Tenable Nessus and Lieberman RED Integration Guide

Last Revised: August 31, 2023

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

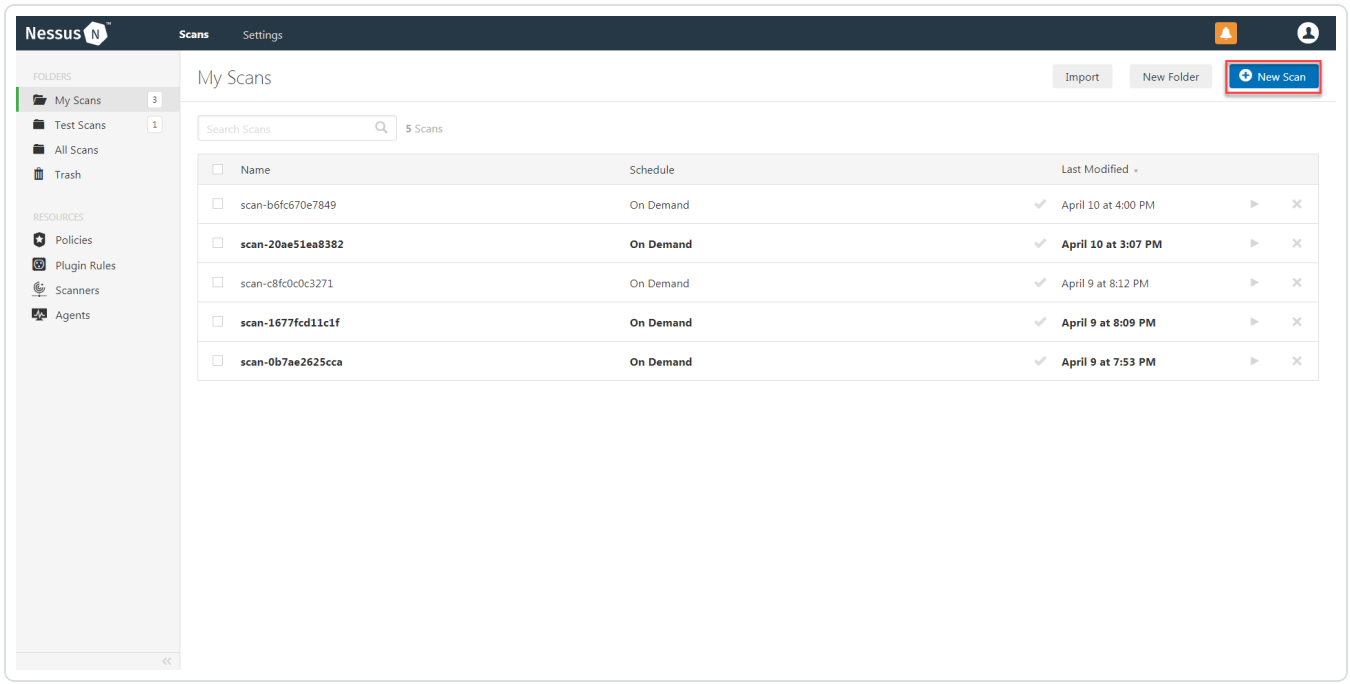
Configure Tenable Nessus for Lieberman SSH

Configure Tenable Nessus for Lieberman Database

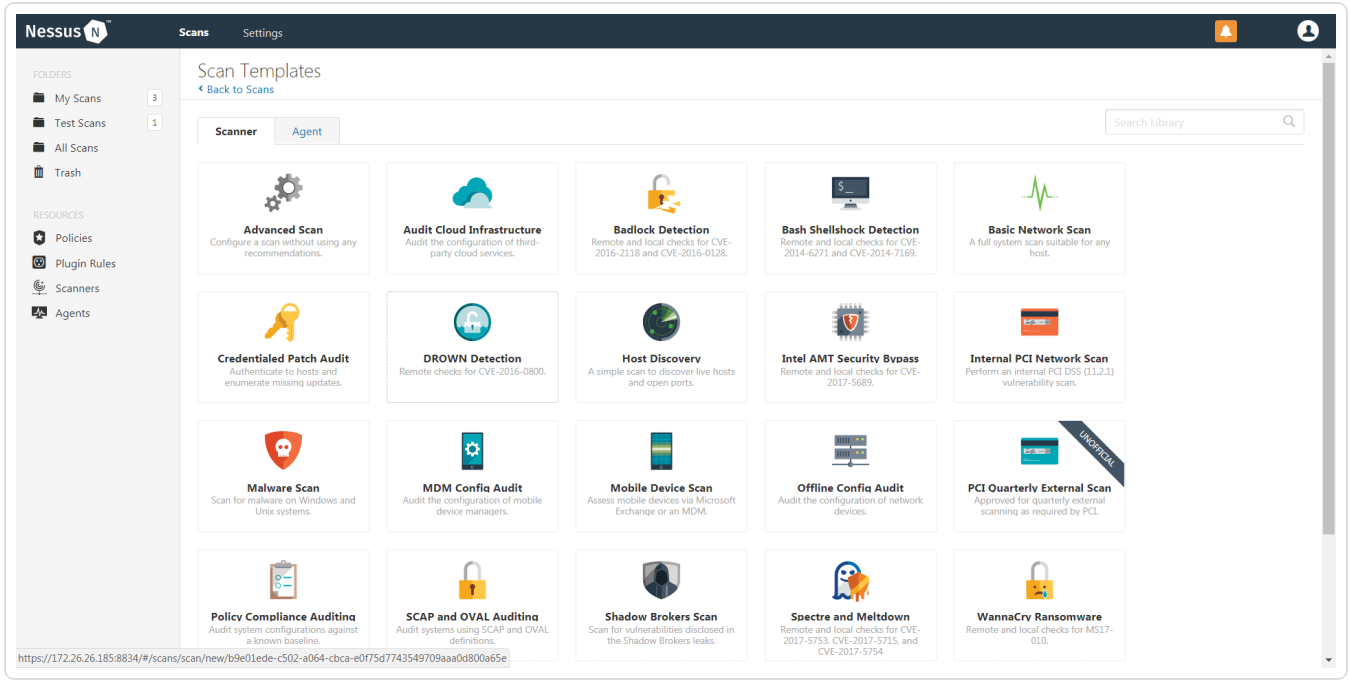
Configure Tenable Nessus for Lieberman Windows

To integrate with Windows:

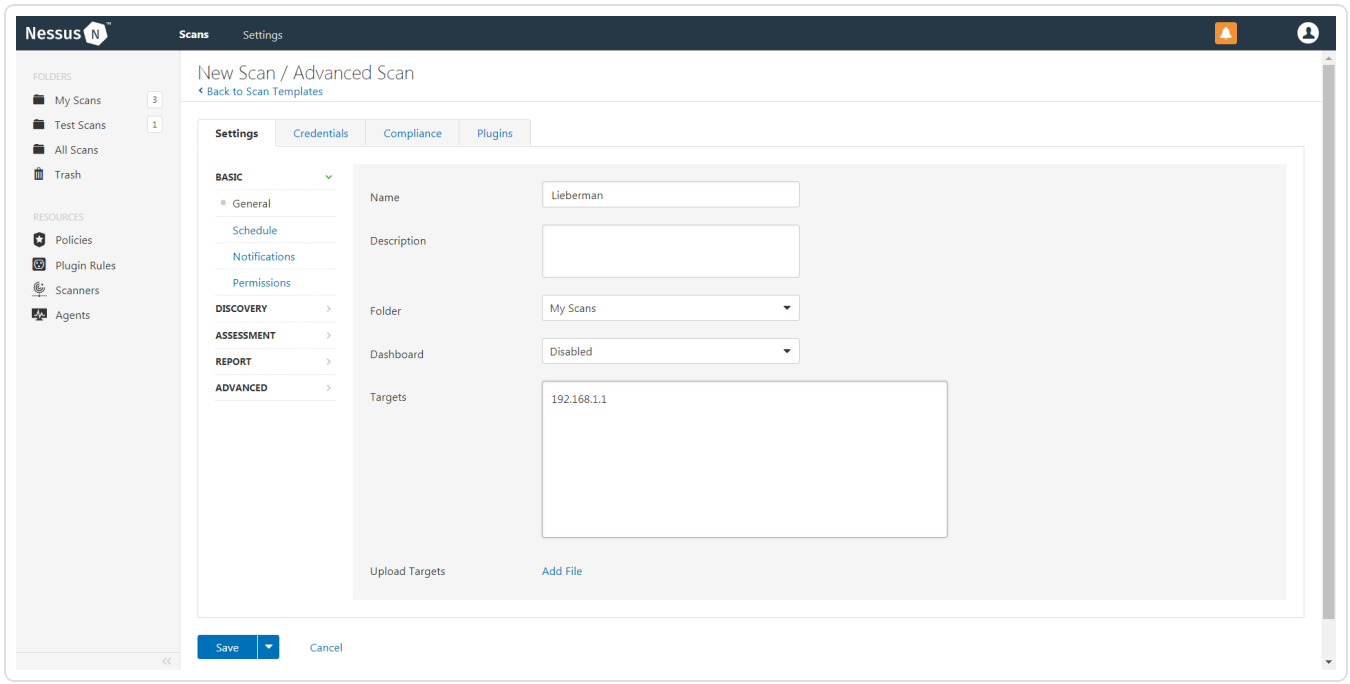
1. In a browser, log in to Nessus.
2. Navigate to the **Scans** section.
3. Click the **+ New Scan** button to configure Nessus for credentialed scans of Windows systems using Lieberman's password management solution.



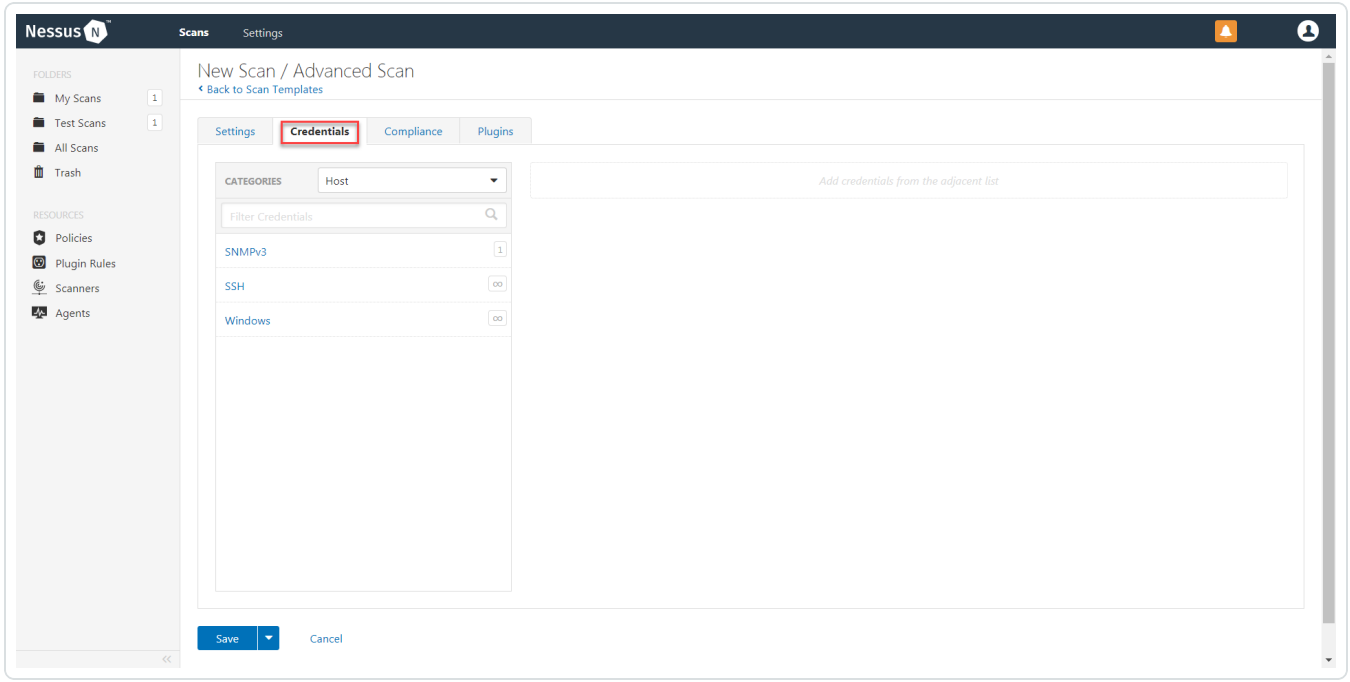
4. Select a **Scan Template** for the scan type required for your scan. For demonstration purposes, the **Advanced Network Scan** template is used.



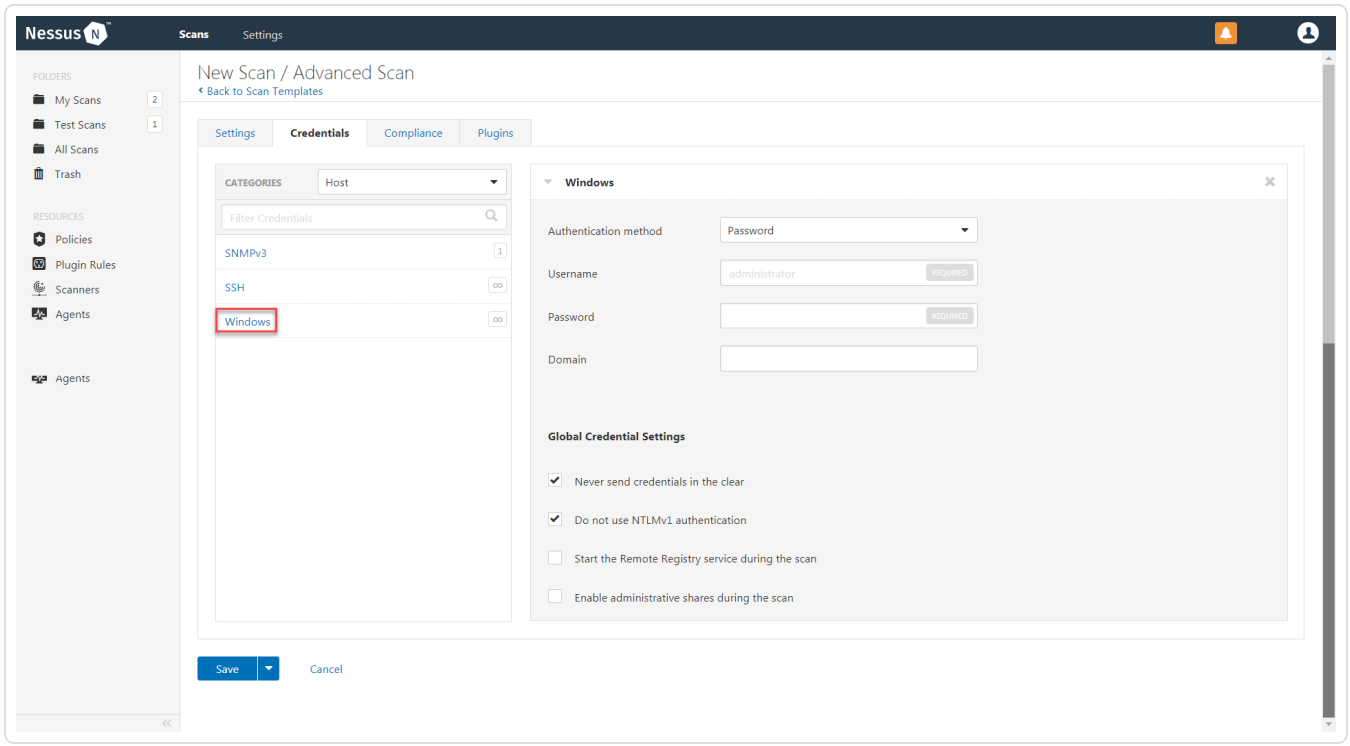
5. Enter a descriptive **Name** and the IP address(es) or hostname(s) of the scan **Targets**.



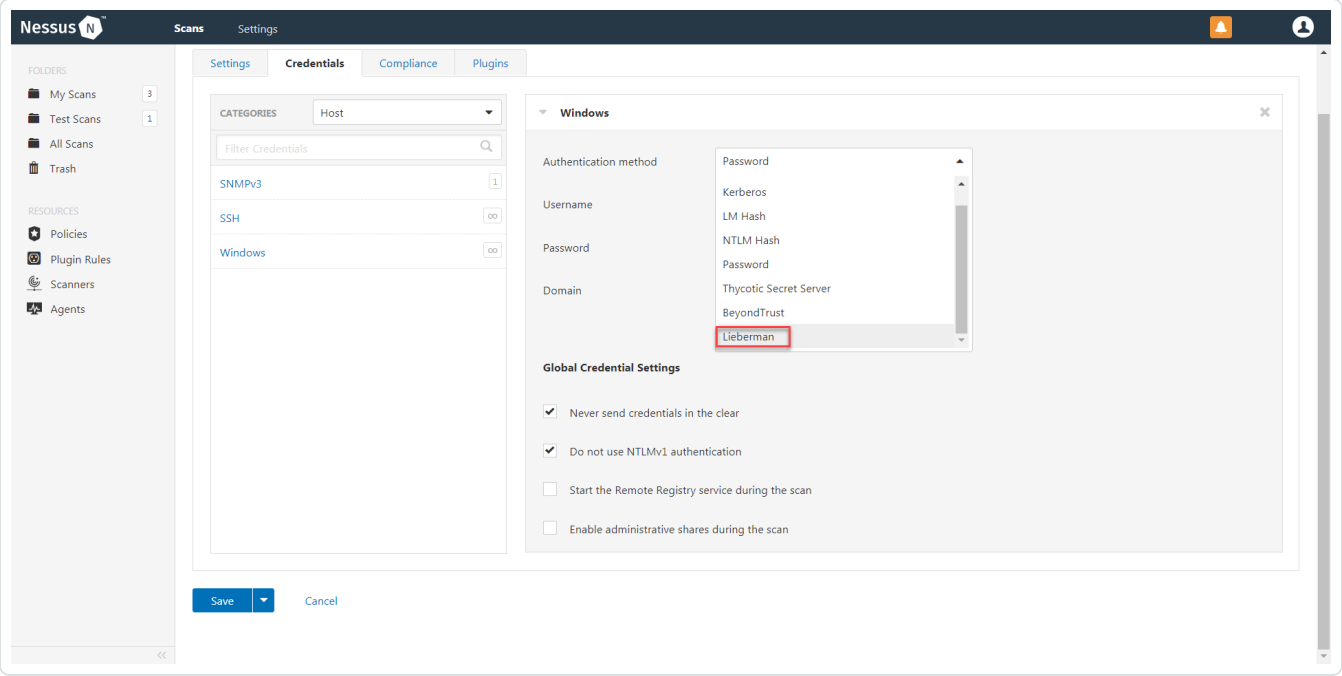
6. Click on the **Credentials** tab.



7. In the left-hand menu, select **Windows**.



8. From the **Authentication method** drop-down, select **Lieberman**.

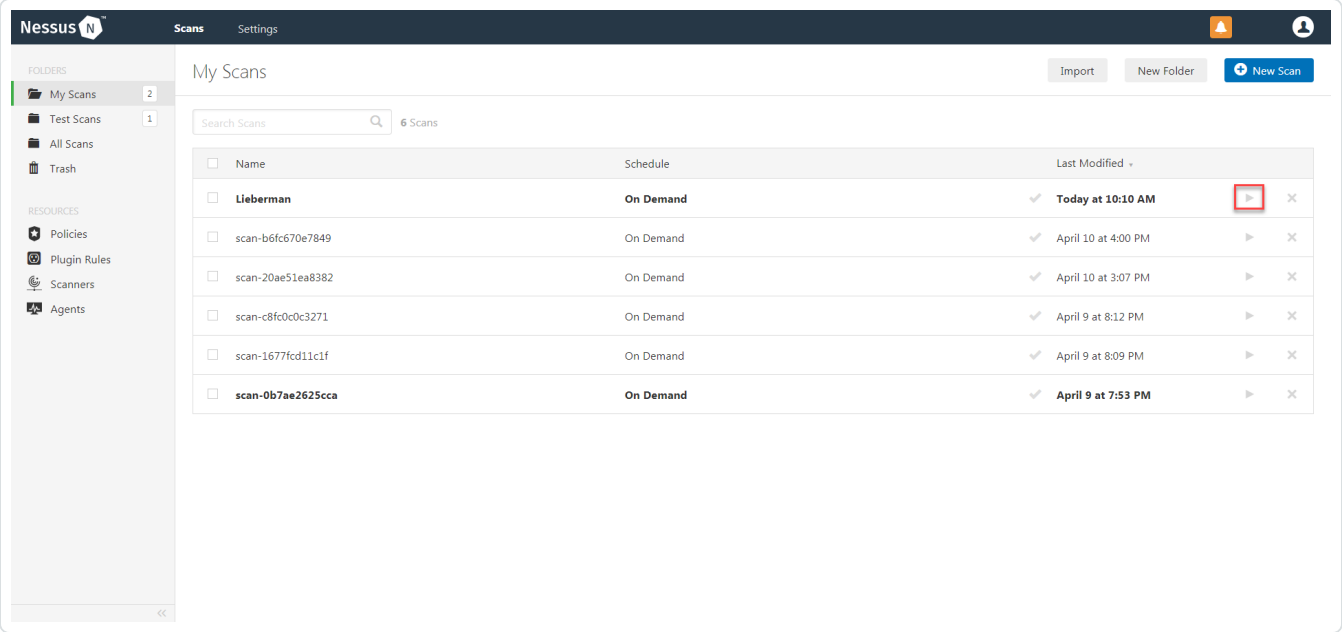


9. Configure each field for Windows authentication.

Option	Default Value
Username	(Required) The target system's username.
Domain	The domain, if the username is part of a domain.
Lieberman host	(Required) 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 host-name/subdirectory path*.
Lieberman port	(Required) The port on which Lieberman listens.
Lieberman user	(Required) The Lieberman explicit user for authenticating to the Lieberman RED API.
Lieberman password	(Required) The password for the Lieberman explicit user.
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*.
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.
Lieberman Client Certificate Private Key	The file that contains the PEM private key for the client certificate.
Lieberman Client Certificate Private Key Passphrase	The passphrase for the private key, if required.
Use SSL	If Lieberman is configured to support SSL through IIS, check for secure communication.
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.
System Name	In the rare case your organization uses one default Lieberman entry for all managed systems, enter the default entry name.

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



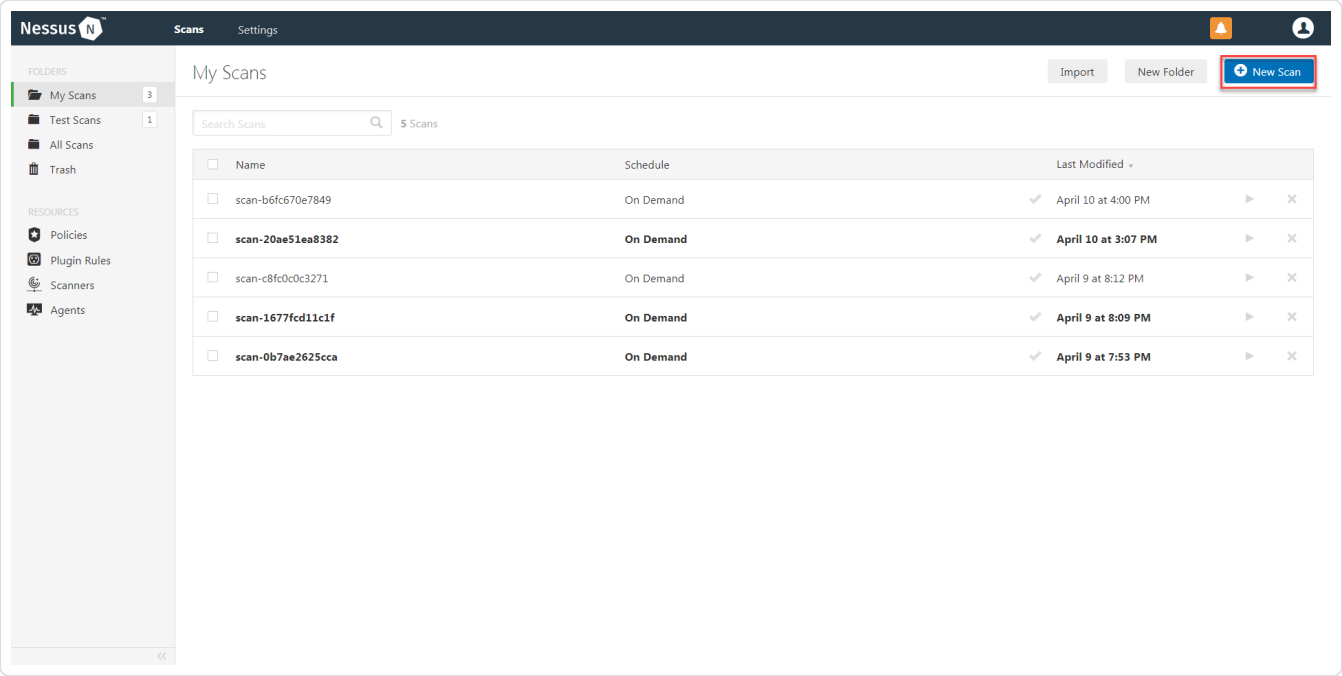
12. Once the scan has completed, select the completed scan and look for the corresponding message - *Microsoft Windows SMB Log In Possible: 10394*. This validates that authentication was successful.

Configure Tenable Nessus for Lieberman SSH

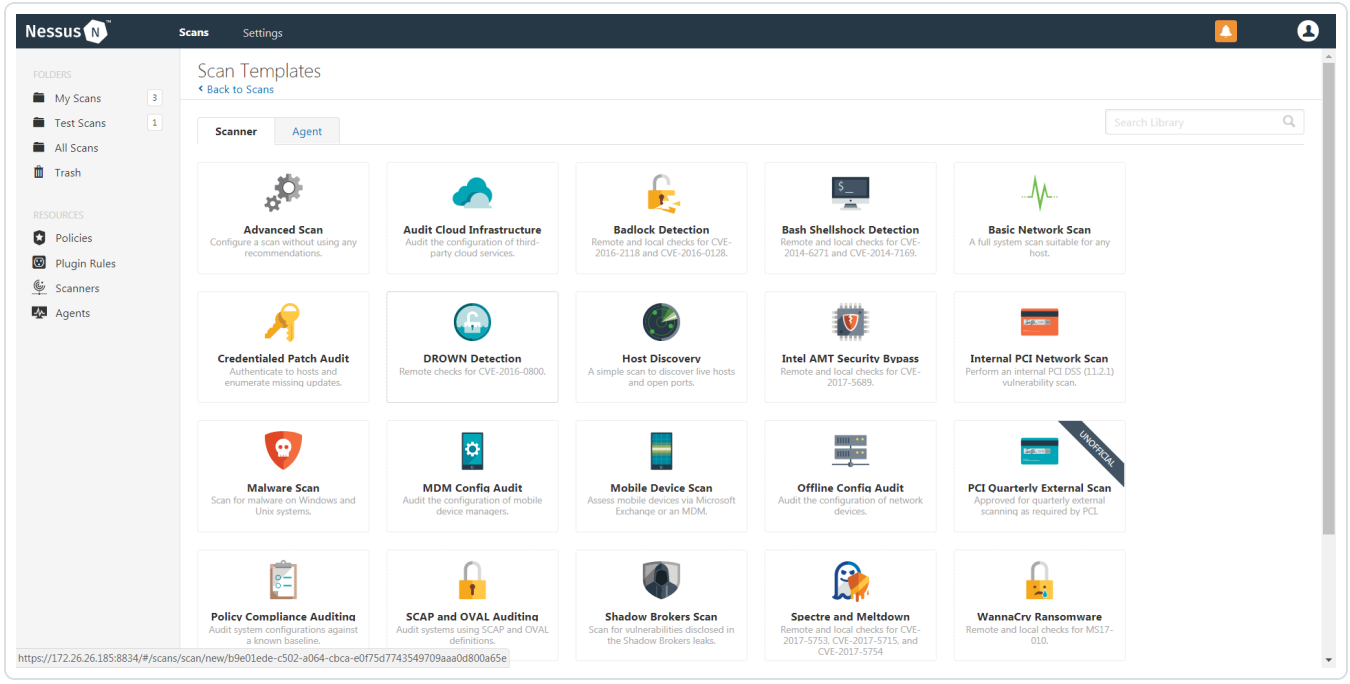
Tenable Nessus provides an option for Lieberman SSH integration. Complete the following steps to configure Nessus with Lieberman SSH. (Any other descriptive verbiage we can add here?)

To configure Nessus for Lieberman SSH:

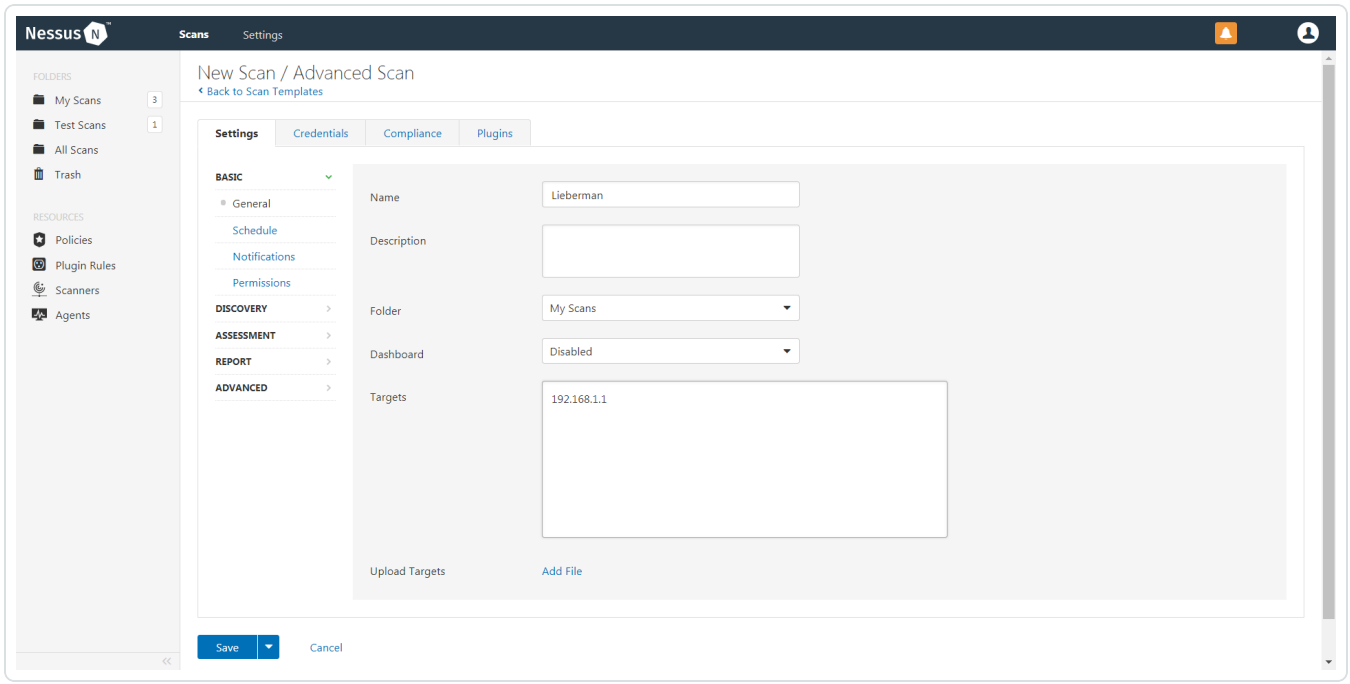
1. In a browser, log in to Nessus.
2. Navigate to the **Scans** section.
3. Click the **+ New Scan** button to configure Nessus for credentialed scans of Windows systems using Lieberman's password management solution.



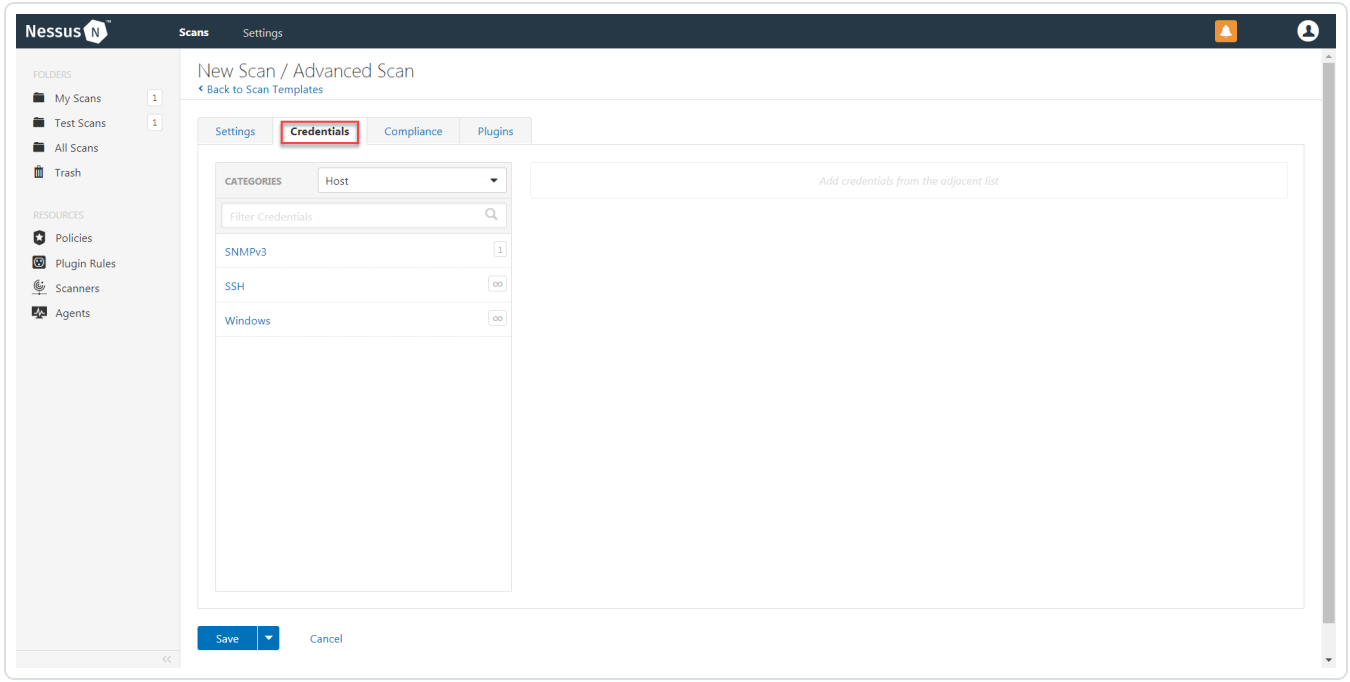
4. Select a **Scan Template** for the scan type required for your scan. For demonstration purposes, the **Advanced Network Scan** template is used.



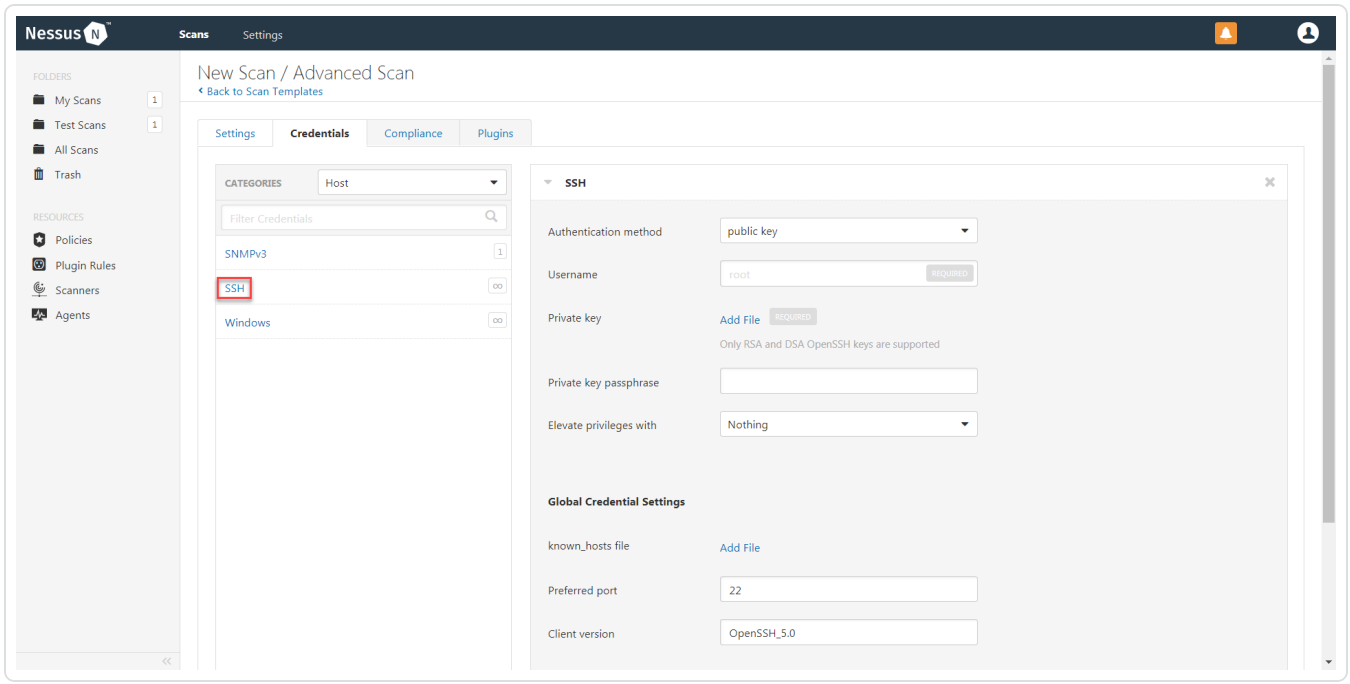
5. Enter a descriptive **Name** and the IP address(es) or hostname(s) of the scan **Targets**.



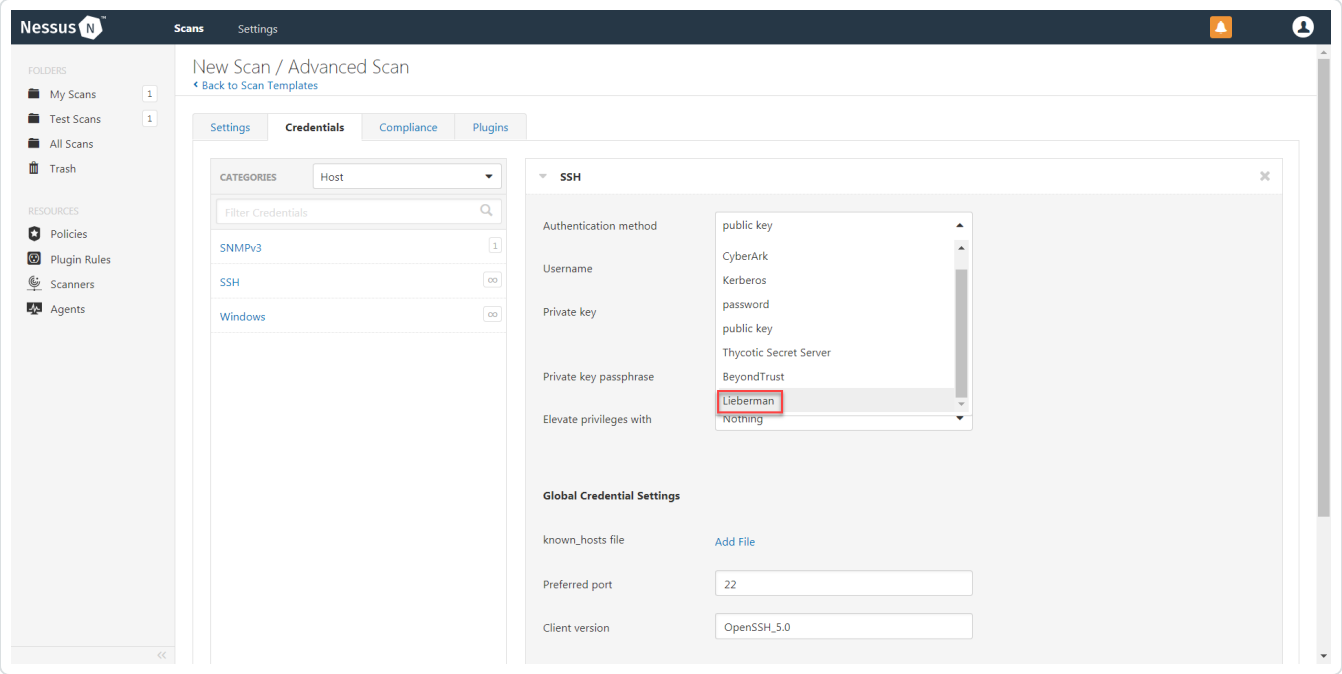
6. Click on the **Credentials** tab.



7. In the left-hand menu, select **SSH**.



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



9. Configure each field for SSH authentication.

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 sub-directory, 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 ManagementTen-able Nessus uses to access Lieberman.	no
Lieberman user	The Lieberman explicit user for authenticating to the Lieberman RED API.	yes
Lieberman pass-word	The password for the Lieberman explicit user.	yes

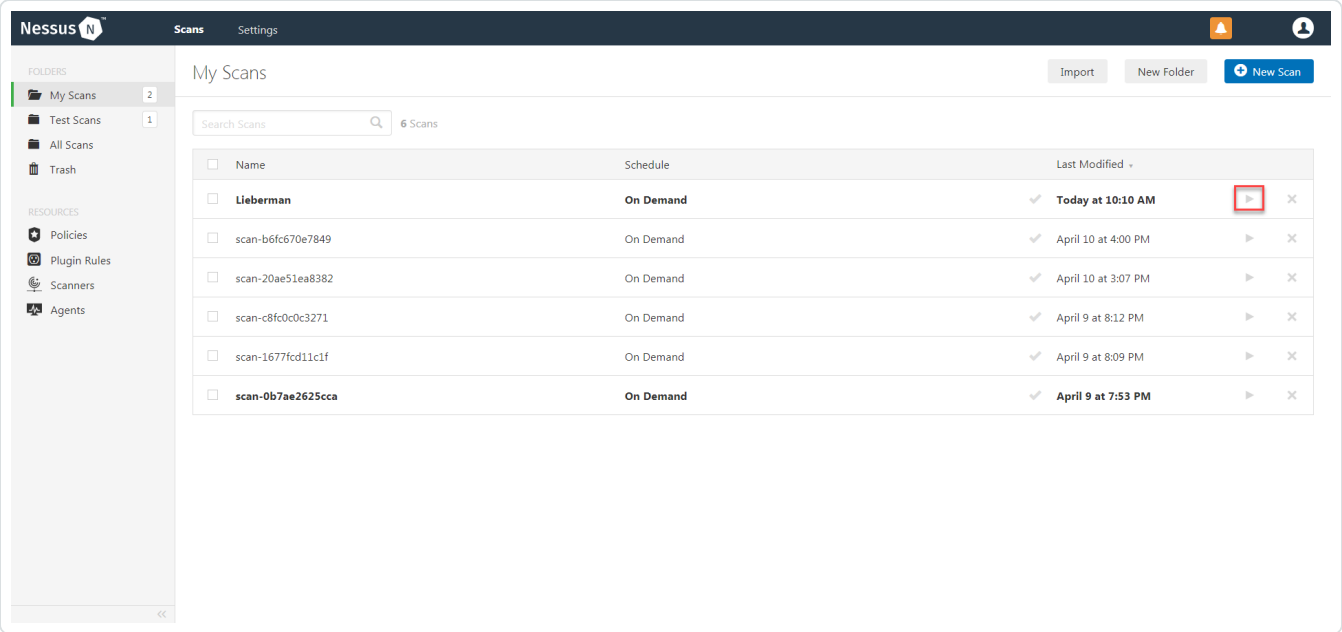
Option	Description	Required
Lieberman Authenticator	The alias used for the authenticator in Lieberman. The name should match the name used in Lieberman. **Note:** If you use this option, append a domain to the **Lieberman user** option, i.e., *domain\user*.	no
Lieberman Client Certificate	The file that 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 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 pass-	The password prompt used by the target host. Only	no

Option	Description	Required
word prompt	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.	

10. Click **Save**.

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 Database

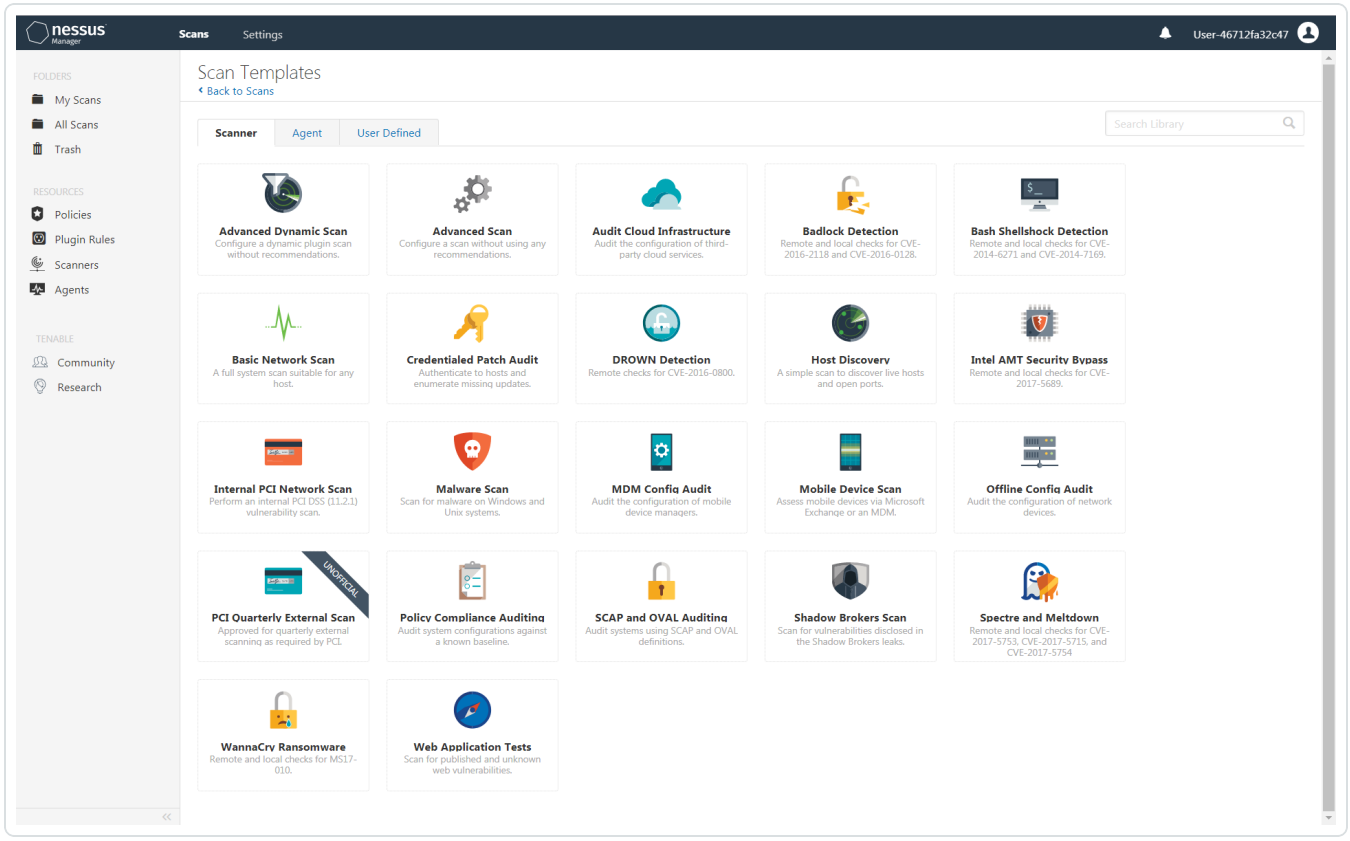
Tenable Nessus provides full database support for Lieberman. Enable Database Plugins in Nessus in the scanner to display them in the output.

To configure Nessus for Lieberman database:

1. Log in to Tenable Nessus Manager.
2. Click **Scans**.

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

   The **Scan Templates** page appears.

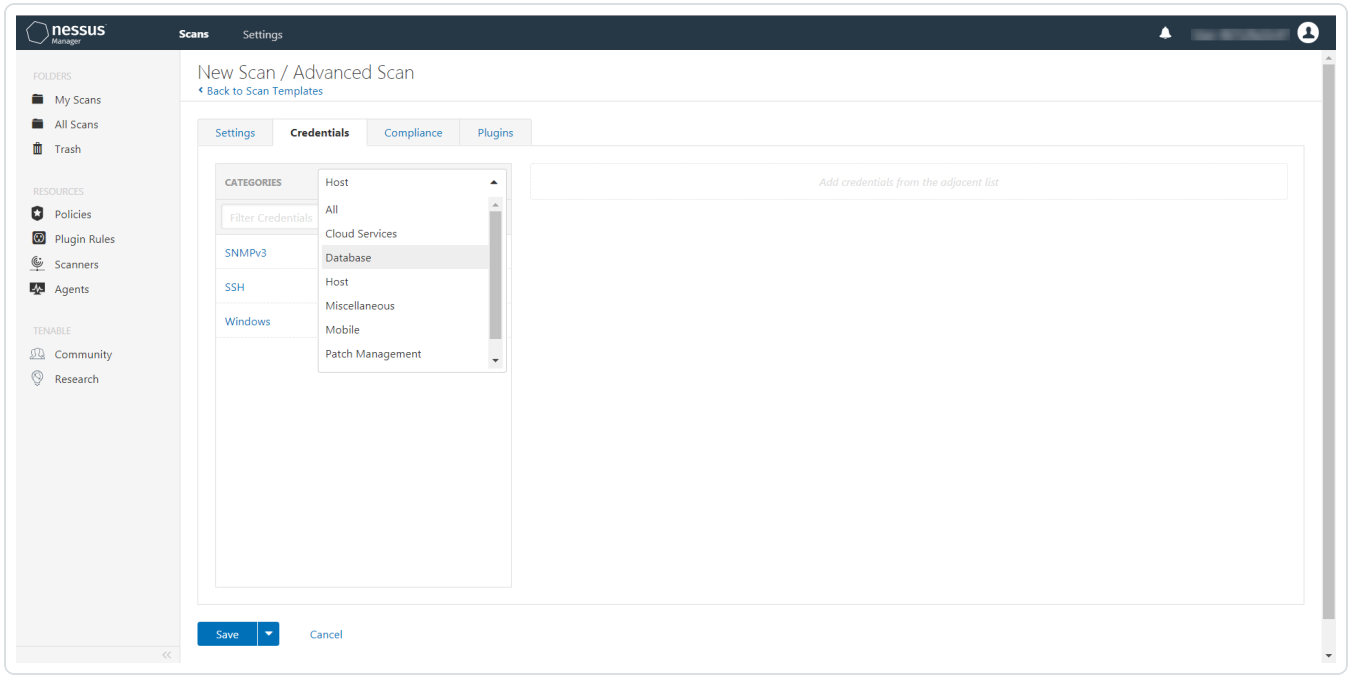


4. Select a **Scan Template**. For example, this procedure walks through the **Advanced Network Scan** template.

   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. By default, the **Categories** drop-down box displays **Host**.
9. In the **Categories** drop-down box, select **Database**.



   The **Database** options appear below.
10. In the **Categories** list, click **Database**.

    The **Database** options appear.
11. Click the **Database Type** drop-down box.

    The **Database** options appear.
12. In the **Database Type** drop-down box, click **Oracle**.
13. In the **Auth Type** drop-down box, click **Lieberman**.

The **Lieberman** options appear.

14. Configure each option for the **Database** authentication.
15. Click **Save**.

Enable Database Plugins in Nessus

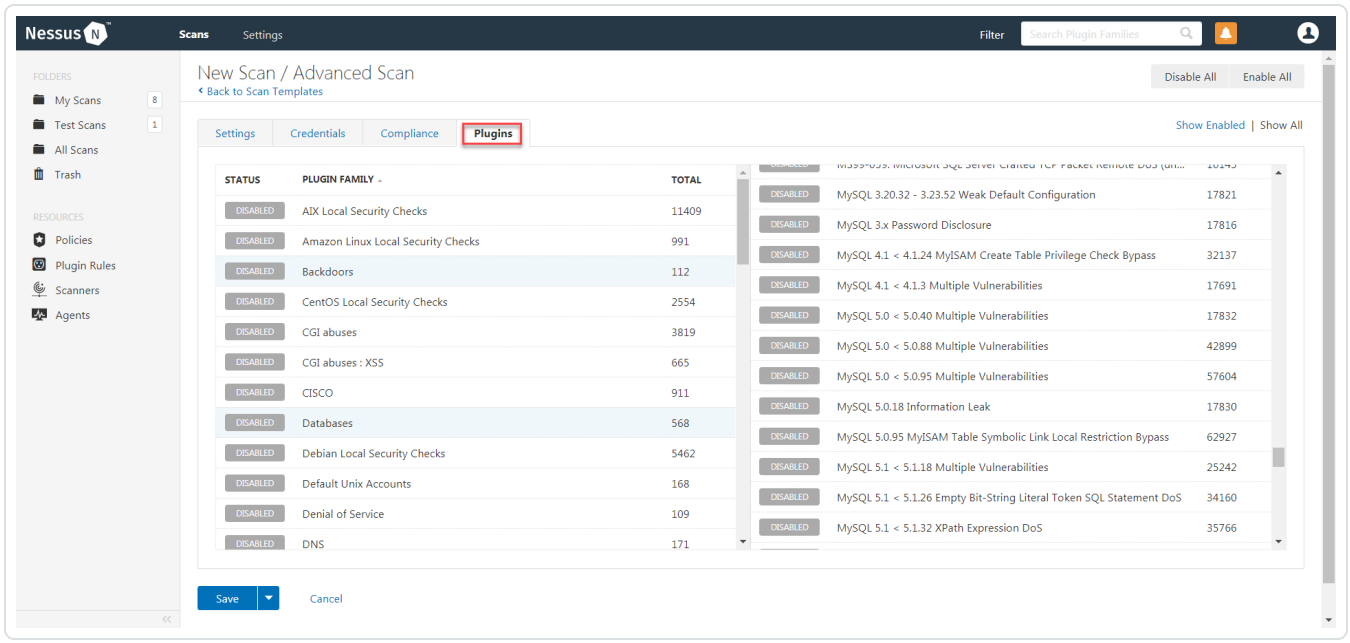
You can enable database plugins in your Tenable Application for your configured Lieberman Database account.

To enable database plugins:

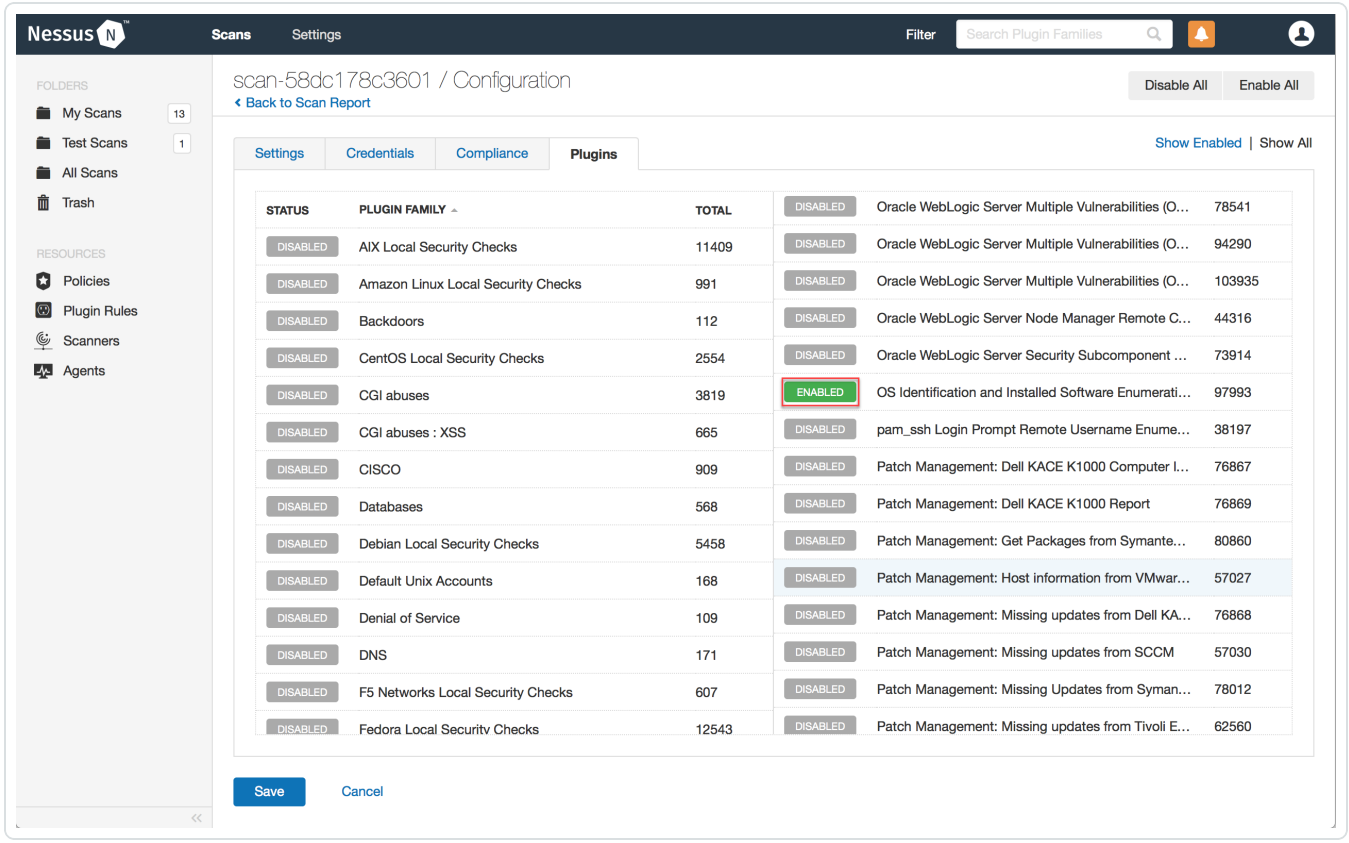
1. In the scan where you configured the Lieberman credentials, click the **Plugins** tab.

   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

Tenable Vulnerability Management 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 Vulnerability Management for Lieberman Windows

Configure Tenable Vulnerability Management for Lieberman SSH

Configure Tenable Vulnerability Management for Lieberman Database

Configure Tenable Vulnerability Management for Lieberman Windows

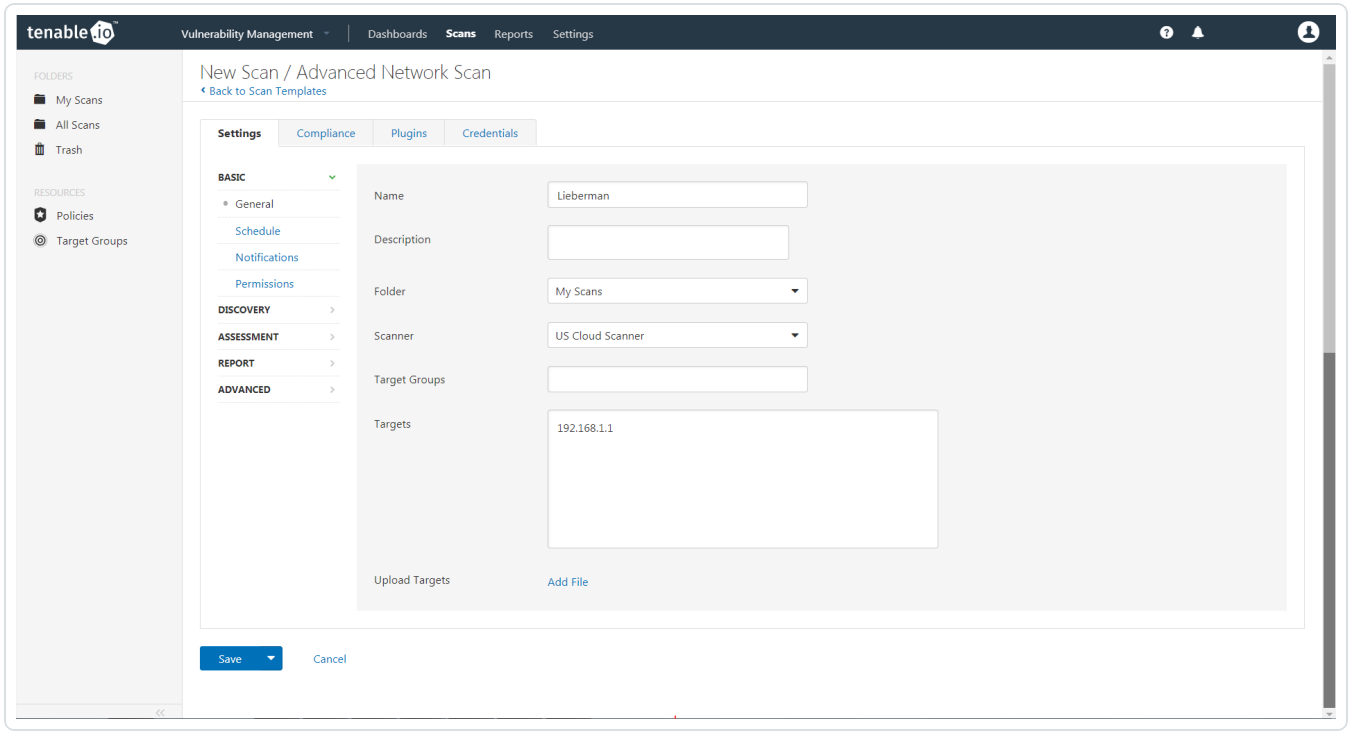
To integrate with Windows:

1. Log in to Tenable Vulnerability Management.
2. Click **Scans**.

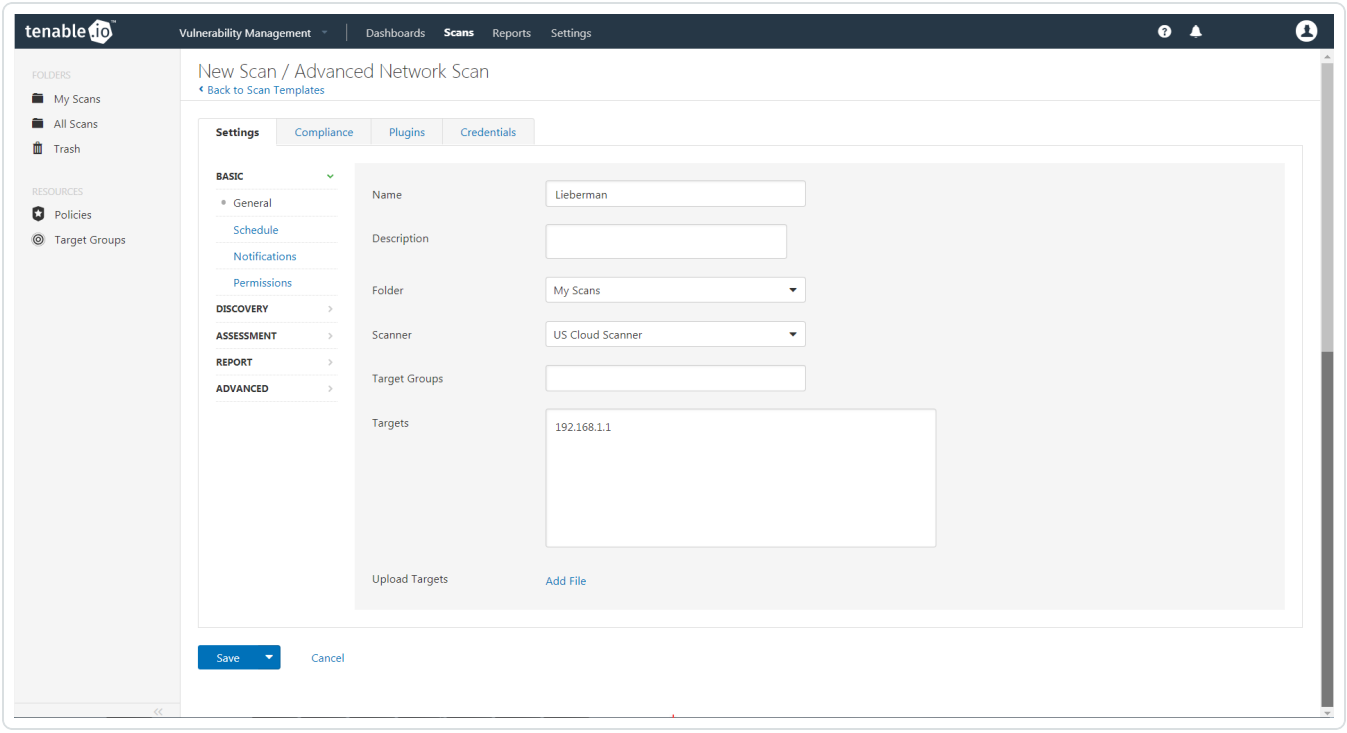
   The **My Scans** page appears.
3. Click **+ New Scan**.

   The **Scan Templates** page appears.
4. Select a **Scan Template**.

   The **Settings** for the selected scan template appears.



5. Enter a descriptive **Name** and the IP address(es) or hostname(s) of the scan **Targets**.

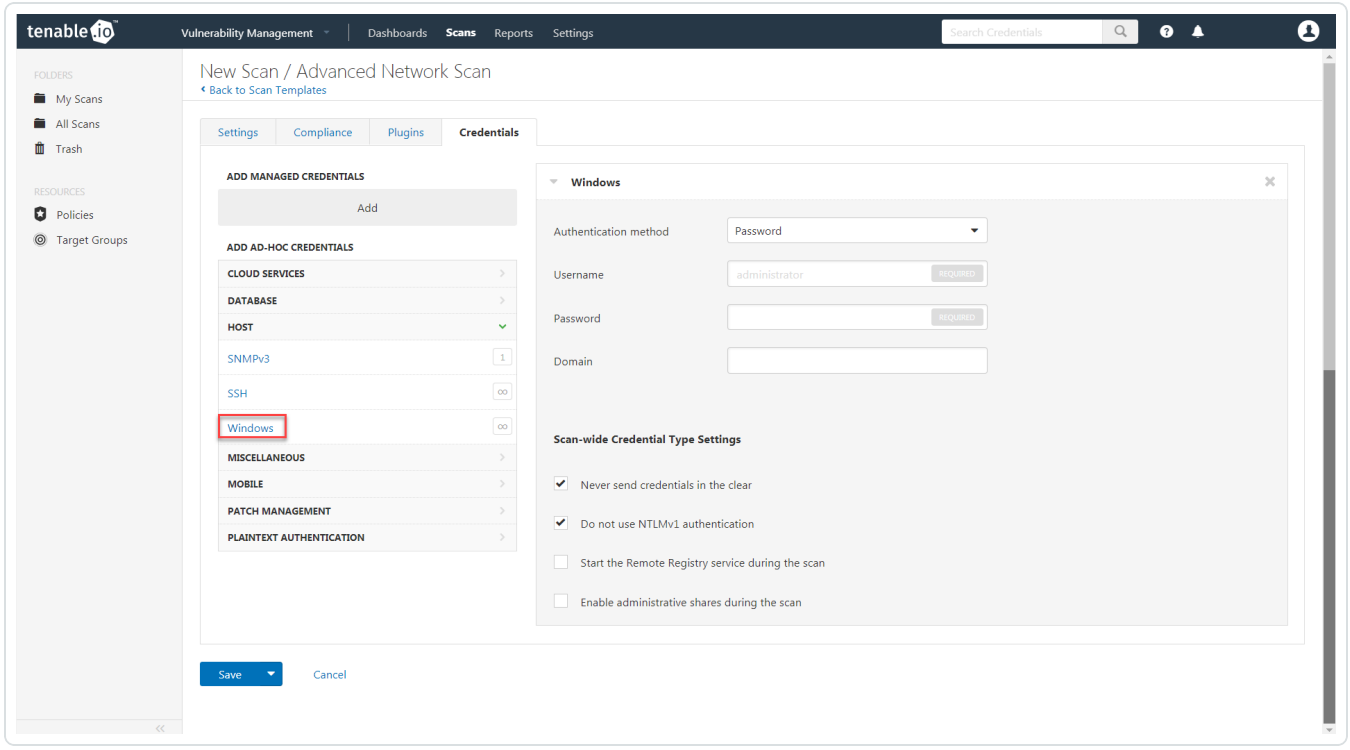


6. Click on the **Credentials** tab.

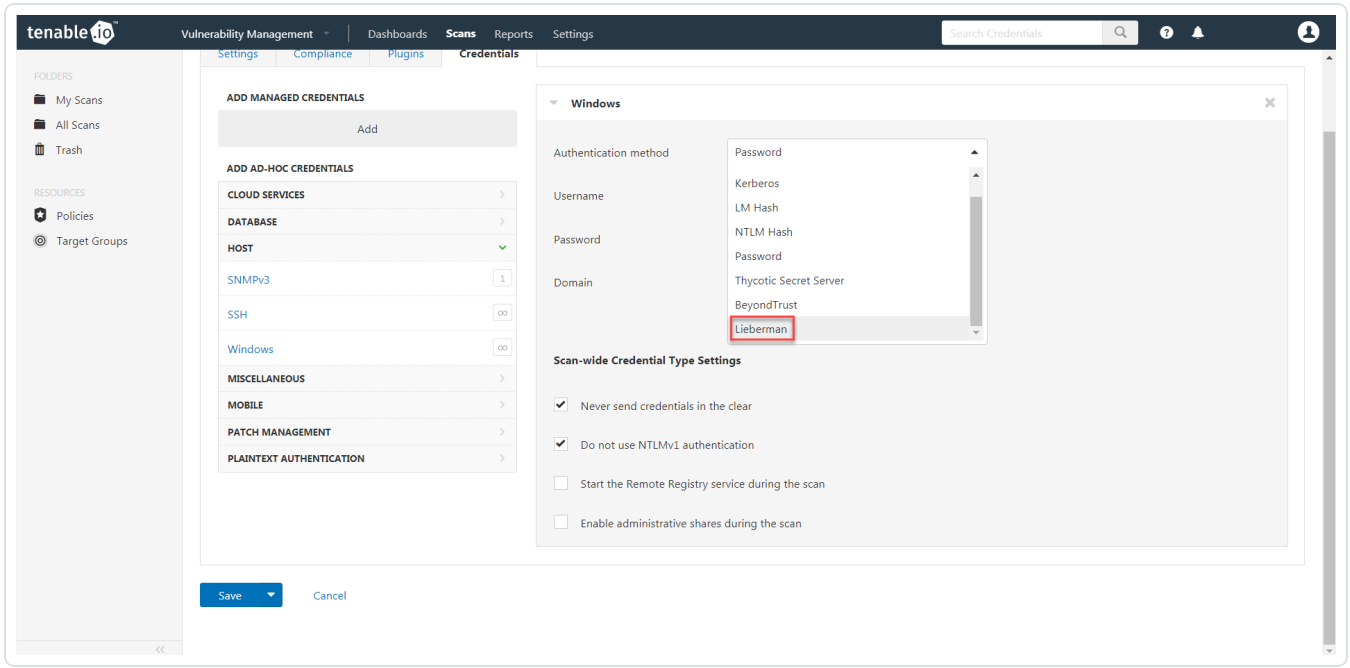
   The **Add Managed Credentials** section appears.

7. In the left-hand menu, select **Windows**.

   The **Windows** section appears.



8. From the **Authentication method** drop-down, select **Lieberman**.



The **Lieberman** options appear.

9. Configure each field for Windows authentication.

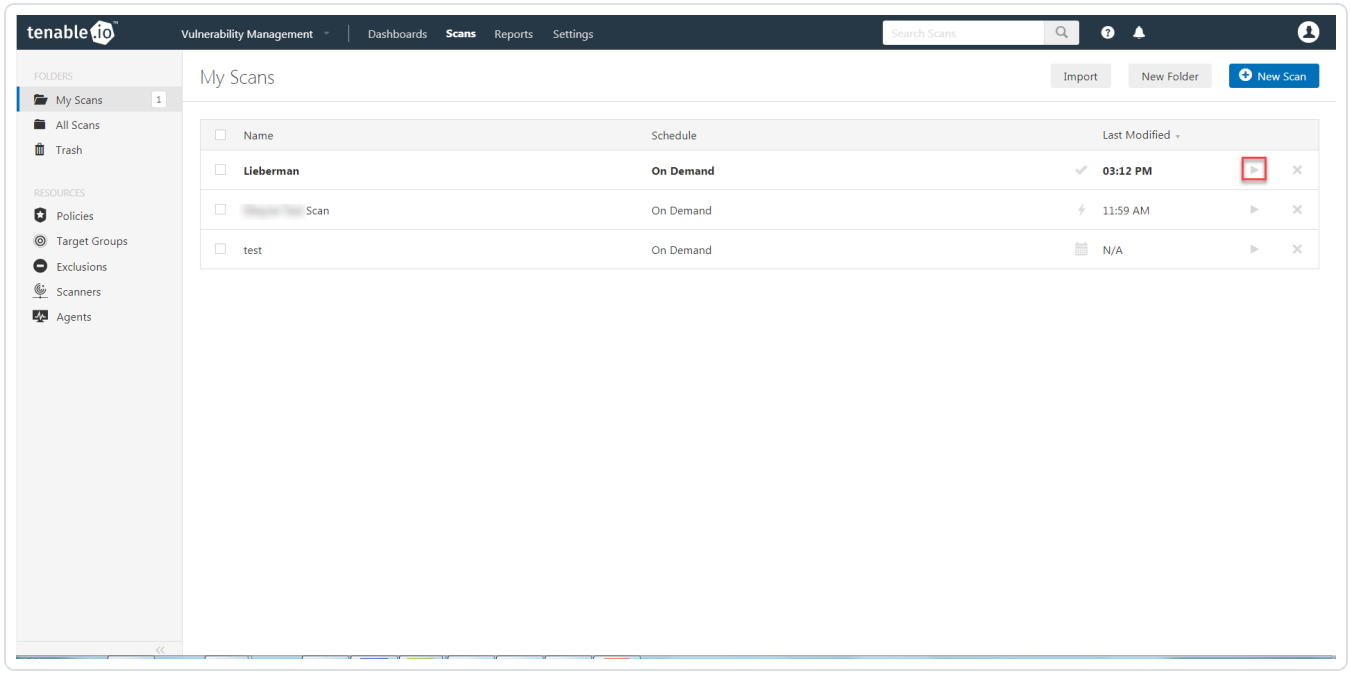
Option	Description	Required
Username	The target system's username.	yes
Domain	The domain, if the username is part of a domain.	no
Lieberman host	The Lieberman IP/DNS address. **Note:** If your Lieberman installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname / subdirectory path*.	yes
Lieberman port	The port on which Lieberman listens.	yes
Lieberman 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, you should 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

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

10. Click **Save**.

What to do next:

1. To verify the integration works, click the **Launch** button to initiate an on-demand scan.



2. After the scan completes, click the completed scan and look for the following message - *Microsoft Windows SMB Log In Possible: 10394*. This validates that authentication was successful.

Configure Tenable Vulnerability Management for Lieberman SSH

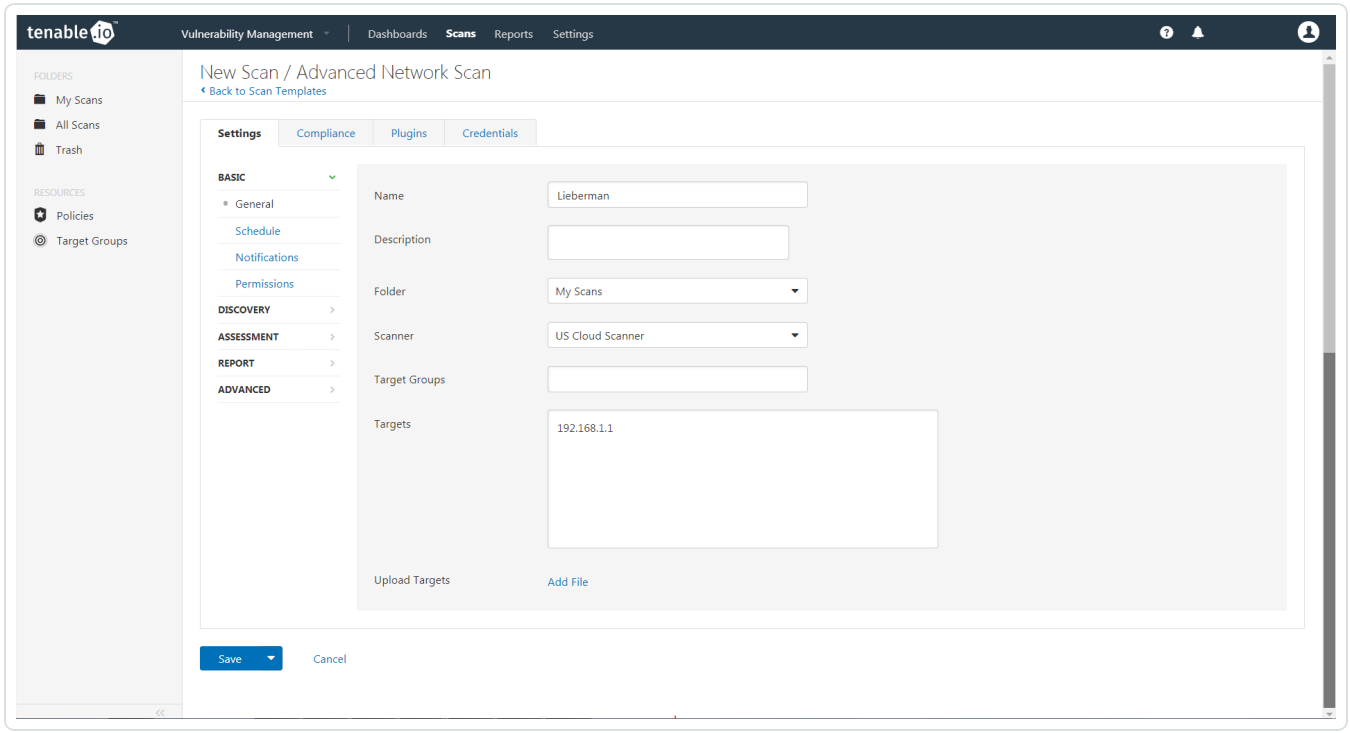
To integrate with SSH:

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. Select a **Scan Template**.

   The **Settings** page for the selected scan appears.

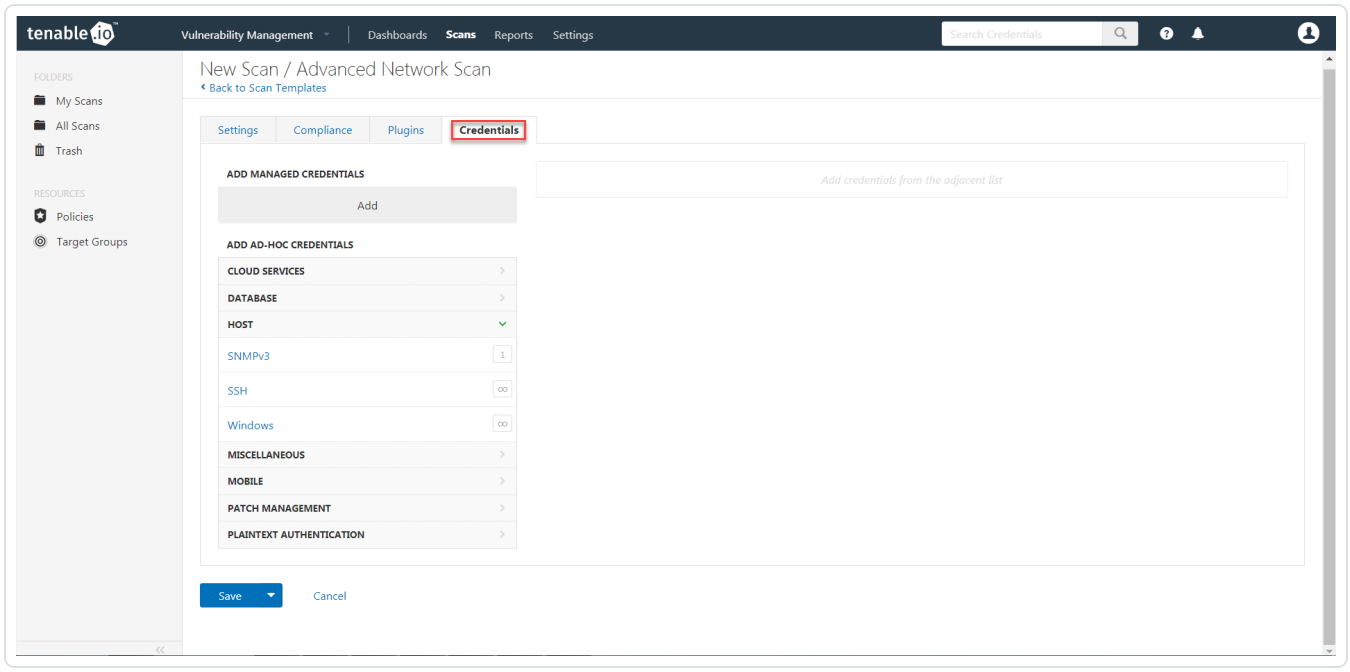


5. In the **Name** box, type a name for the scan.
6. In the **Targets** box, type an IP address, hostname, or range of IP addresses.

7. (Optional) You can add a description, folder location, scanner location, and specify target groups.

8. Click on the **Credentials** tab.

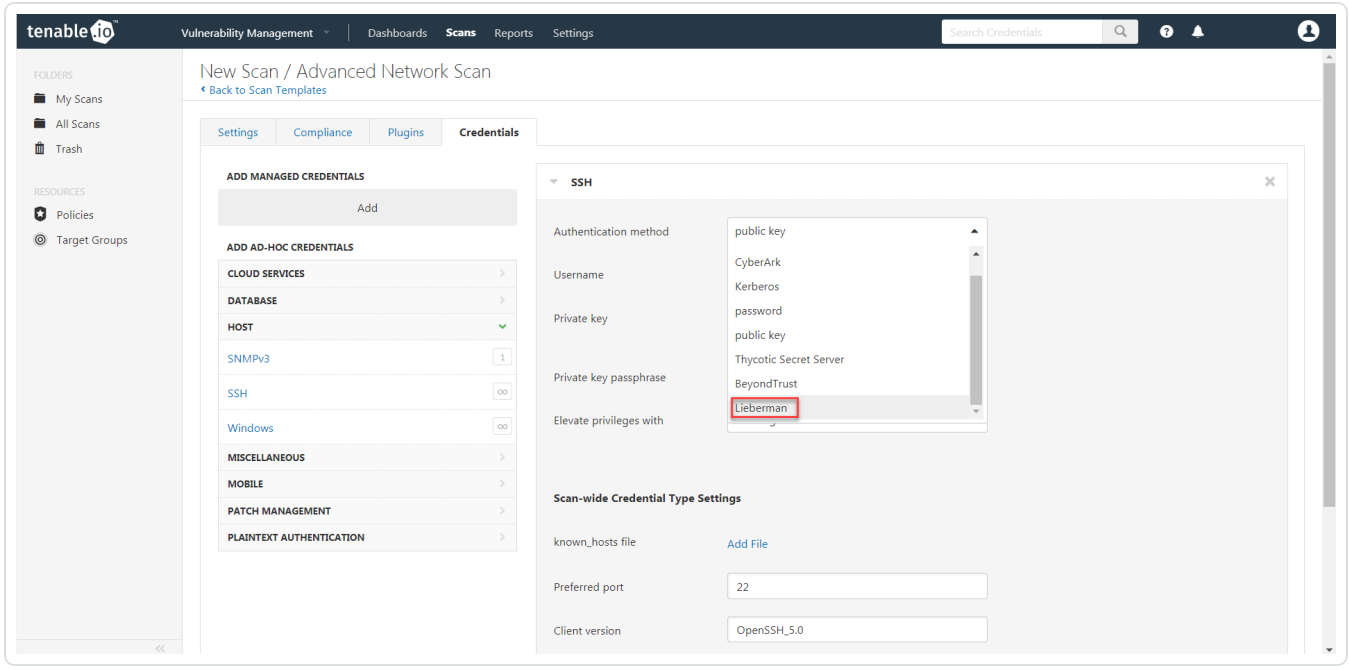
   The **Add Managed Credentials** options appear.



9. In the left-hand menu, select **SSH**.

   The SSH options appear.

10. From the **Authentication method** drop-down, select **Lieberman**.



The Lieberman options appear.

11. Configure each field for SSH authentication.

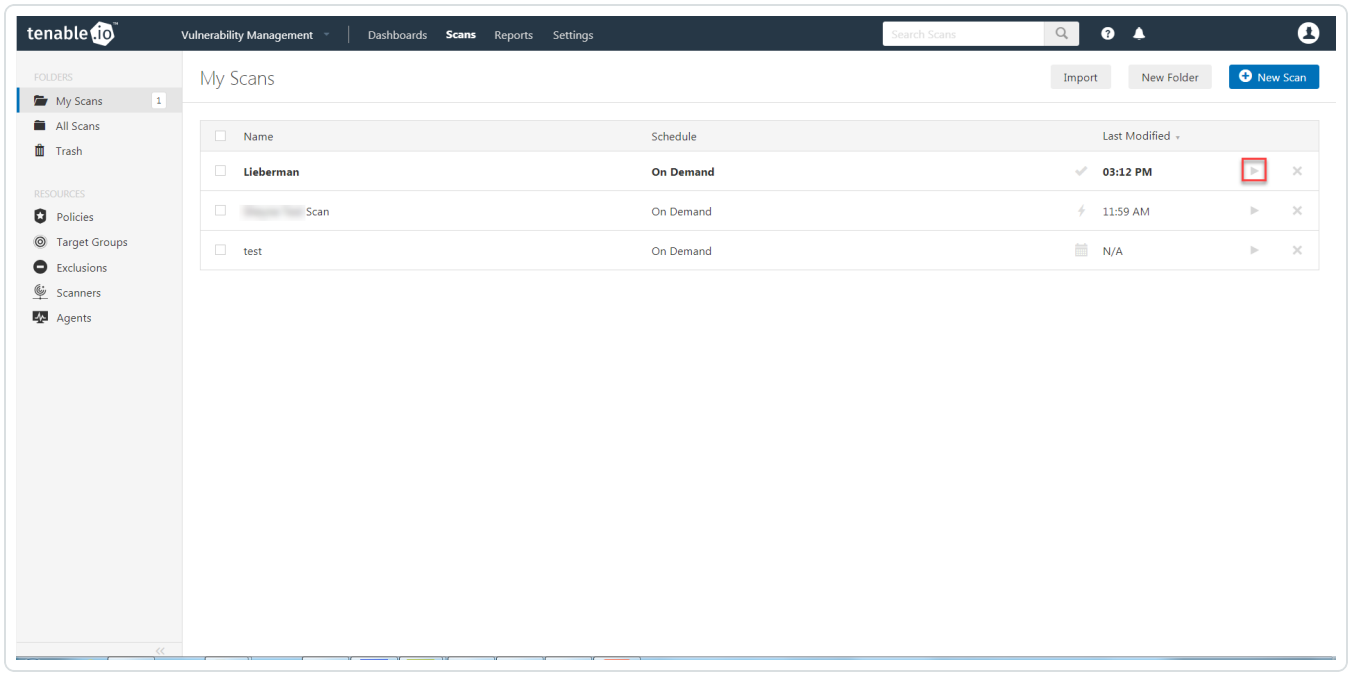
Option	Description	Required
Username	The target system's username.	yes
Lieberman host	The Lieberman IP/DNS address. **Note:** If your Lieberman installation is in a sub-directory, you must include the subdirectory path. For example, type *IP address or hostname / subdirectory path*.	yes
Lieberman port	The port on which Lieberman listens.	yes
Lieberman API URL	The URL Tenable Vulnerability Management uses to access Lieberman.	no
Lieberman user	The Lieberman explicit user for authenticating to the Lieberman RED API.	yes
Lieberman pass-	The password for the Lieberman explicit user.	yes

Option	Description	Required
word		
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 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

12. Click **Save**.

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 Vulnerability Management for Lieberman Database

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

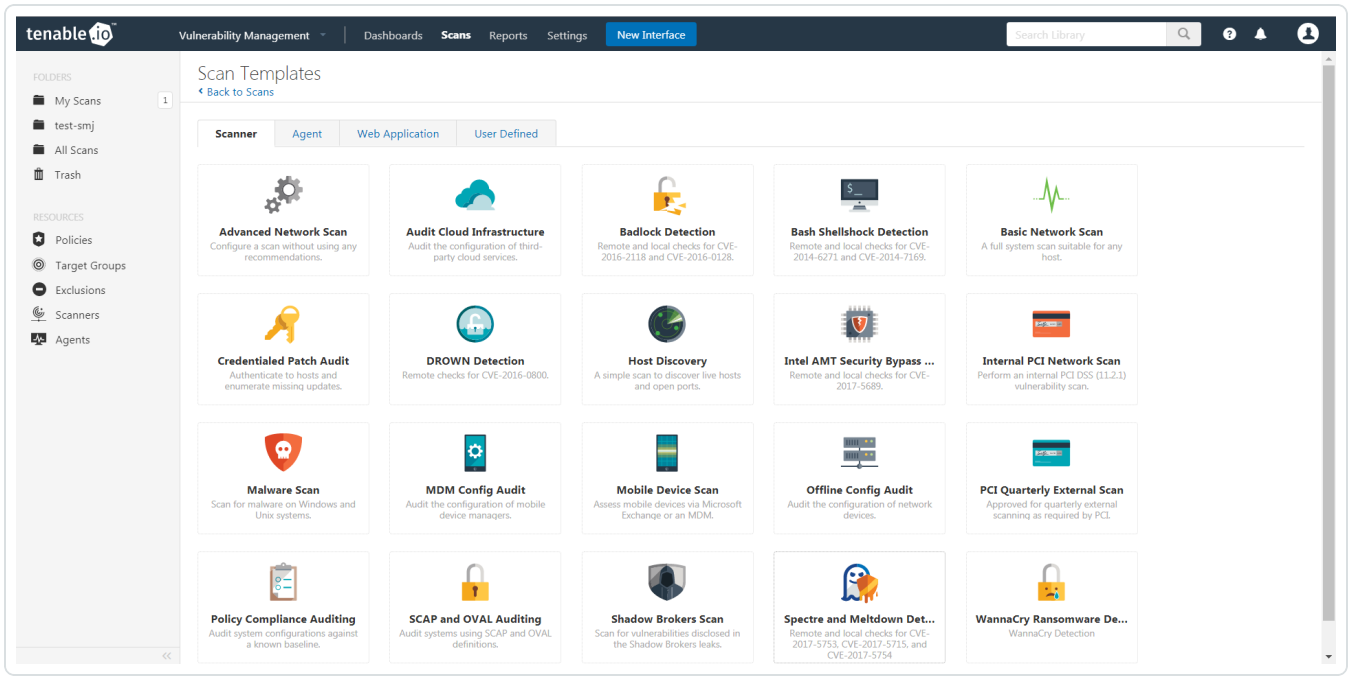
What role is required to perform this configuration?

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.



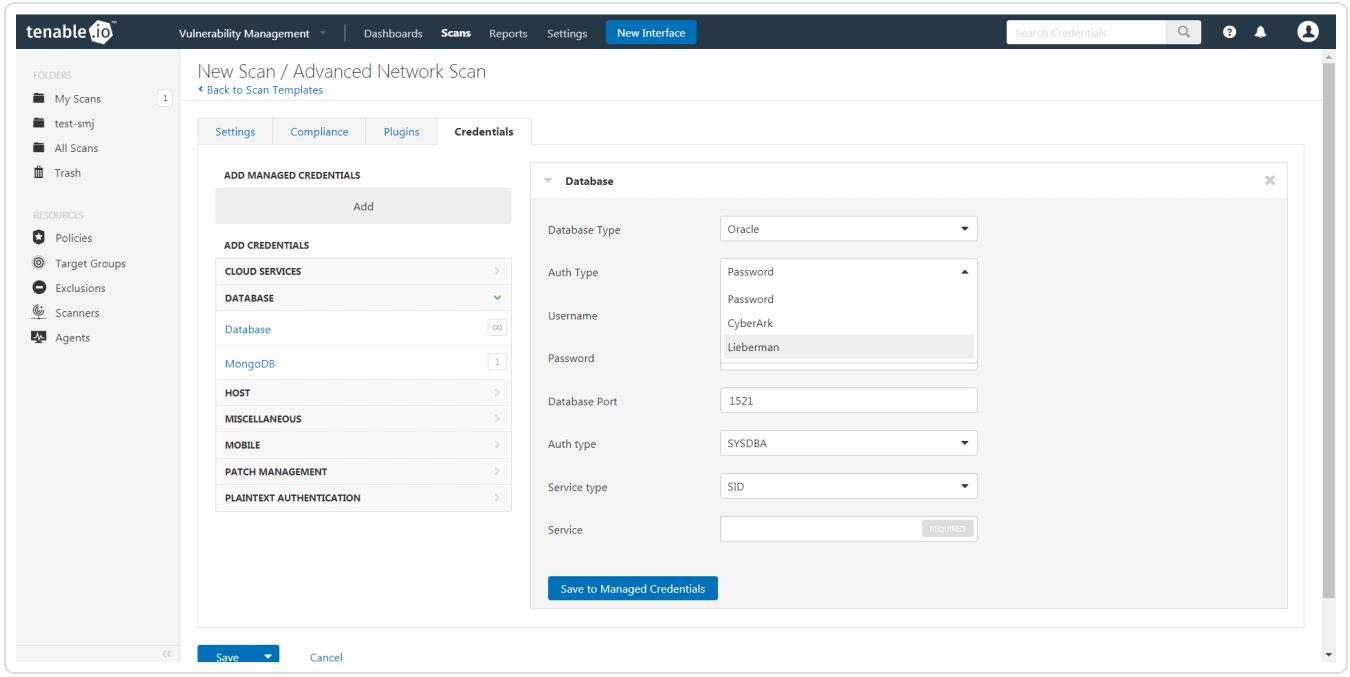
4. Click a **Scan Template**. For example, this procedure walks through the **Advanced Network Scan** template.

   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 **Lieberman** options appear.

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

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
Lieberman port	The port on which Lieberman listens.	yes
Lieberman user	The Lieberman explicit user for authenticating to the Lieberman API.	yes
Lieberman password	The password for the Lieberman explicit user.	yes
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
Database Port	The port on which Tenable Vulnerability Management communicates with the database.	yes
Database Name	(PostgreSQL and DB2 databases only) The name of the database.	no

16. Click **Save**.

Tenable Security Center Supported Credentials

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

Configure Tenable Security Center for Lieberman Windows

Configure Tenable Security Center for Lieberman SSH

Configure Tenable Security Center for Lieberman Database

Add a Credential to a Scan

Configure Tenable Security Center for Lieberman Windows

To integrate with Windows:

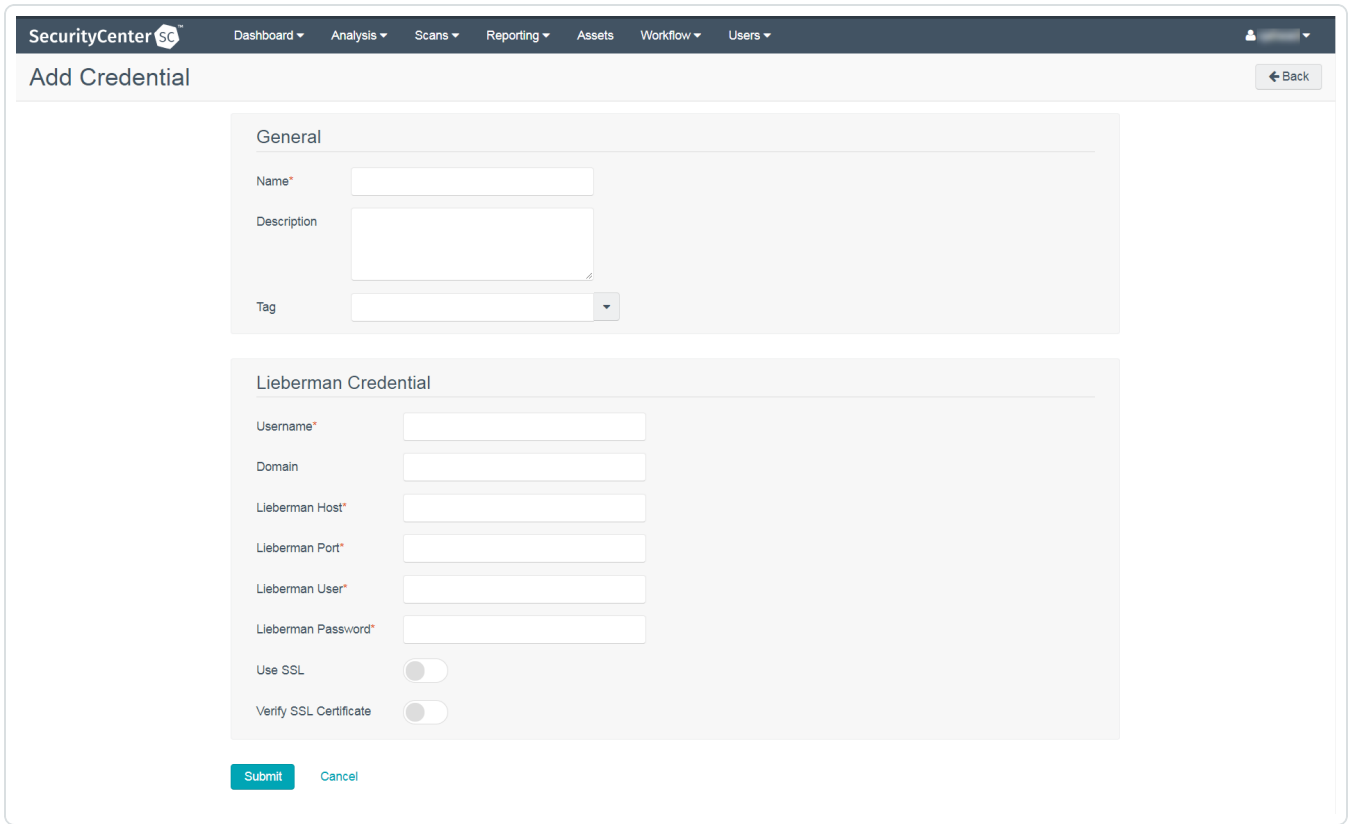
1. Log in to Tenable Security Center.
2. In the top navigation bar, click **Scanning**.

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

   The **Credentials** window opens.
4. In the upper-right corner, 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 General section:
    - (Required) In the **Name** box, enter a descriptive name.
    - (Optional) In the **Description** box, type a brief description.
    - (Optional) In the **Tag** box, select a tag in from the drop-down menu.
7. Configure each field for **Windows** authentication.

Option	Description
Username	The username for a user on the database.
Domain	The domain of the username, if required by Lieberman.
Lieberman Host	The Lieberman IP address or 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*.
Lieberman Port	The port Lieberman is listening on.
Lieberman User	The username for the Lieberman explicit user you want Tenable Security Center to use for authentication to the Lieberman Rapid Enterprise Defense (RED) API.
Lieberman Password	The password for the Lieberman explicit user.
Use SSL	When enabled, Tenable Security Center uses SSL through IIS for secure communications. You must configure SSL through IIS in Lieberman before enabling this option.
Verify SSL Certificate	When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL through IIS in Lieberman before enabling this option. For more information about using self-signed certificates, see Upload a Custom CA Certificate.

Option	Description
System Name	The name for the database credentials in Lieberman.

8. Click **Save**.

What to do next:

- Next, follow the steps to Add a Credential to a Scan.

Configure Tenable Security Center for Lieberman SSH

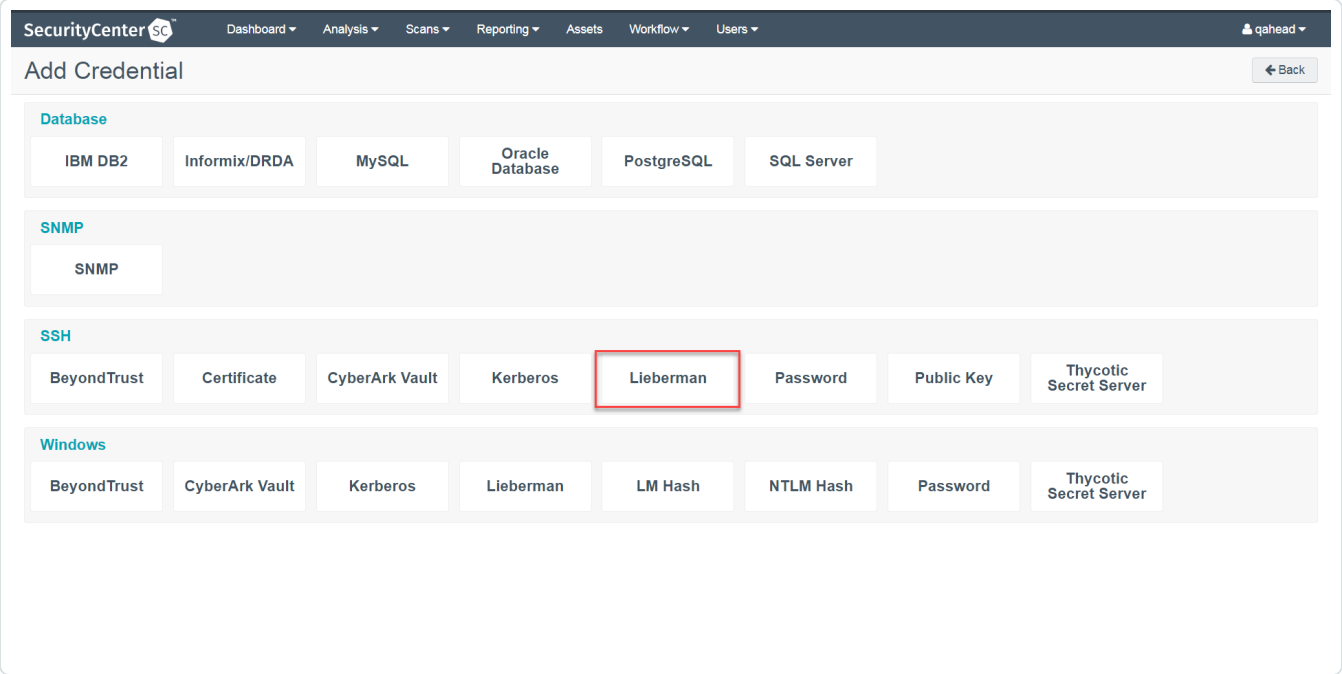
To configure a **SSH** credentialed network scan with Lieberman:

1. Log in to Tenable Security Center.
2. In the top navigation bar, click **Scanning**.

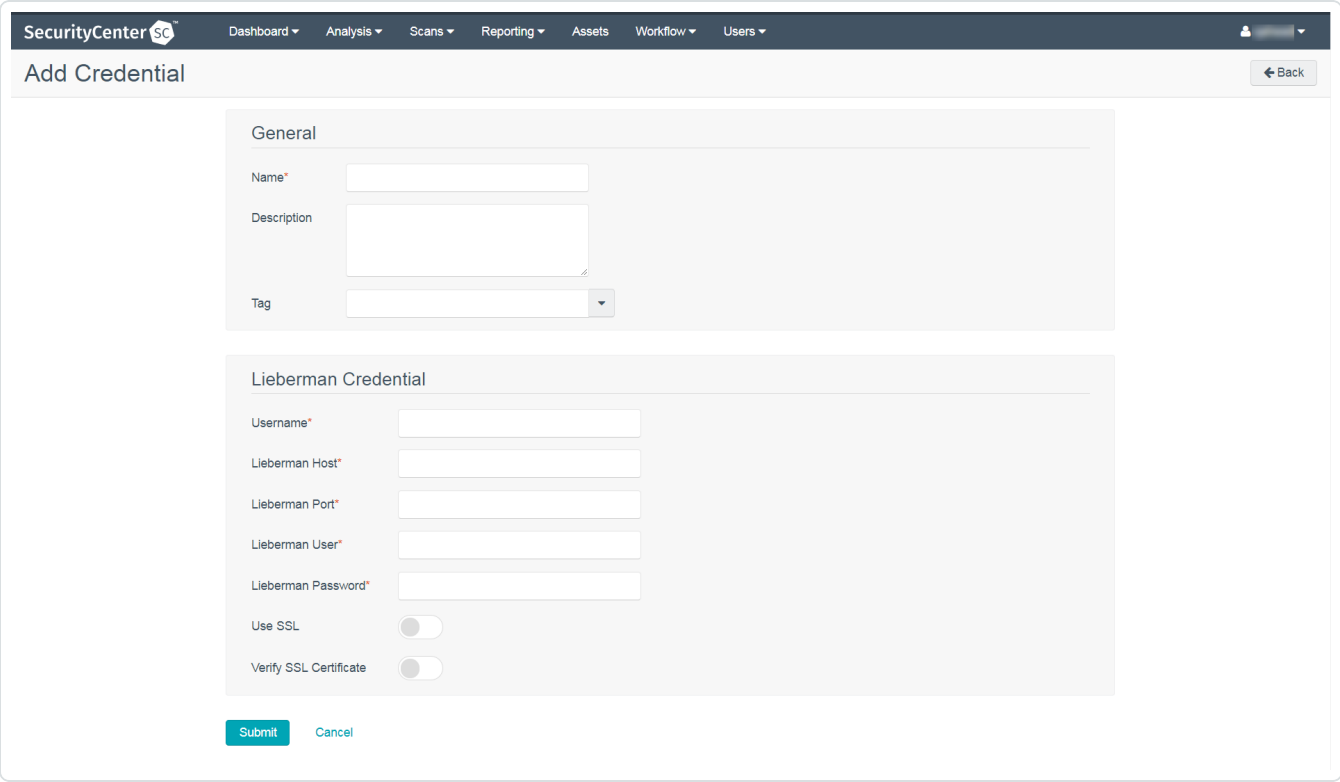
   A drop-down appears.
3. Click **Credentials**.

   The **Credentials** window opens.
4. In the upper-right corner, 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 **General** section enter:
    - (Required) In the **Name** box, enter a descriptive name.
    - (Optional) In the **Description** box, type a brief description.
    - (Optional) In the **Tag** box, select a tag in from the drop-down menu.
7. Configure each field for **SSH** authentication.

Option	Description
Username	The username for a user on the database.
Lieberman Host	The Lieberman IP address or 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`*.
Lieberman Port	The port Lieberman is listening on.

Option	Description
Lieberman User	The username for the Lieberman explicit user you want Tenable Security Center to use for authentication to the Lieberman Rapid Enterprise Defense (RED) API.
Lieberman Password	The password for the Lieberman explicit user.
Use SSL	When enabled, Tenable Security Center uses SSL through IIS for secure communications. You must configure SSL through IIS in Lieberman before enabling this option.
Verify SSL Certificate	When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL through IIS in Lieberman before enabling this option.
System Name	The name for the database credentials in Lieberman.

8. Click **Save**.

What to do next:

- Next, follow the steps to Add a Credential to a Scan.

Configure Tenable Security Center for Lieberman Database

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:

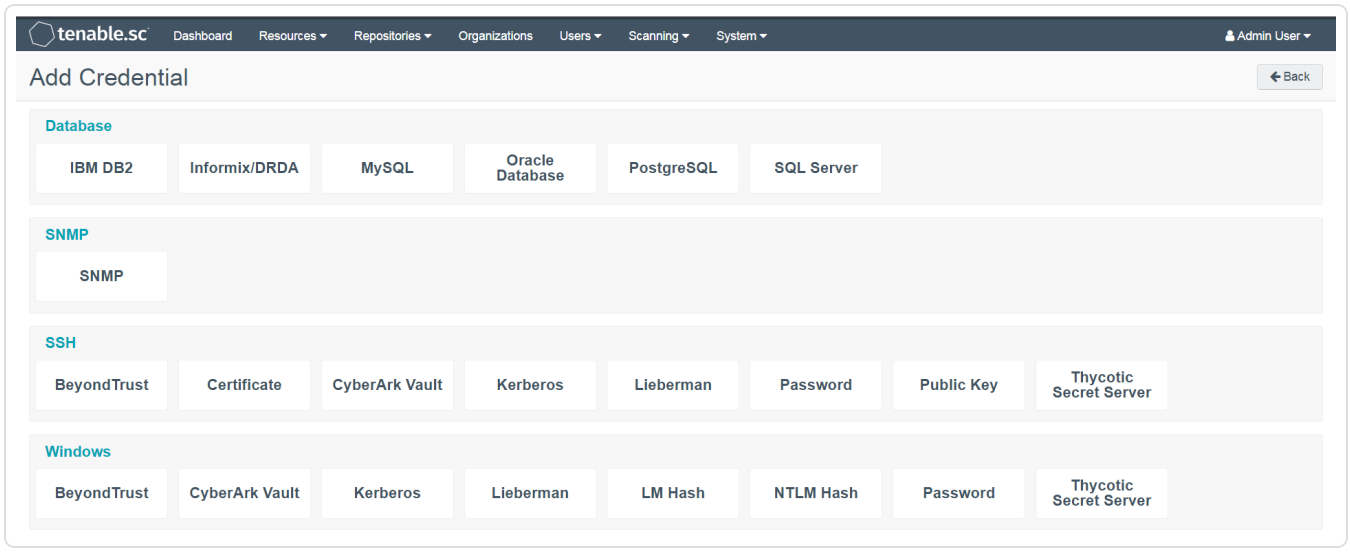
1. Log in to Tenable Security Center.
2. In the top navigation bar, click **Scanning**.

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

   The **Credentials** window opens.
4. In the upper-right corner, click the **+ Add** button.

   The **Add Credential** window opens.
5. In the **Database** section, click **Oracle Database**.

   The **Add Credential** page appears.



6. In the **Name** field, type a descriptive name.
7. (Optional) In the **Descriptionn** field, type a description.
8. (Optional) In the **Tag** drop-down, select a tag.

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

   The **Lieberman** options appear.

10. Configure each option for the **Oracle Database** authentication.

Option	Database Types	Description
Username	All	The username for a user on the database.
Port	All	The port the database is listening on.
Database Name	IBM DB2 PostgreSQL	The name for your database instance.
Authentication	Oracle Database SQL Server	The type of account you want Tenable Security Center to use to access the database instance.
Service Type	Oracle Database	The Oracle parameter you want to use to identify the database instance: **SID** or **Service Name**.
Service	Oracle Database	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.
Instance Name	SQL Server	The name for your database instance.
Lieberman Host	All	The Lieberman IP address or DNS address.
Lieberman Port	All	The port Lieberman is listening on.
Lieberman User	All	The username for the Lieberman explicit user you want Tenable Security Center to use for authentication to the Lieberman Rapid Enterprise Defense (RED) API.
Lieberman Pass-	All	The password for the Lieberman explicit user.

Option	Database Types	Description
word		
Use SSL	All	When enabled, Tenable Security Center uses SSL through IIS for secure communications. You must configure SSL through IIS in Lieberman before enabling this option.
Verify SSL Certificate	All	When enabled, Tenable Security Center validates the SSL certificate. You must configure SSL through IIS in Lieberman before enabling this option.
System Name	All	The name for the database credentials in Lieberman.

11. Click **Submit**.

What to do next:

- Next, follow the steps to Add a Credential to a Scan.

Enable Database Plugins in Tenable Security Center

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. Log in to Tenable Security Center.
2. In the top navigation bar, click **Scanning**.

   A drop-down appears.
3. Select **Active Scans**.

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

   The **Add Active Scan** window appears.
5. In the left column, click **Credentials**.

   The **Scan Credentials** section appears.
6. In the **Scan Credentials** section, click **+Add Credential**.

   A drop-down appears.
7. Select the system type.

   The **Select Credential** option appears.
8. Click **Select Credential**.

   A drop-down appears.
9. Select the previously created credential.
10. Enter information for the **General**, **Settings**, **Targets**, and **Post Scan** sections.
11. Click **Submit**.

Allow Shared Accounts

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

Before you begin:

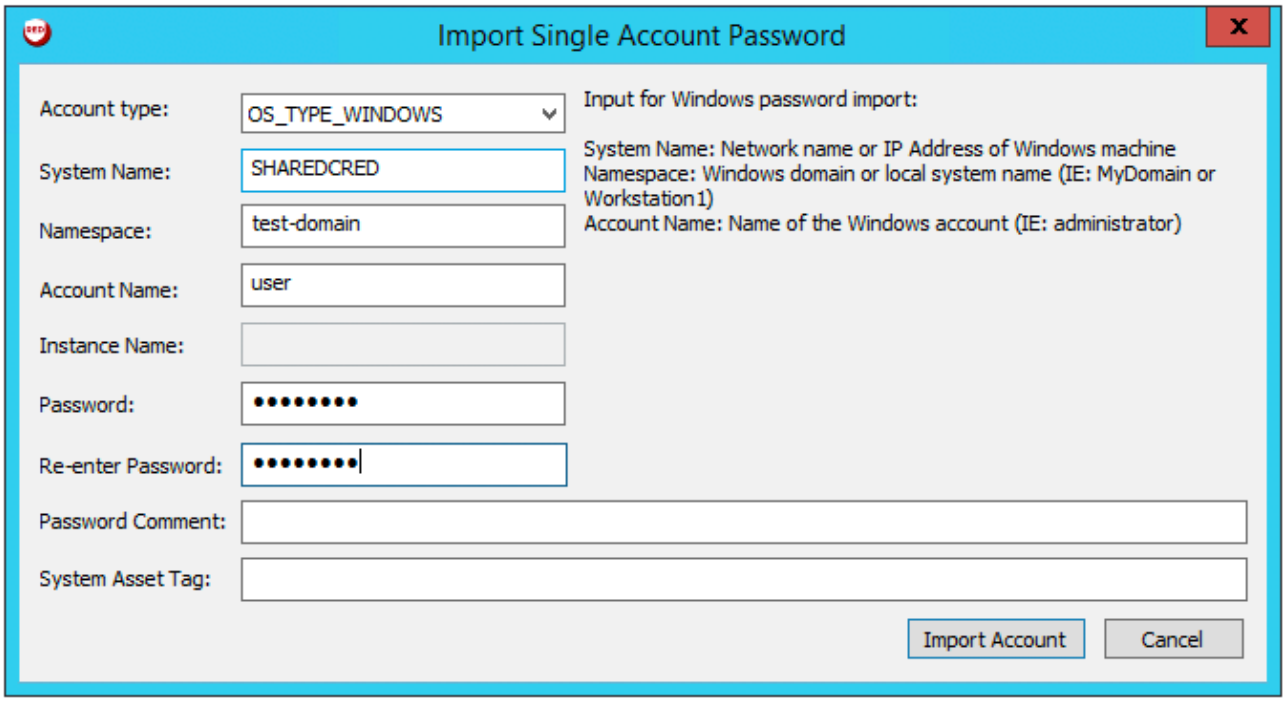
You must have the following permissions selected in Lieberman:

- 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

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.