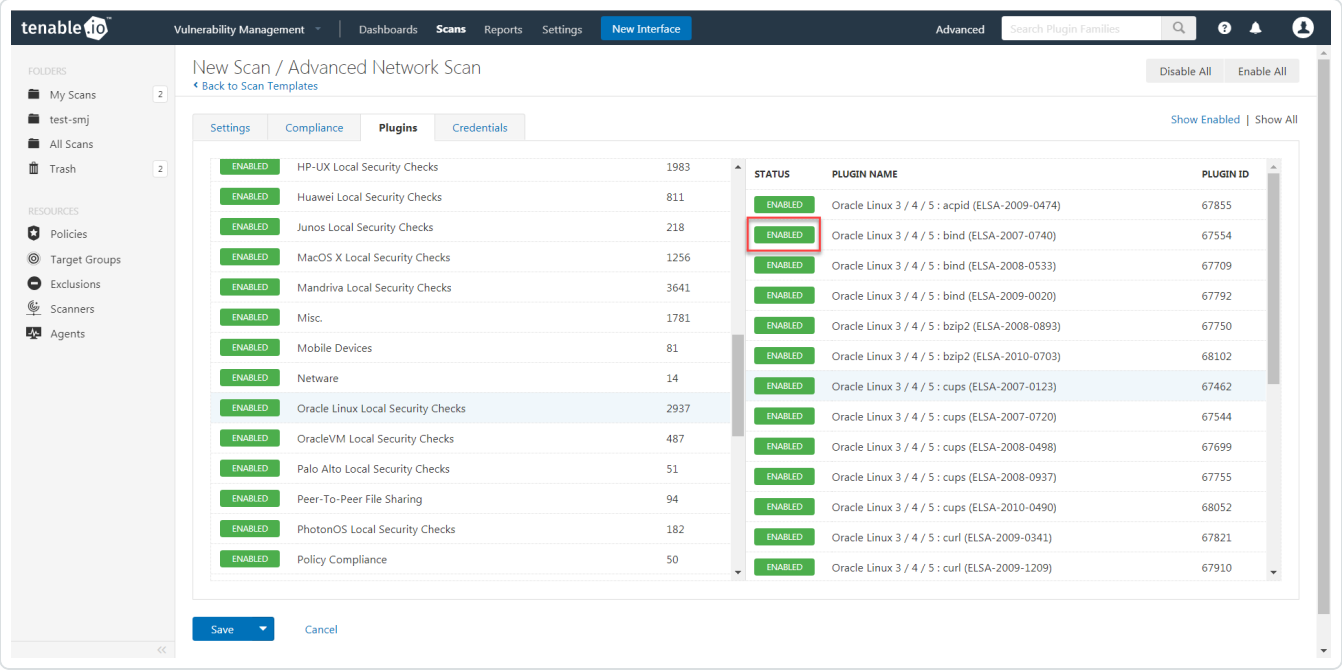
To enable database plugins:

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

   The **Plugins** section appears.



2. Click the **Status** button to nable the database plugin.



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

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.