



Tenable Vulnerability Management and Lieberman RED Integration Guide

Last Revised: October 06, 2023



Table of Contents

Welcome to Tenable Vulnerability Management for Lieberman	3
Integrations	4
Configure Windows Integration	5
Shared Accounts	8
Configure SSH Integration	10
Configure Database Integration	14
Enable Database Plugins	17
Additional Information	19
Lieberman System	20
About Tenable	21



Welcome to Tenable Vulnerability Management 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 Vulnerability Management 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 Vulnerability Management with Lieberman, customers have more choice and flexibility.

The benefits of integrating Tenable Vulnerability Management with Lieberman include:

- Credentials update directly in Tenable Vulnerability Management, 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 Vulnerability Management.
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. <div>Note: If your Lieberman installation is in a subdirectory, you must include the subdirectory path. For example, type <i>IP address or hostname /</i></div>	yes



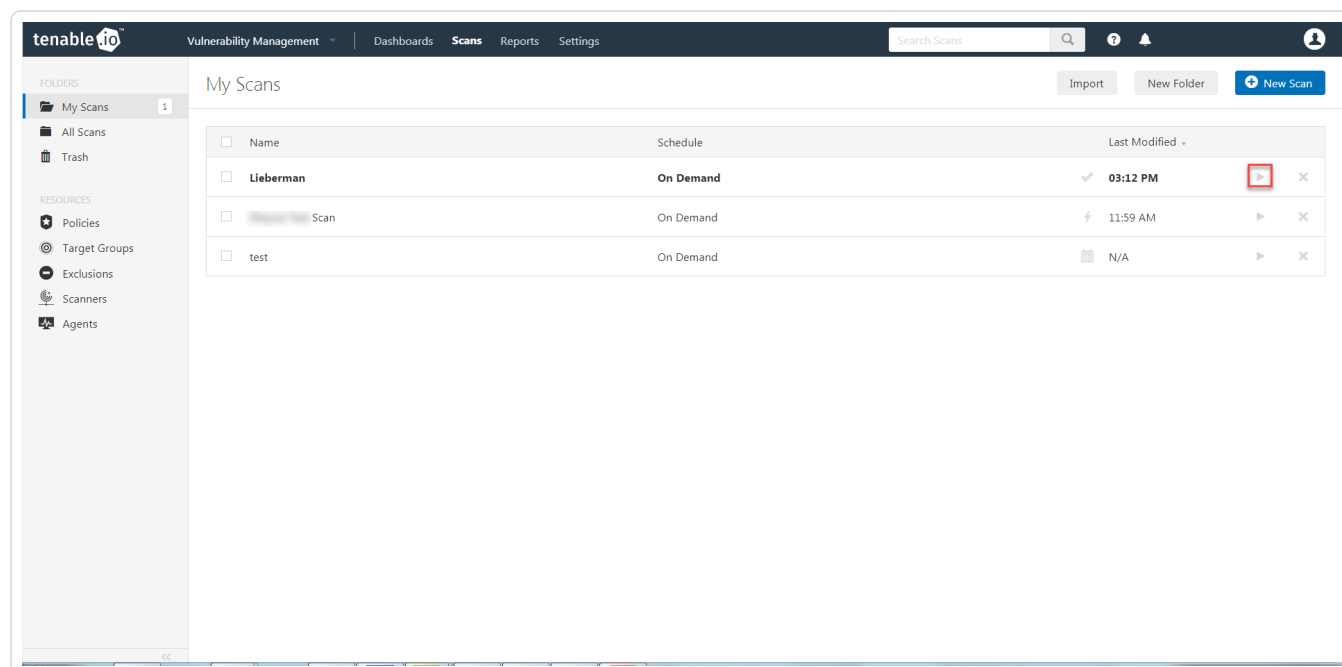
Option	Description	Required
	<div><i>subdirectory path.</i></div>	
Lieberman port	The port on which Lieberman listens.	yes
Lieberman API URL	The URL Tenable Vulnerability Management uses to access Lieberman.	no
Lieberman user	The Lieberman explicit user for authenticating to the Lieberman RED API.	yes
Lieberman password	The password for the Lieberman explicit user.	yes
Lieberman Authenticator	<p>The alias used for the authenticator in Lieberman. The name should match the name used in Lieberman.</p> <div>Note: If you use this option, append a domain to the Lieberman user option, i.e., <i>domain\user</i>.</div>	no
Lieberman Client Certificate	<p>The file that contains the PEM certificate used to communicate with the Lieberman host.</p> <div>Note: If you use this option, you do not have to enter information in the Lieberman user, Lieberman password, and Lieberman Authenticator fields.</div>	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*.

Import Single Account Password

Account type: OS_TYPE_WINDOWS

System Name: SHARED CRED

Namespace: test-domain

Account Name: user

Instance Name:

Password:

Re-enter Password:

Password Comment:

System Asset Tag:

Input for Windows password import:

System Name: Network name or IP Address of Windows machine

Namespace: Windows domain or local system name (IE: MyDomain or Workstation1)

Account Name: Name of the Windows account (IE: administrator)

Import Account Cancel



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 Vulnerability Management.
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	<div>The Lieberman IP/DNS address. Note: If your Lieberman installation is in a subdirectory, you must include the subdirectory path. For example, type <i>IP address or hostname / subdirectory path</i>.</div>	yes

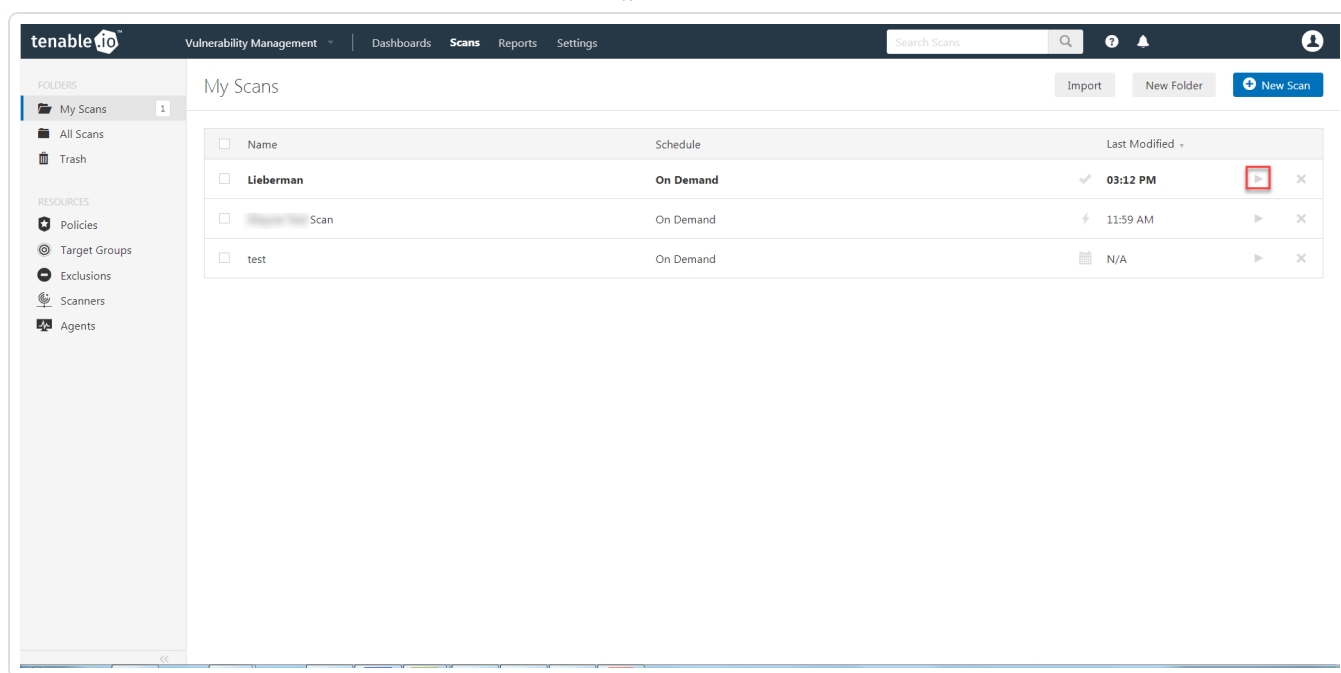


Option	Description	Required
Lieberman port	The port on which Lieberman listens.	yes
Lieberman API URL	The URL Tenable Vulnerability Management uses to access Lieberman.	no
Lieberman user	The Lieberman explicit user for authenticating to the Lieberman RED API.	yes
Lieberman password	The password for the Lieberman explicit user.	yes
Lieberman Authenticator	<p>The alias used for the authenticator in Lieberman. The name should match the name used in Lieberman.</p> <div>Note: If you use this option, append a domain to the Lieberman user option, i.e., <i>domain\user</i>.</div>	no
Lieberman Client Certificate	<p>The file that contains the PEM certificate used to communicate with the Lieberman host.</p> <div>Note: If you use this option, you do not have to enter information in the Lieberman user, Lieberman password, and Lieberman Authenticator fields.</div>	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



Option	Description	Required
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
Targets to Prioritize Credentials	(missing or bad snippet)	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 Management 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 Vulnerability Management provides full database support for Lieberman. Enable the plugins in the scanner to display them in the output.

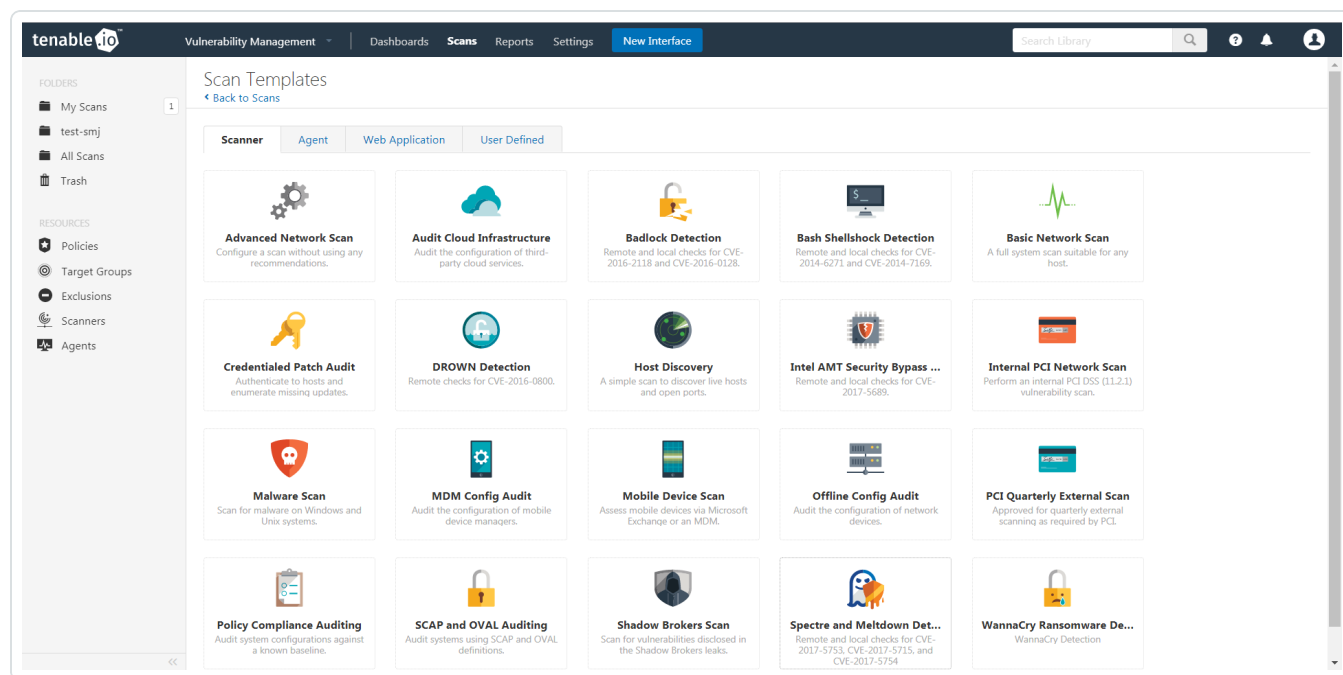
To configure Lieberman database integration:

1. Log in to Tenable Vulnerability Management.
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 screenshot shows the Tenable Vulnerability Management interface. The top navigation bar includes 'Vulnerability Management', 'Dashboards', 'Scans', 'Reports', 'Settings', and 'New Interface'. The left sidebar shows 'FOLDERS' (My Scans, test-smj, All Scans, Trash) and 'RESOURCES' (Policies, Target Groups, Exclusions, Scanners, Agents). The main content area is titled 'New Scan / Advanced Network Scan' and has tabs for 'Settings', 'Compliance', 'Plugins', and 'Credentials'. The 'Credentials' tab is active, showing the 'ADD CREDENTIALS' section. The 'DATABASE' category is expanded, and the 'Database' option is selected. The 'Database' configuration panel is open, showing fields for Database Type (Oracle), Auth Type (Password), Username (CyberArk), Password (Lieberman), Database Port (1521), Auth type (SYSDBA), Service type (SID), and Service (required). A 'Save to Managed Credentials' button is at the bottom.

The **Lieberman** options appear.

15. Configure each option for the **Database** authentication. See the [Database](#) section in the Tenable Vulnerability Management User Guide to get detailed descriptions for each option.

Vulnerability Management

Dashboards

Scans

Reports

Settings

New Interface

Search Credentials

New Scan / Advanced Network Scan

[Back to Scan Templates](#)

SettingsCompliancePluginsCredentials

ADD MANAGED CREDENTIALS

Add

ADD CREDENTIALS

CLOUD SERVICES

DATABASE

Database

MongoDB

HOST

MISCELLANEOUS

MOBILE

PATCH MANAGEMENT

PLAINTEXT AUTHENTICATION

Database

Database Type

Oracle

Auth Type

Lieberman

Username

administrator

Lieberman host

Lieberman port

443

Lieberman user

Lieberman password

Use SSL

Verify SSL certificate

System Name

Database Port

1521

Auth type

SYSDBA

Service type

SID

Service

Save to Managed Credentials

Save

Cancel

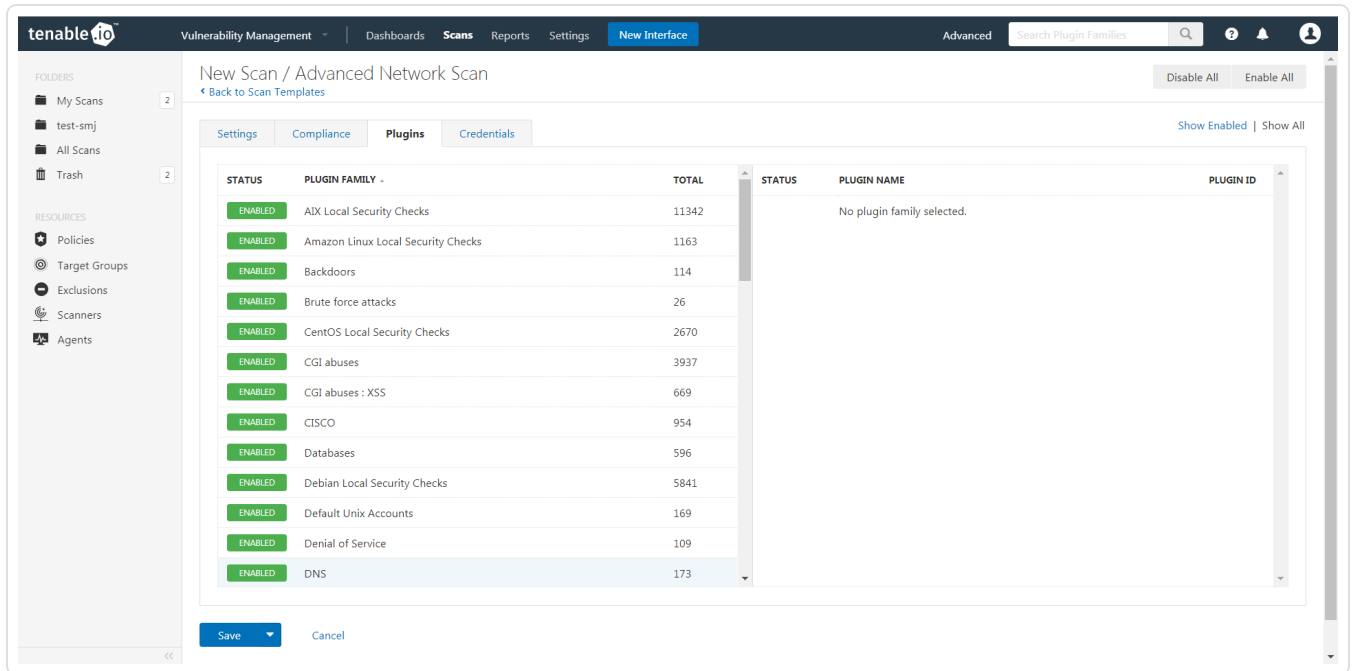
16. Click **Save**.

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.



The screenshot shows the Tenable.io interface for a 'New Scan / Advanced Network Scan'. The 'Plugins' tab is selected, displaying a table of enabled plugins. The table has columns for STATUS, PLUGIN FAMILY, TOTAL, STATUS, PLUGIN NAME, and PLUGIN ID. The 'STATUS' column for all plugins is 'ENABLED'. The 'PLUGIN NAME' column shows 'No plugin family selected.' for the first row. The 'TOTAL' column shows the count of findings for each plugin family.

STATUS	PLUGIN FAMILY	TOTAL	STATUS	PLUGIN NAME	PLUGIN ID
ENABLED	ADX Local Security Checks	11342		No plugin family selected.	
ENABLED	Amazon Linux Local Security Checks	1163			
ENABLED	Backdoors	114			
ENABLED	Brute force attacks	26			
ENABLED	CentOS Local Security Checks	2670			
ENABLED	CGI abuses	3937			
ENABLED	CGI abuses : XSS	669			
ENABLED	CISCO	954			
ENABLED	Databases	596			
ENABLED	Debian Local Security Checks	5841			
ENABLED	Default Unix Accounts	169			
ENABLED	Denial of Service	109			
ENABLED	DNS	173			

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

The screenshot shows the Tenable.io 'New Scan / Advanced Network Scan' configuration page. The 'Plugins' tab is active, showing a list of enabled plugins. The 'Oracle Linux 3 / 4 / 5 : bind (ELSA-2007-0740)' plugin is highlighted with a red box. The 'Save' button is visible at the bottom left.

STATUS	PLUGIN NAME	PLUGIN ID
ENABLED	Oracle Linux 3 / 4 / 5 : acpid (ELSA-2009-0474)	67855
ENABLED	Oracle Linux 3 / 4 / 5 : bind (ELSA-2007-0740)	67554
ENABLED	Oracle Linux 3 / 4 / 5 : bind (ELSA-2008-0533)	67709
ENABLED	Oracle Linux 3 / 4 / 5 : bind (ELSA-2009-0020)	67792
ENABLED	Oracle Linux 3 / 4 / 5 : bzip2 (ELSA-2008-0893)	67750
ENABLED	Oracle Linux 3 / 4 / 5 : bzip2 (ELSA-2010-0703)	68102
ENABLED	Oracle Linux 3 / 4 / 5 : cups (ELSA-2007-0123)	67462
ENABLED	Oracle Linux 3 / 4 / 5 : cups (ELSA-2007-0720)	67544
ENABLED	Oracle Linux 3 / 4 / 5 : cups (ELSA-2008-0498)	67699
ENABLED	Oracle Linux 3 / 4 / 5 : cups (ELSA-2008-0937)	67755
ENABLED	Oracle Linux 3 / 4 / 5 : cups (ELSA-2010-0490)	68052
ENABLED	Oracle Linux 3 / 4 / 5 : curl (ELSA-2009-0341)	67821
ENABLED	Oracle Linux 3 / 4 / 5 : curl (ELSA-2009-1209)	67910

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://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.