How-to Guide: Tenable.io™ for Lieberman

Last Revised: November 16, 2018

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

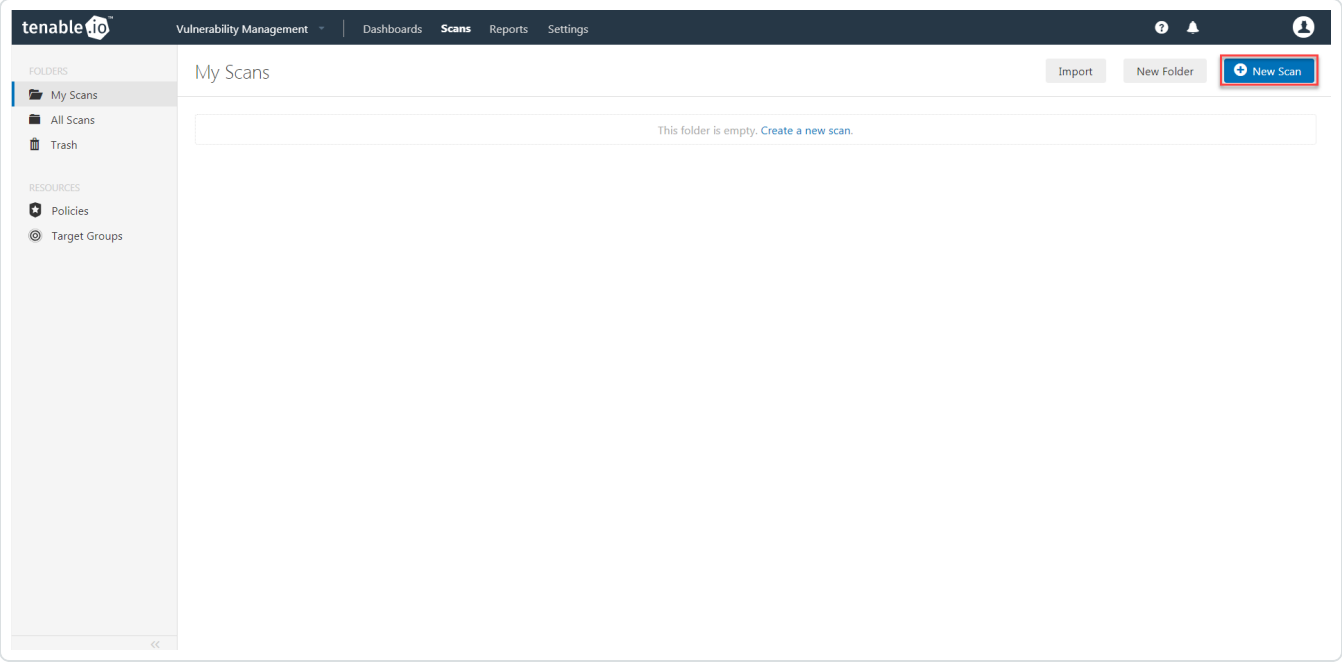
Windows Integration

Before you begin:

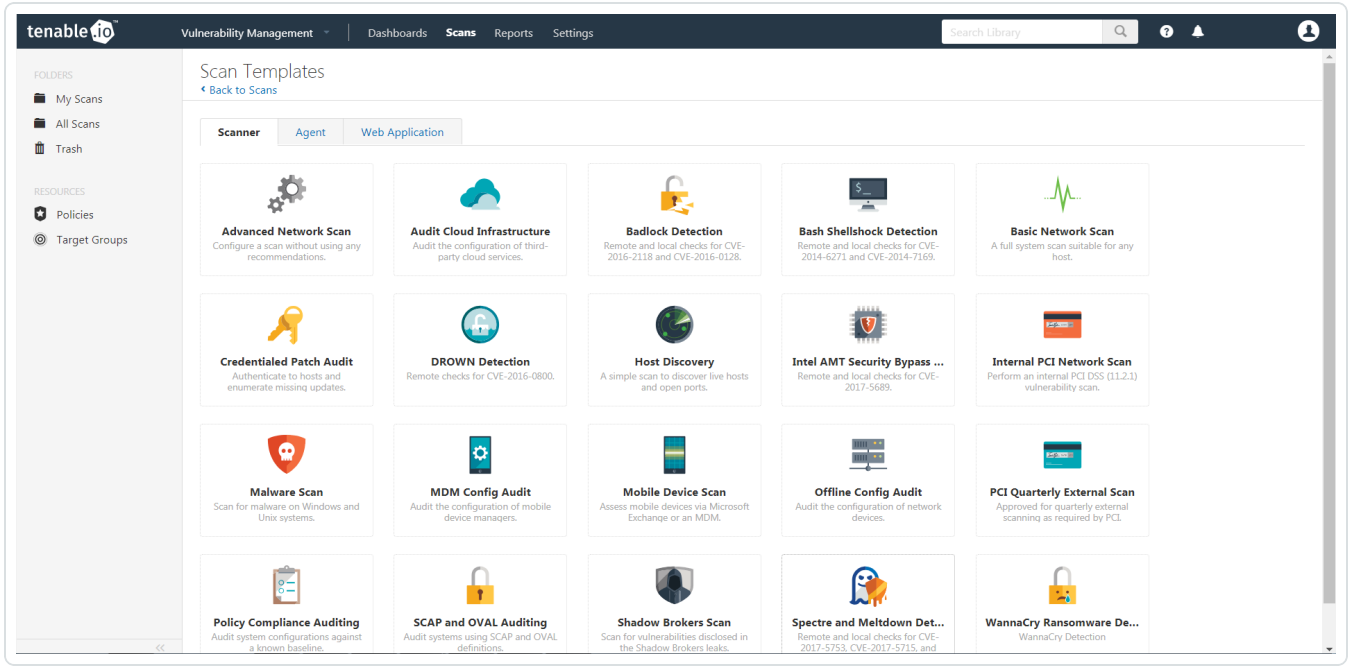
Caution: You must create an **Explicit Account** under *Delegation* > *Delegation Identities* in Lieberman. For additional information on how to create an Explicit Account, see the Explicit Accounts section in the Lieberman RED Identity Management Administrator's Guide.

To integrate with Windows:

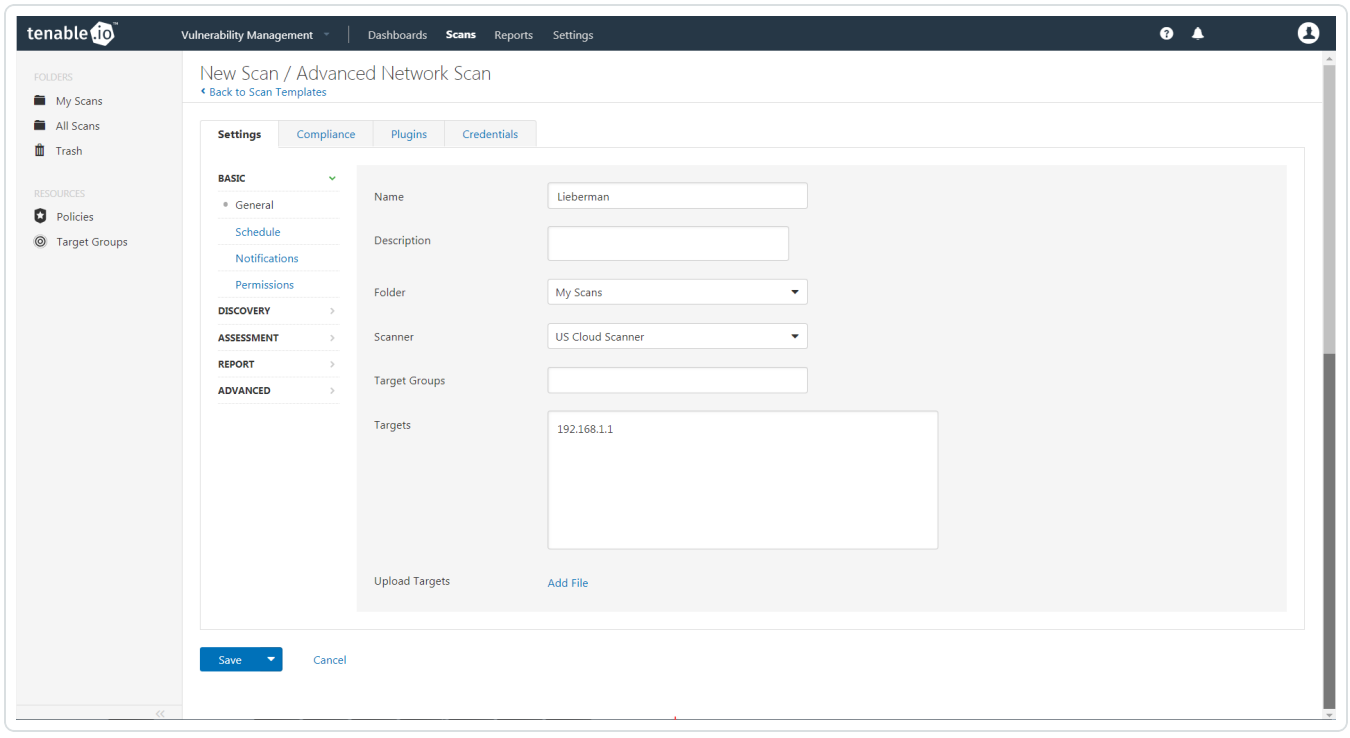
1. In a browser, log in to Tenable.io.
2. Navigate to the **Scans** section.
3. Click the **+ New Scan** button to configure Tenable.io for credentialed scans of Windows systems using Lieberman's password management solution.



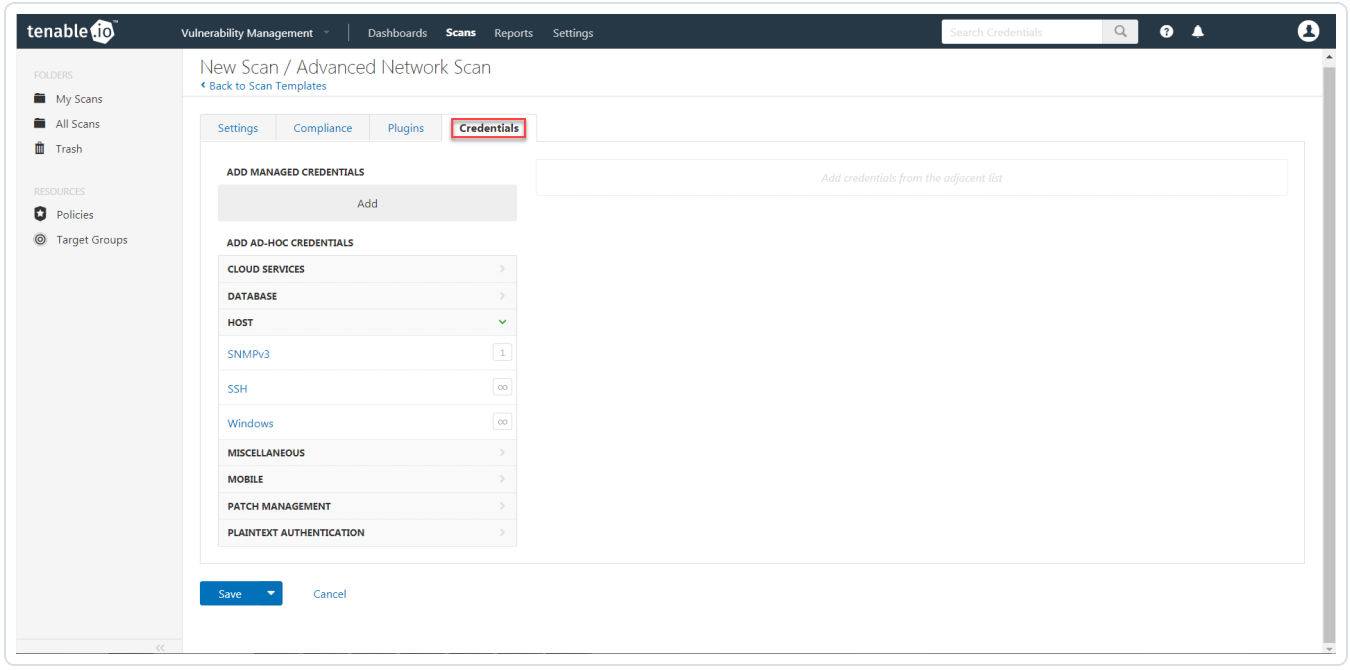
4. Select a **Scan Template** for the scan type required for your scan. For demonstration purposes, the **Advanced Network Scan** template is used.



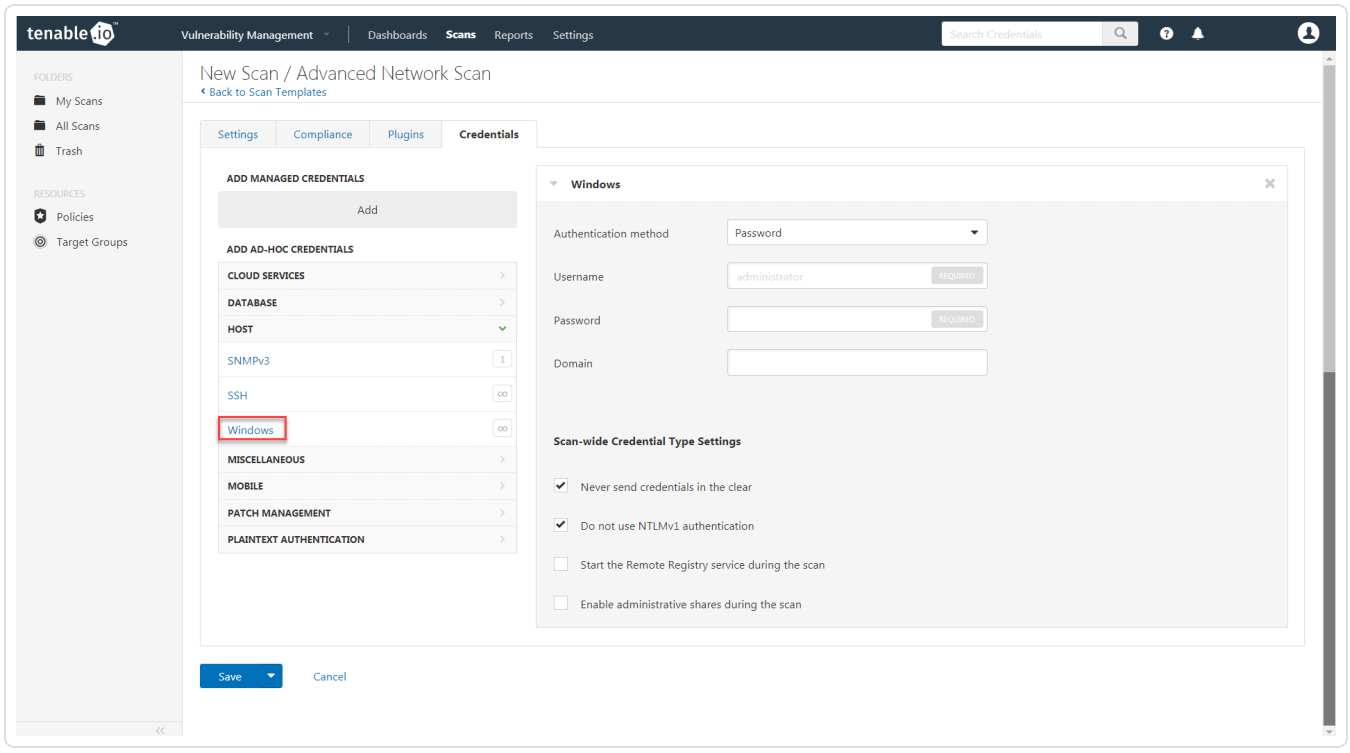
5. Enter a descriptive **Name** and the IP address(es) or hostname(s) of the scan **Targets**.



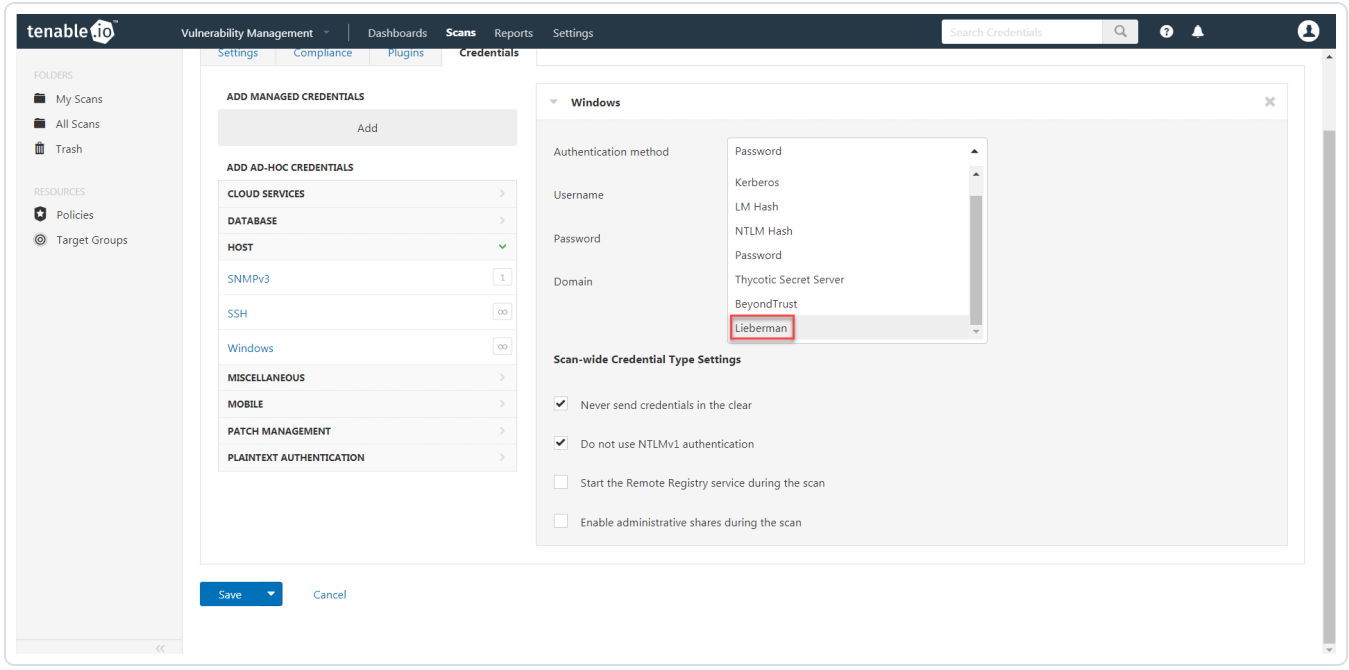
6. Click on the **Credentials** tab.



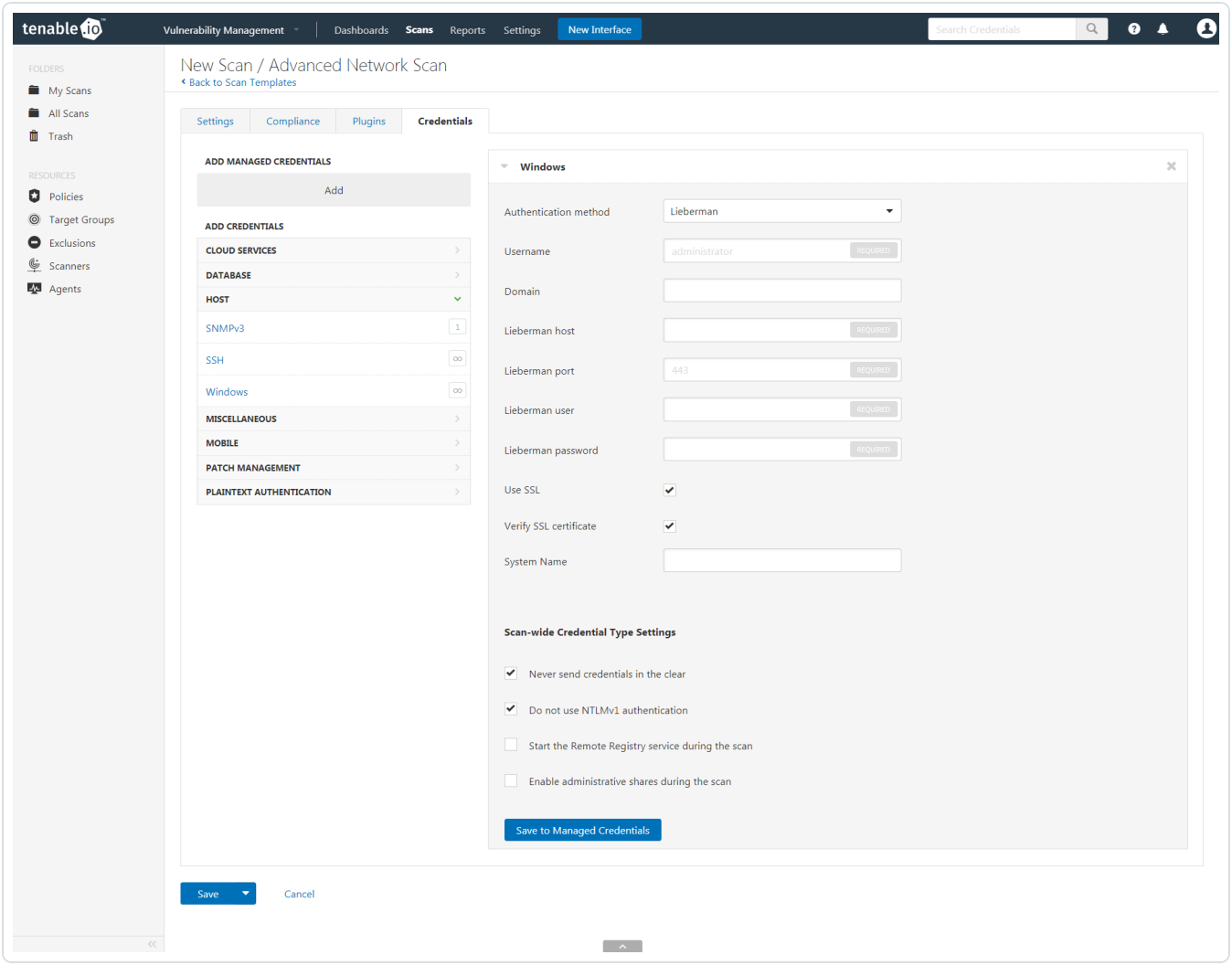
7. In the left-hand menu, select **Windows**.



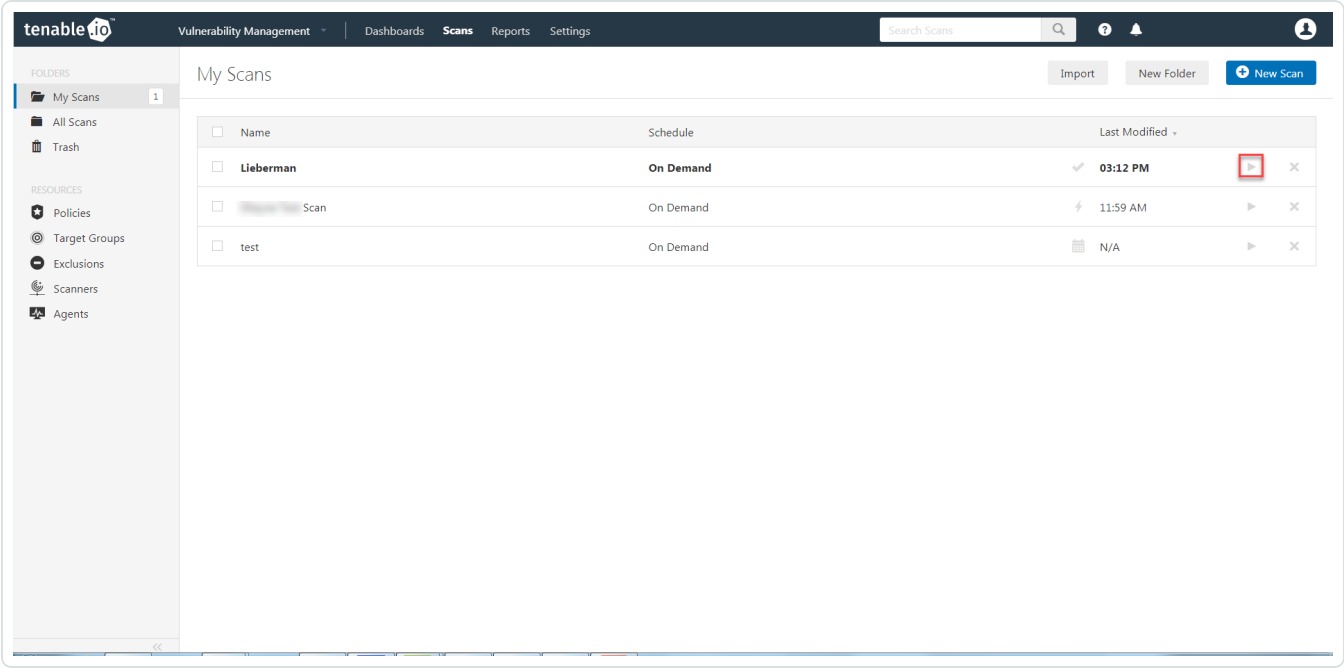
8. From the **Authentication method** drop-down, select **Lieberman**.



9. Configure each field for Windows authentication. See the Tenable.io User Guide to get detailed descriptions for each option.



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.

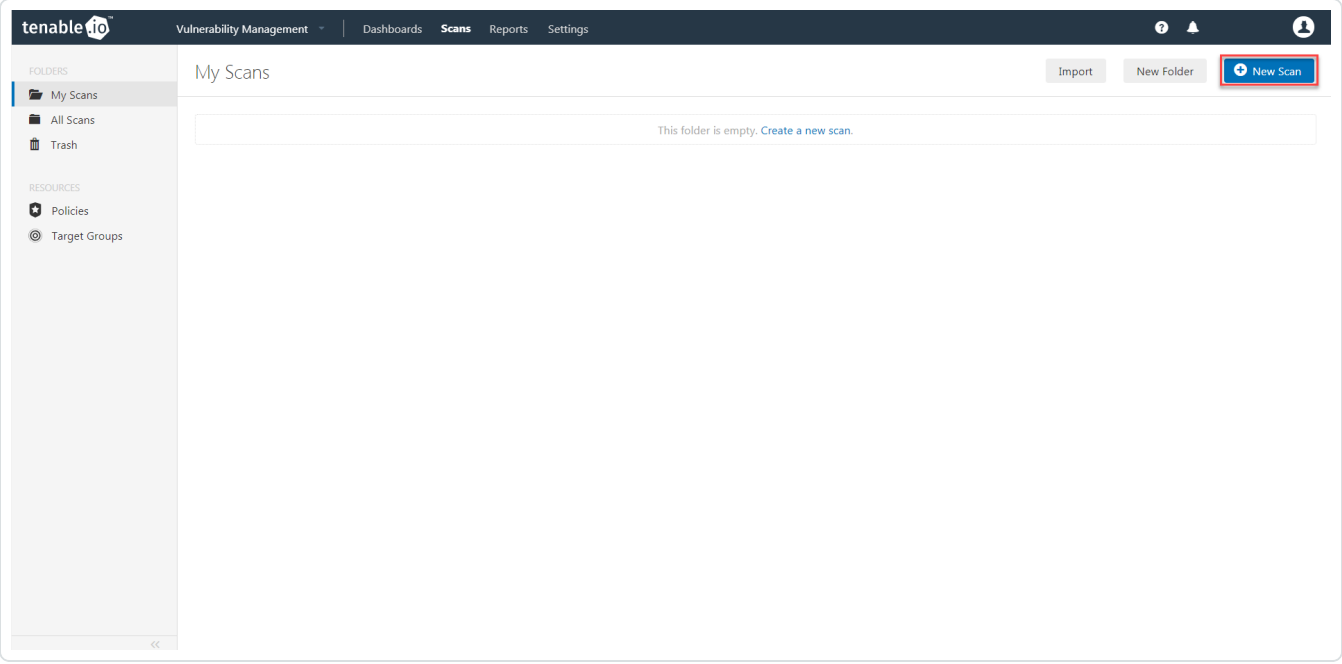
SSH Integration

Before you begin:

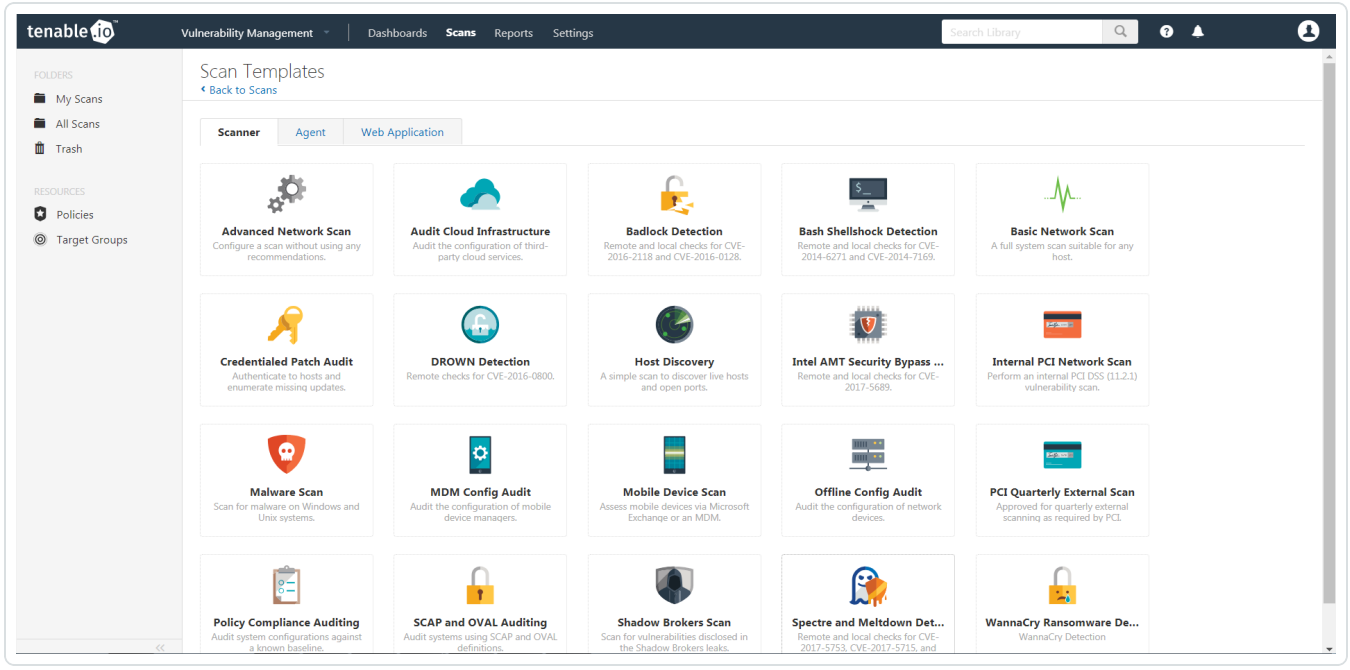
Caution: You must create an **Explicit Account** under *Delegation* > *Delegation Identities* in Lieberman. For additional information on how to create an Explicit Account, see the Explicit Accounts section in the Lieberman RED Identity Management Administrator's Guide.

To integrate with SSH:

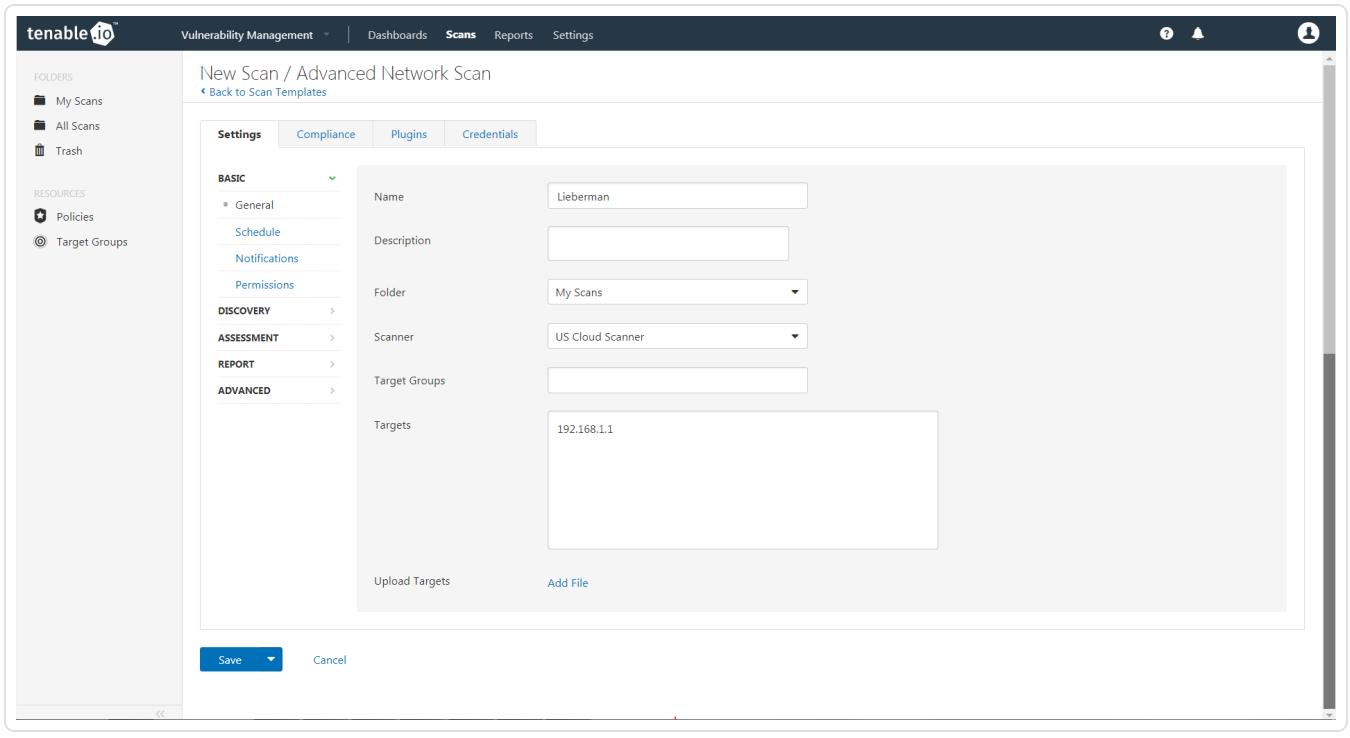
1. In a browser, log in to Tenable.io.
2. Navigate to the **Scans** section.
3. Click the **+ New Scan** button to configure Tenable.io for credentialed scans of Windows systems using Lieberman's password management solution.



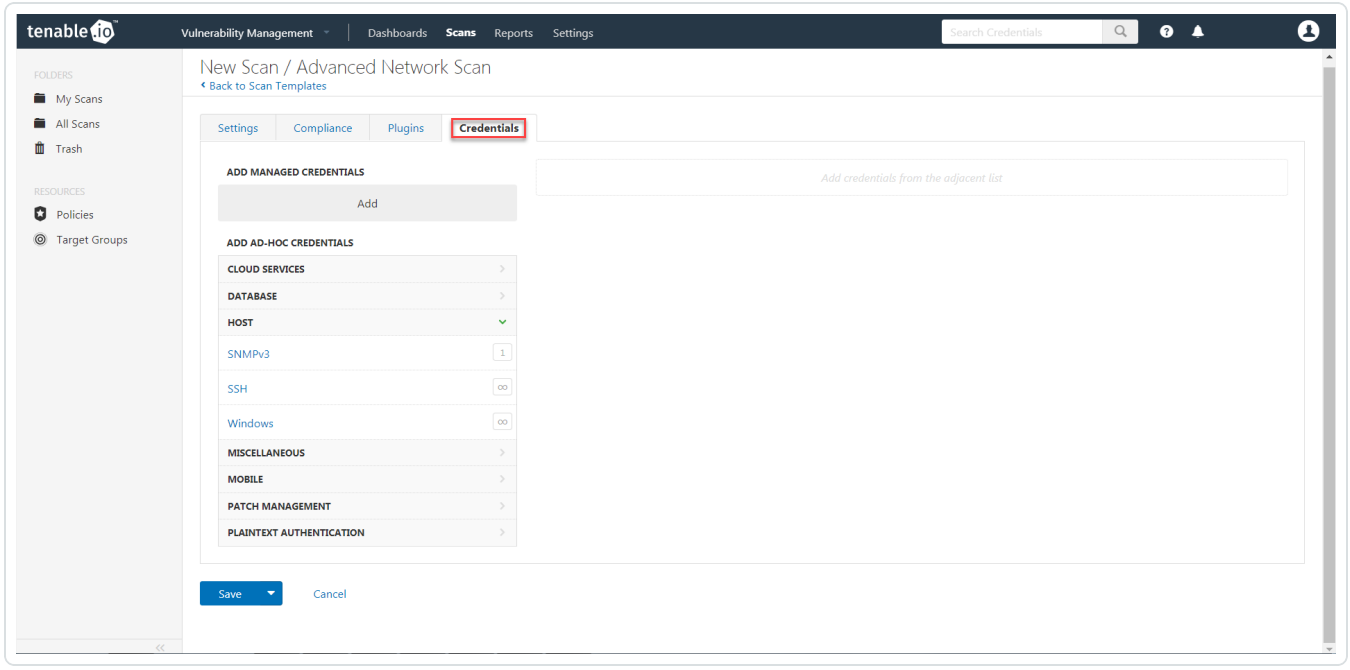
4. Select a **Scan Template** for the scan type required for your scan. For demonstration purposes, the **Advanced Network Scan** template is used.



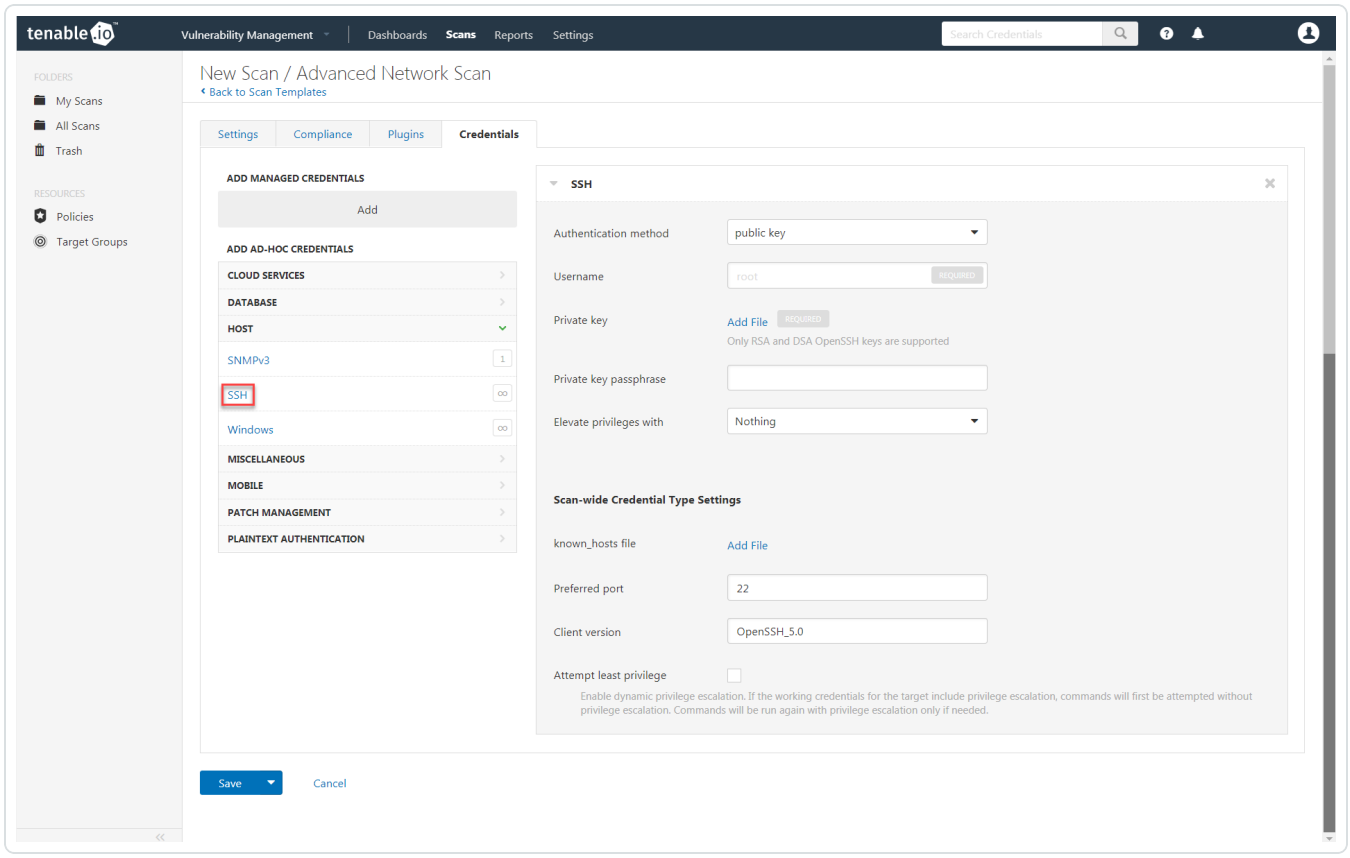
5. Enter a descriptive **Name** and the IP address(es) or hostname(s) of the scan **Targets**.



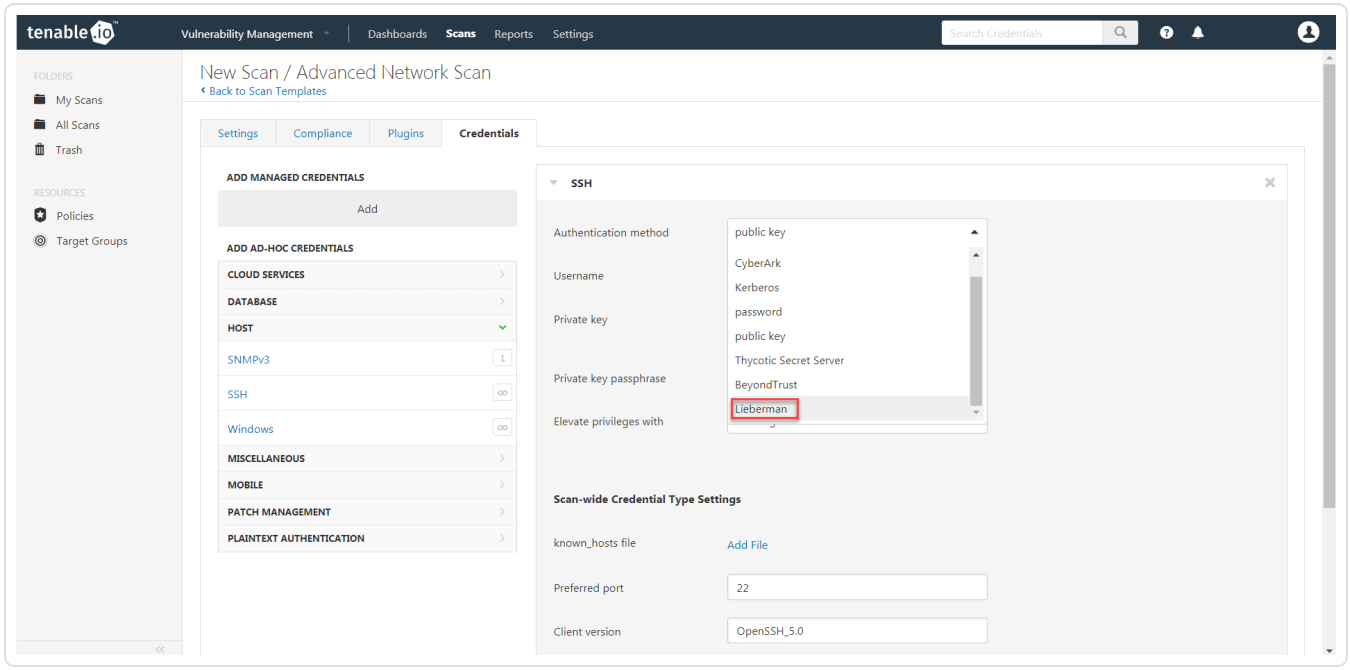
6. Click on the **Credentials** tab.



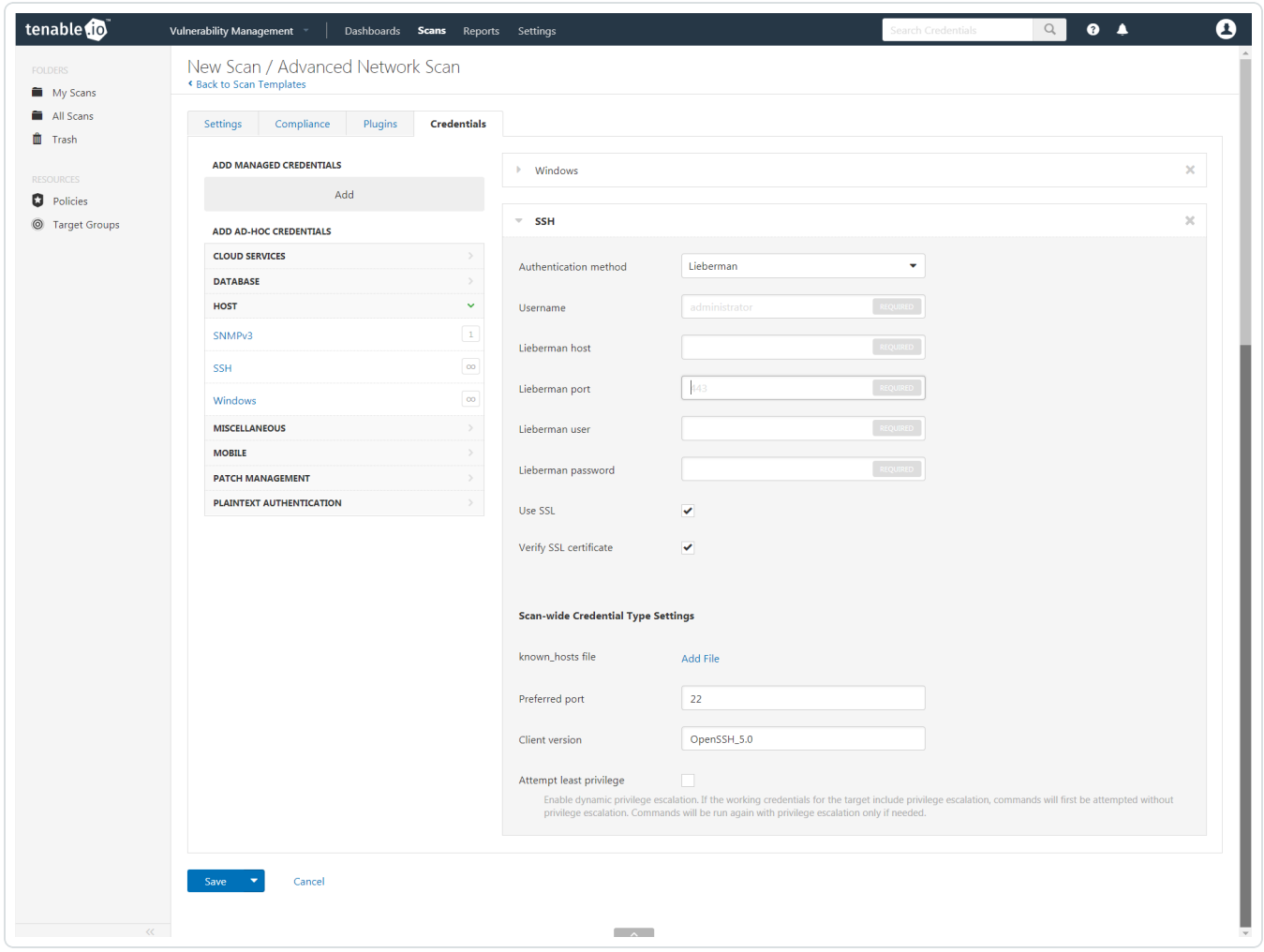
7. In the left-hand menu, select **SSH**.



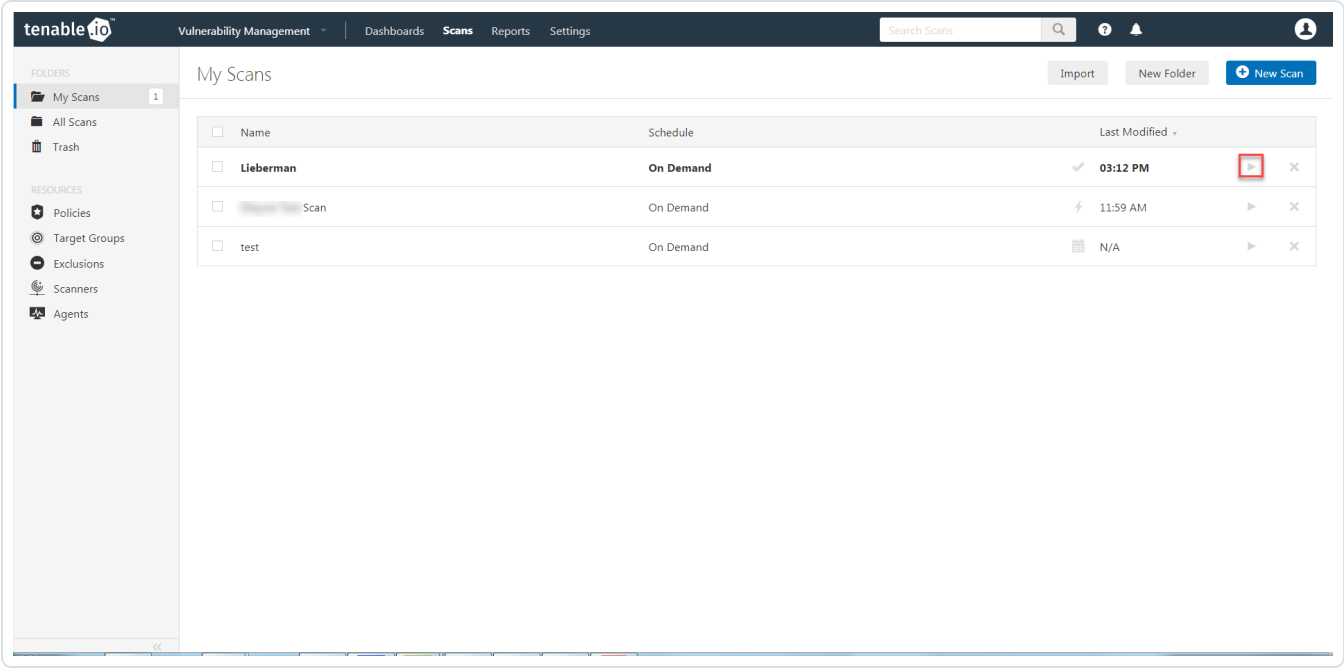
8. From the **Authentication method** drop-down, select **Lieberman**.



9. Configure each field for SSH authentication. See the Tenable.io User Guide to get detailed descriptions for each option.



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

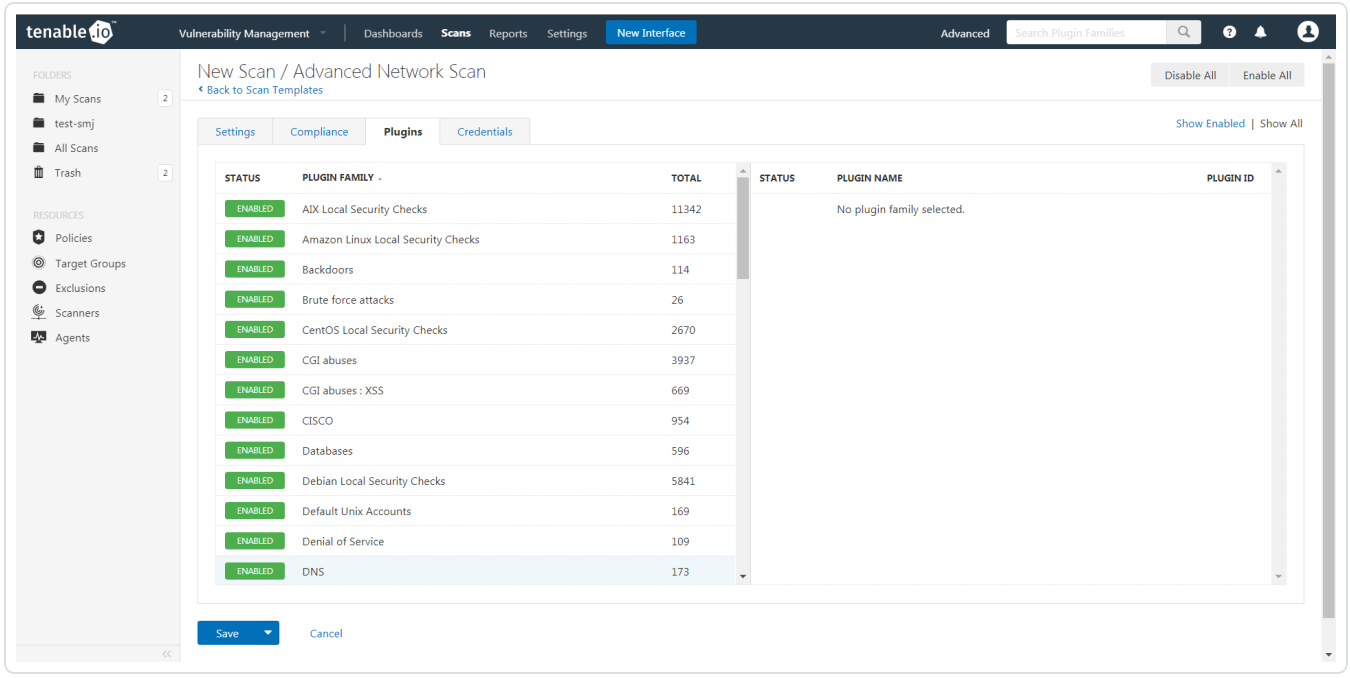


12. Once the scan has completed, select the completed scan and look for **Plugin ID 97993** and the corresponding message - *It was possible to log into the remote host via SSH using 'password' authentication*. This validates that authentication was successful.

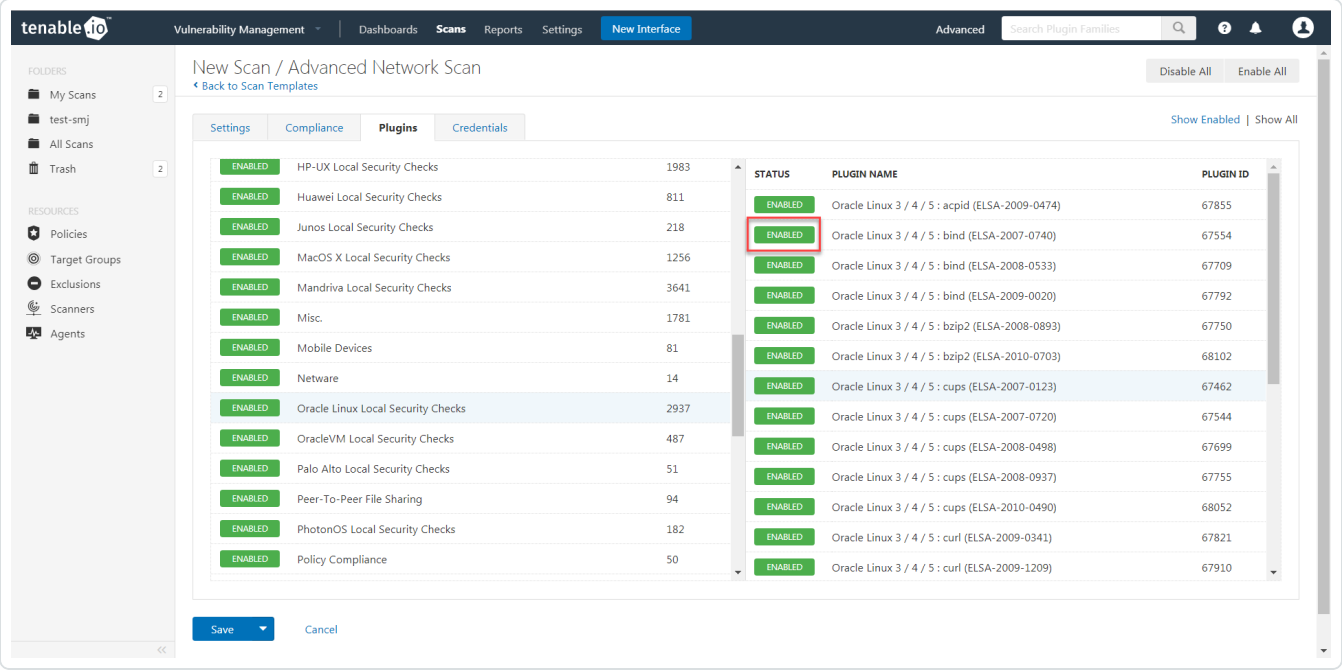
Database Integration

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

1. Go to the **Plugins** tab on the scan configurations page.



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



3. Click **Save**.

Note: 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://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.