



## How-to Guide: Tenable Nessus for Lieberman RED

---

Last Revised: May 18, 2018

---

# Table of Contents

<b>Introduction</b> .....	<b>3</b>
<b>Integrations</b> .....	<b>4</b>
Windows Integration .....	5
SSH Integration .....	11
Database Integration .....	17
<b>Additional Information</b> .....	<b>19</b>
Lieberman RED System .....	20
About Tenable .....	21

---

# Introduction

---

This document describes how to configure Tenable Nessus for integration with Lieberman RED Identity Management system. Please email any comments and suggestions to [support@tenable.com](mailto:support@tenable.com).

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 the Lieberman RED with Tenable's solutions, customers are now granted even more options and flexibility for reducing the credentials headache.

Benefits of integrating Tenable Nessus with Lieberman RED include:

- Credentials stored in Lieberman RED do not need to be managed and updated directly within Tenable Nessus.
- Reduce the time and effort needed to document where credentials are stored within the entire organizational environment.
- Automatically enforce security policies within specific departments or for specific business unit requirements, which simplifies compliance.
- Reduce the risk of unsecured privileged accounts and credentials across the enterprise.

---

# Integrations

---

The Lieberman RED Identity Management system can be configured using either Windows or SSH. Click the corresponding link to view the configuration steps.

[Windows Integration](#)

[SSH Integration](#)

[Database Integration](#)

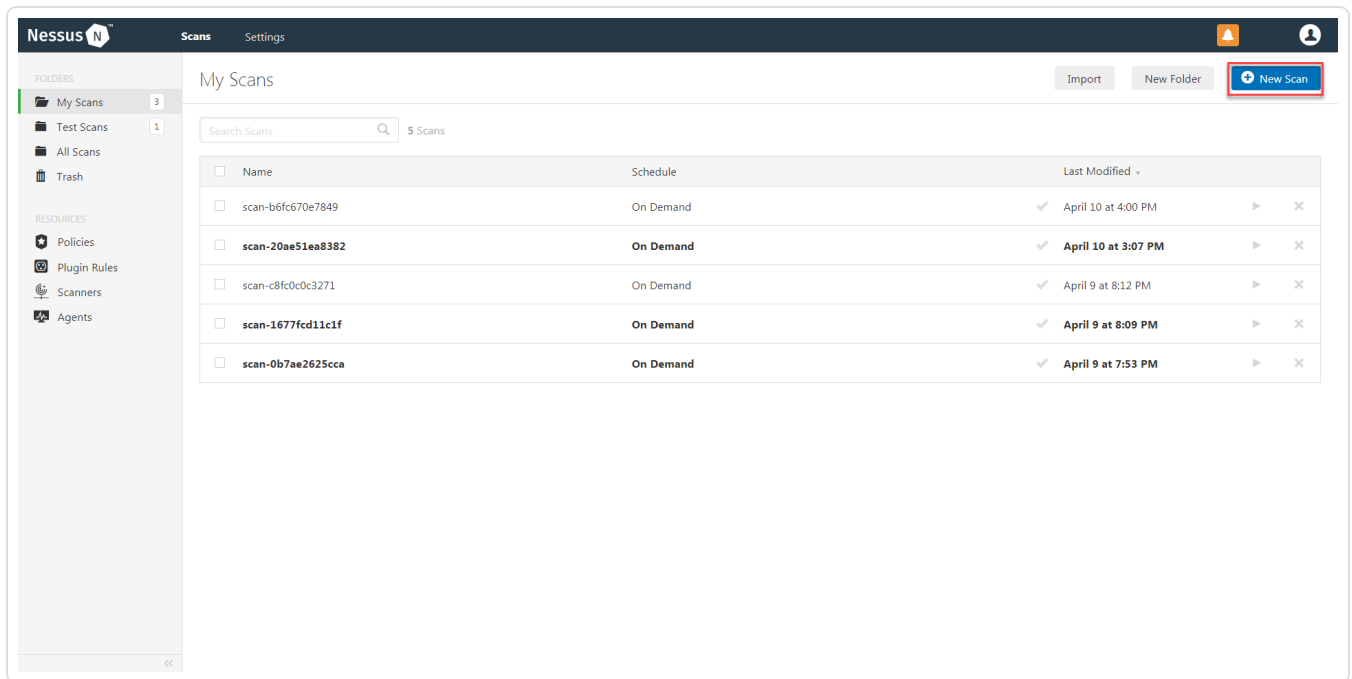
# Windows Integration

## Before you begin:

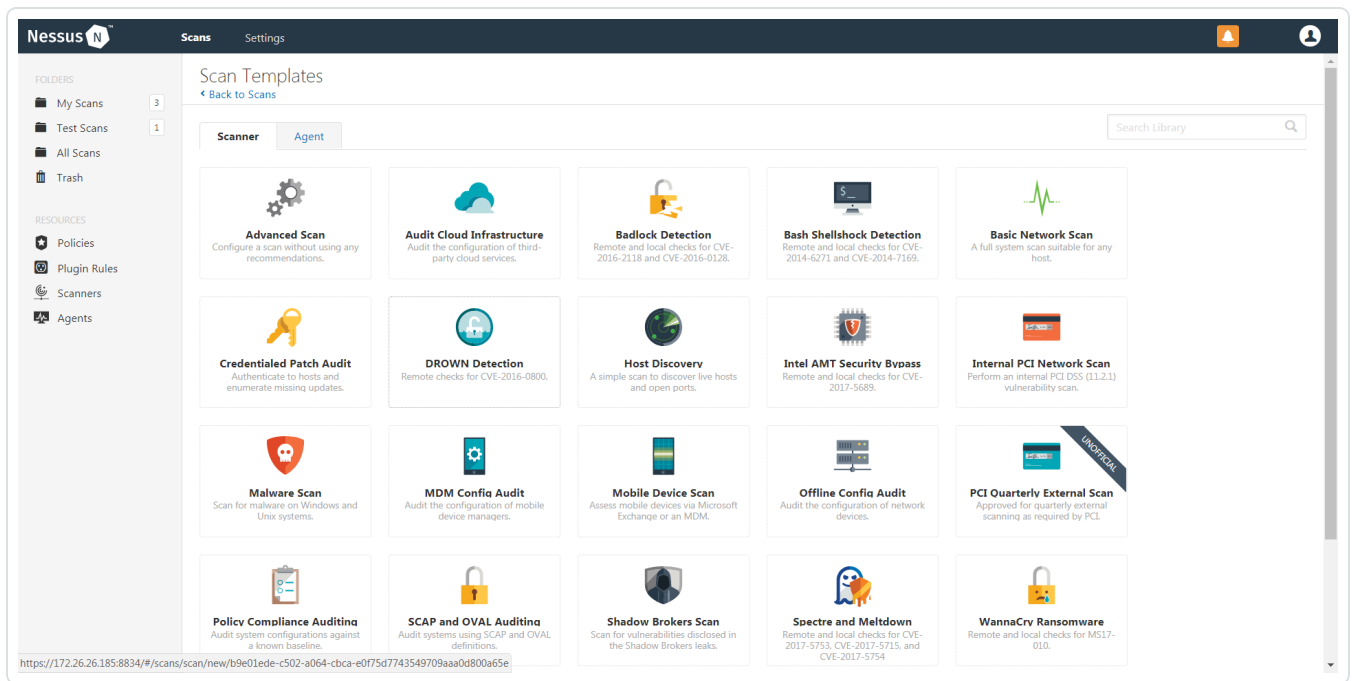
- You must create an **Explicit Account** under *Delegation > Delegation Identities* in Lieberman.

## To integrate with Windows:

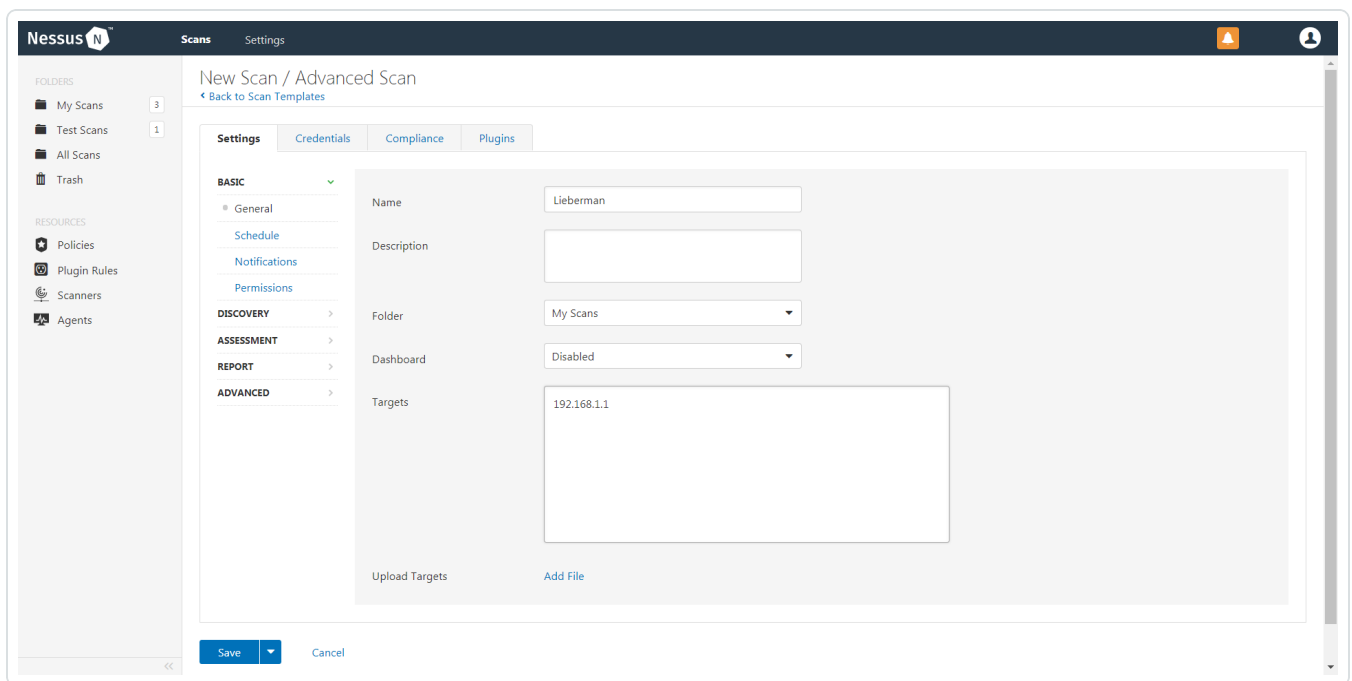
- In a browser, log in to Nessus.
- Navigate to the **Scans** section.
- Click the **+ New Scan** button to configure Nessus for credentialed scans of Windows systems using Lieberman's password management solution.



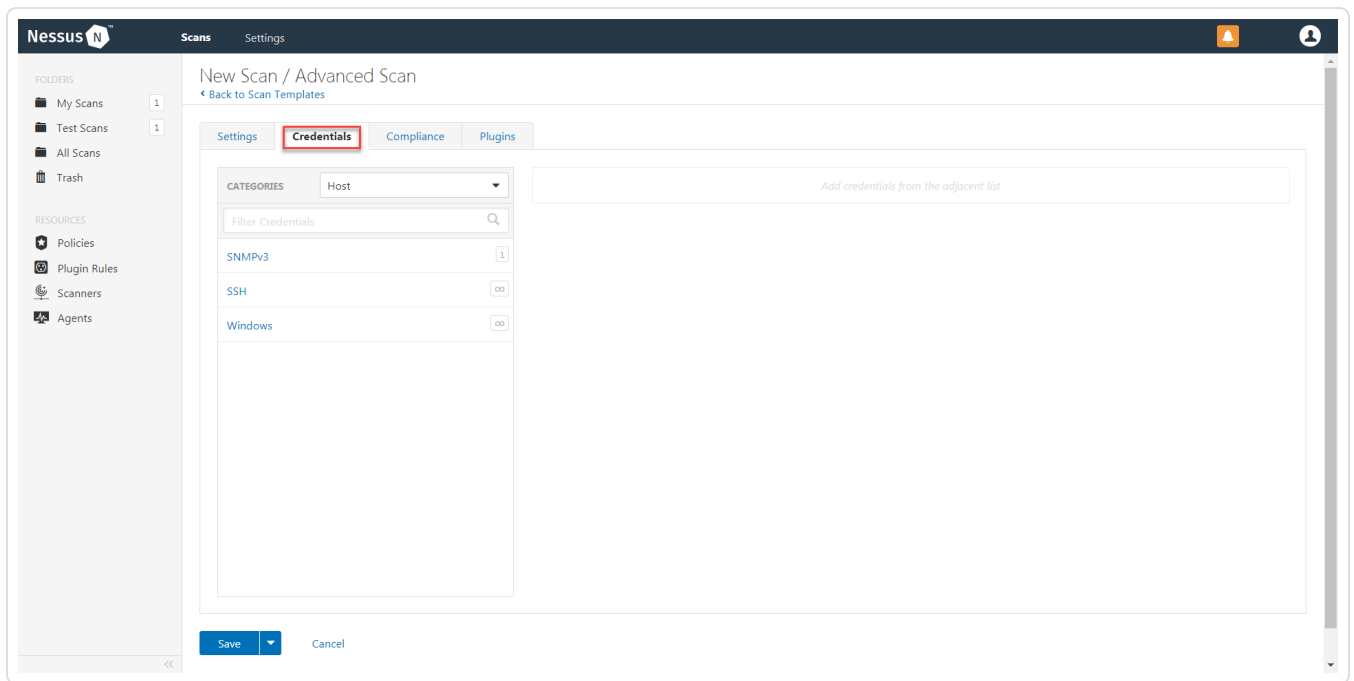
- Select a **Scan Template** for the scan type required for your scan. For demonstration purposes, the **Advanced Network Scan** template is used.



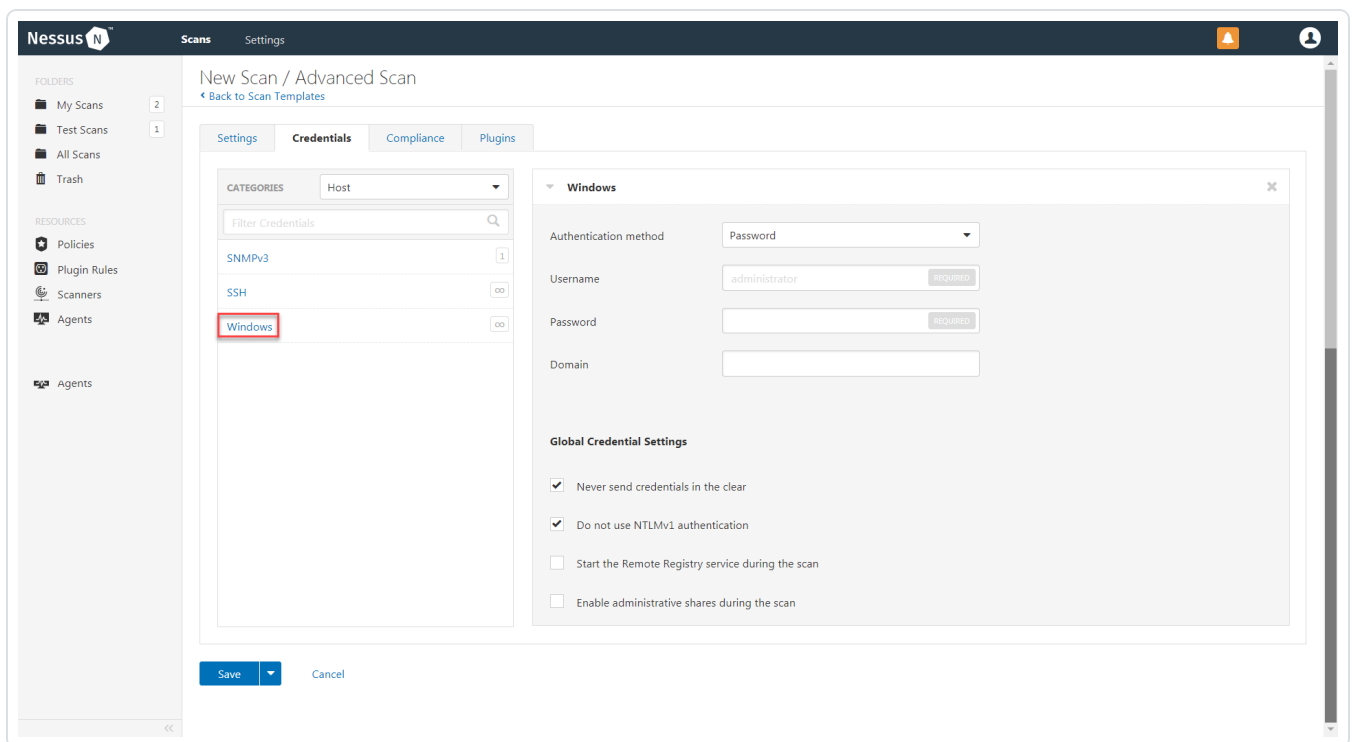
5. Enter a descriptive **Name** and the IP address(es) or hostname(s) of the scan **Targets**.



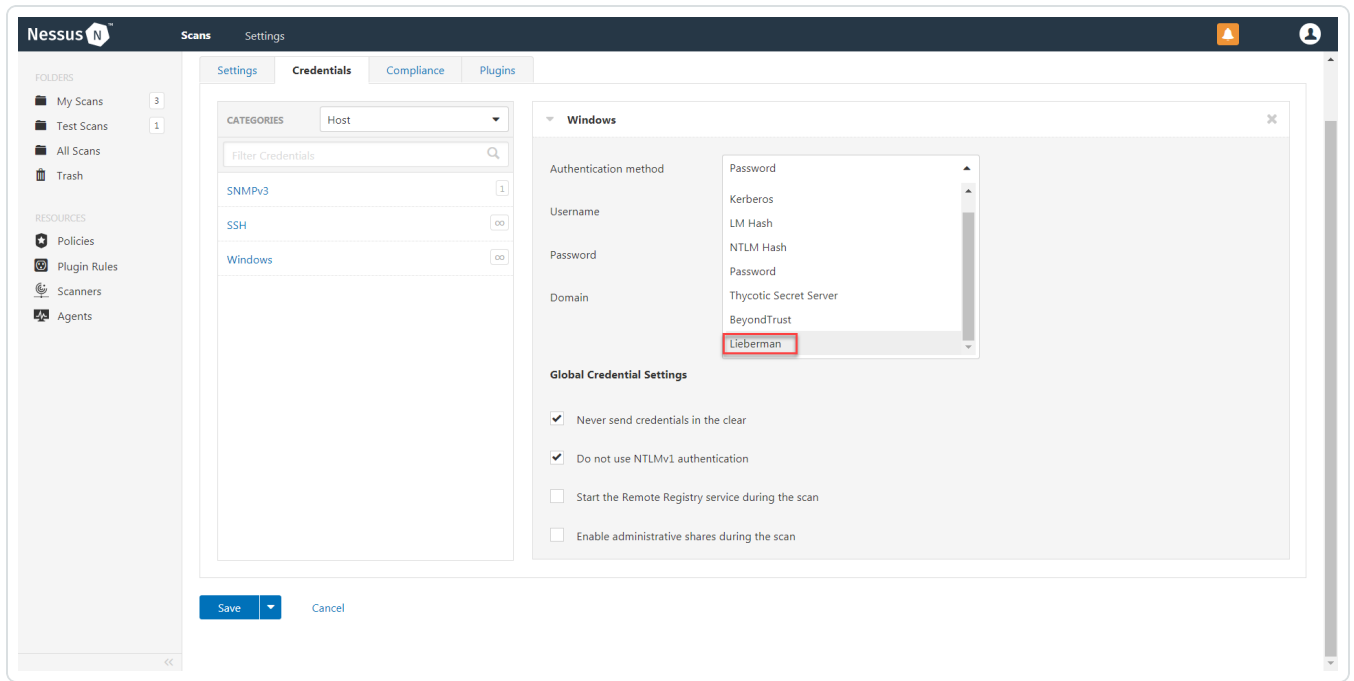
6. Click on the **Credentials** tab.



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

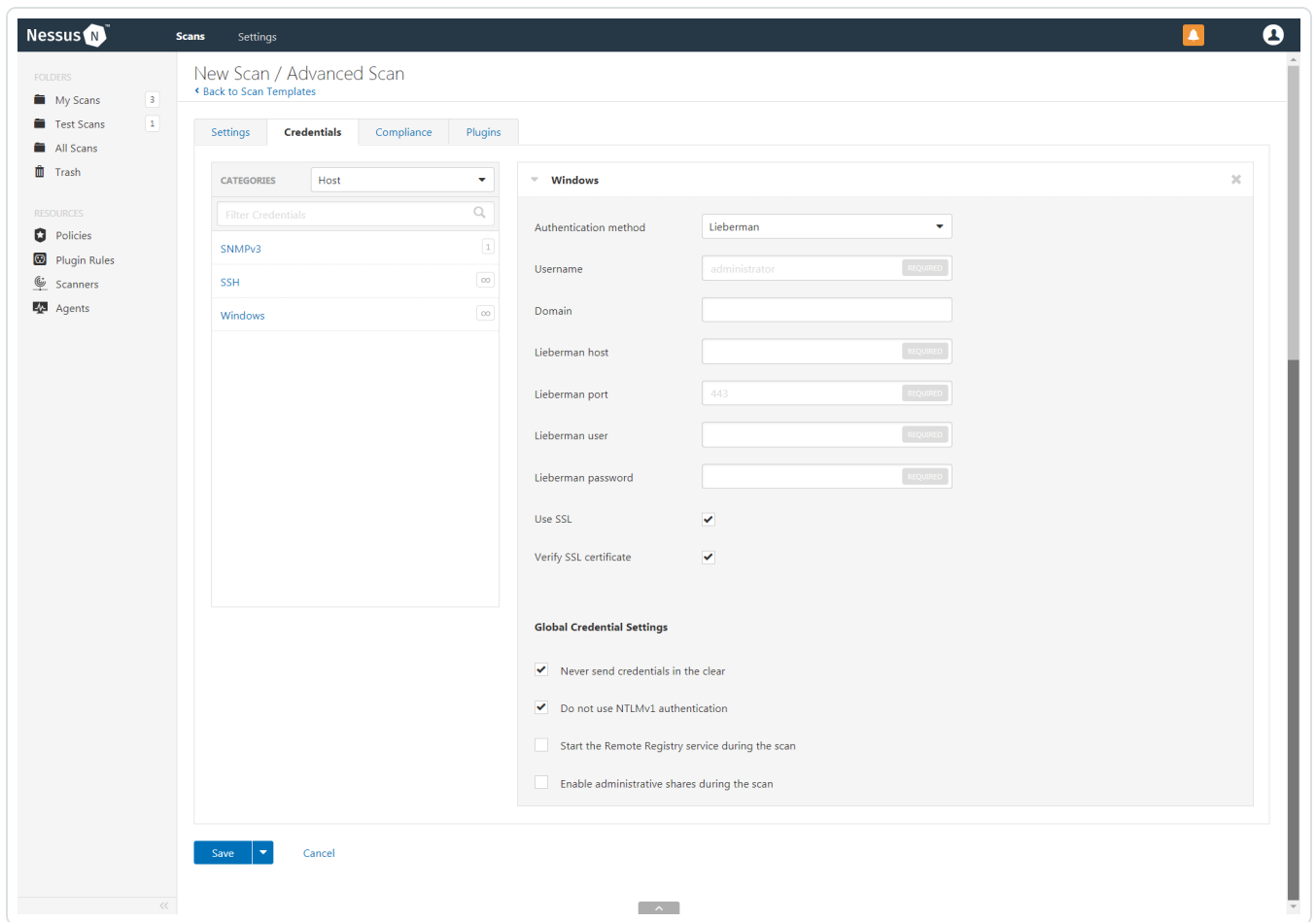


8. From the **Authentication method** drop-down, select **Lieberman**.



9. Configure each field for Windows authentication. Refer to the table below for a description of each field.





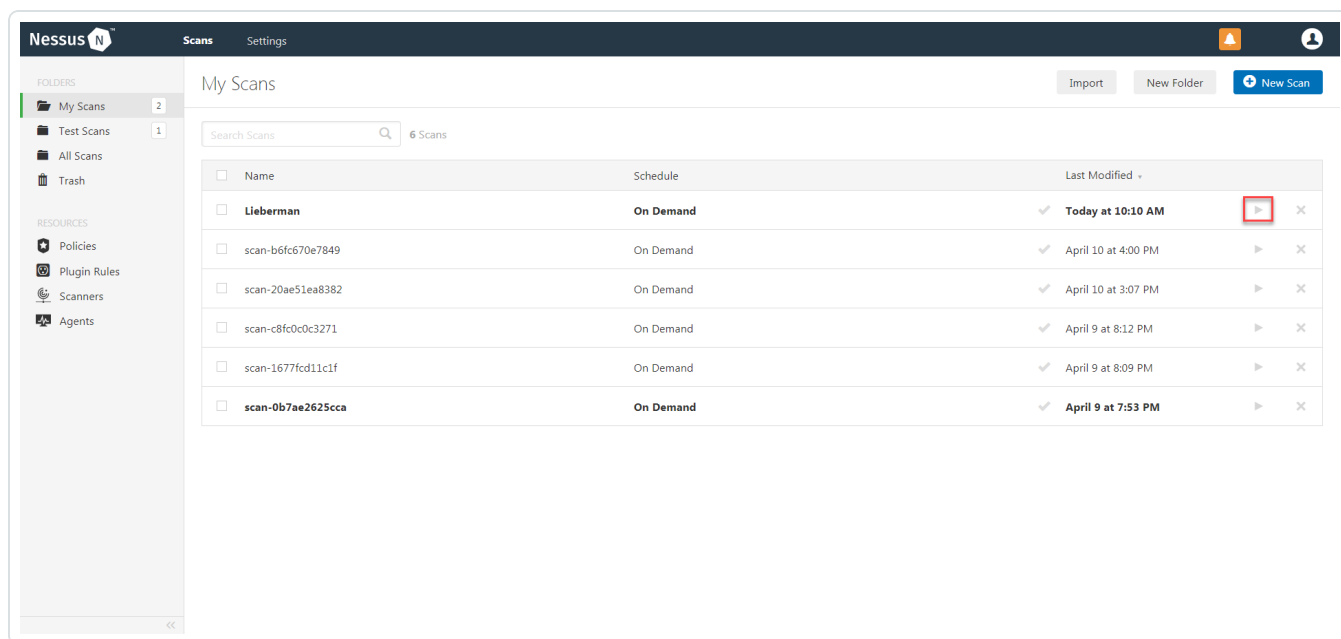
The table below contains a description of each option:

Option	Description
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.
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.
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.

10. Once the options to reach Lieberman are set, 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.

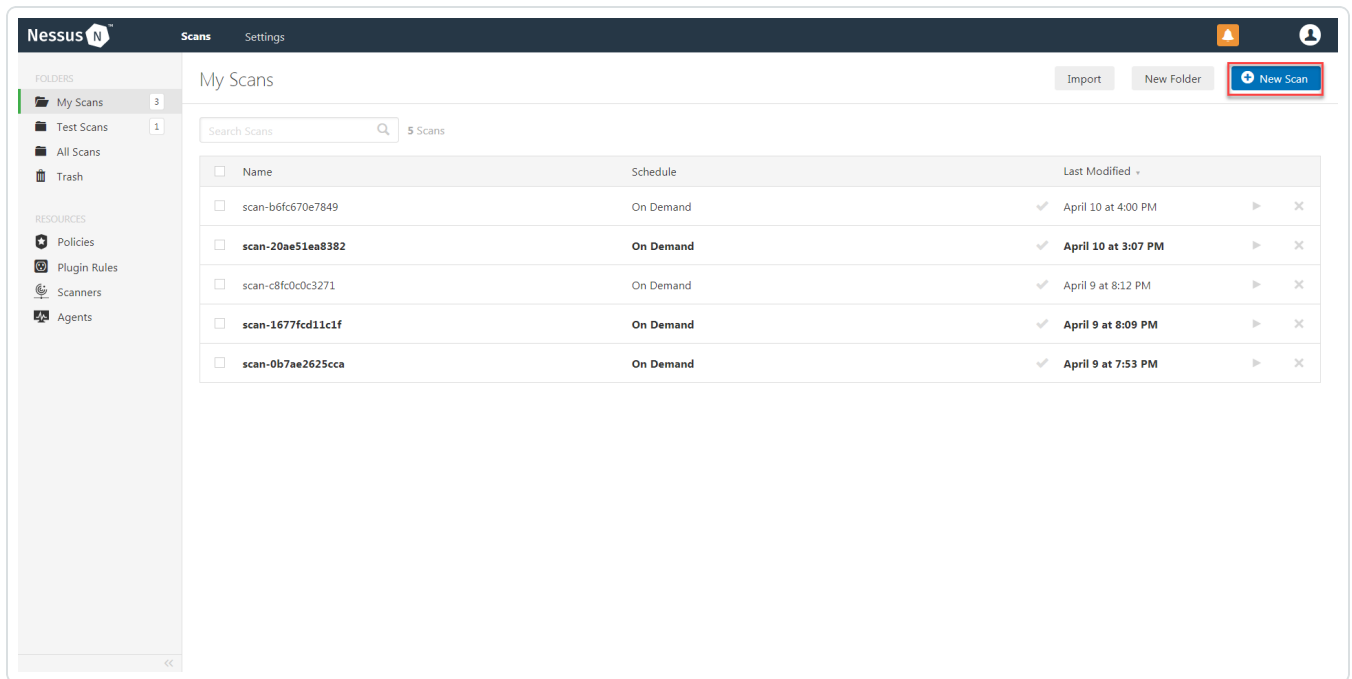
# SSH Integration

## Before you begin:

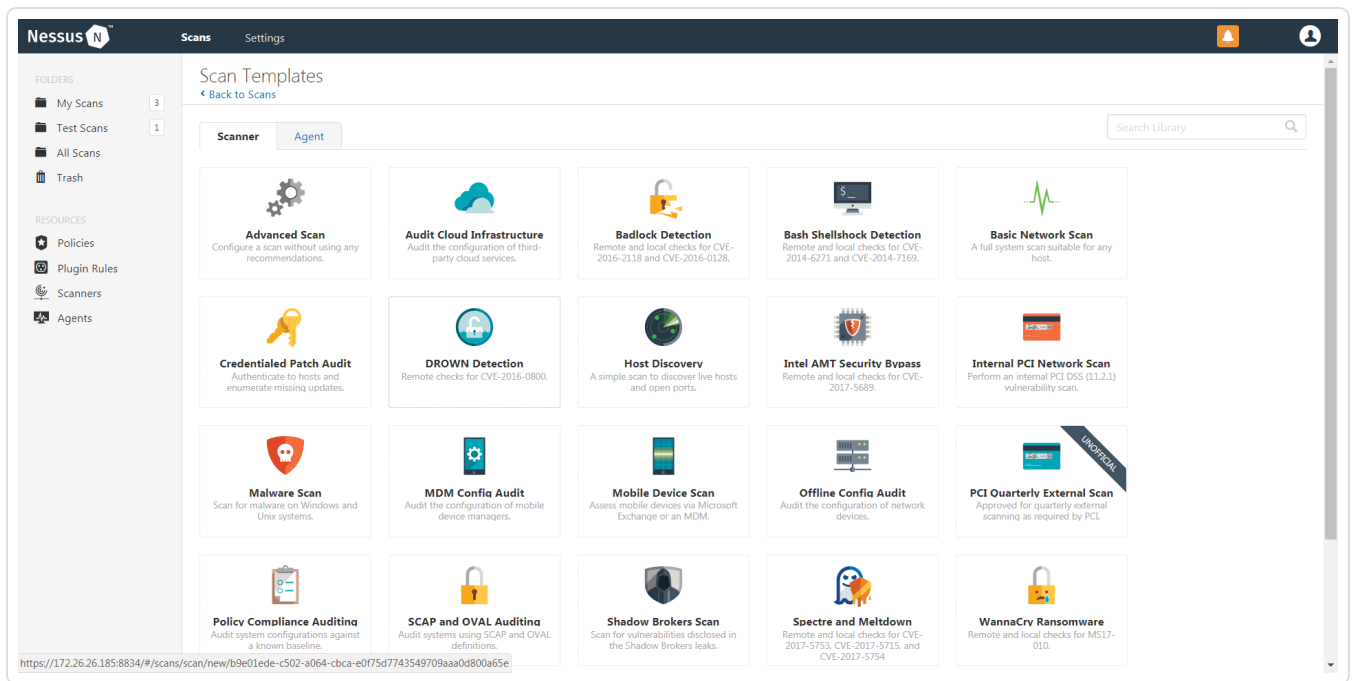
- You must create an **Explicit Account** under *Delegation > Delegation Identities* in Lieberman.

## To integrate with SSH:

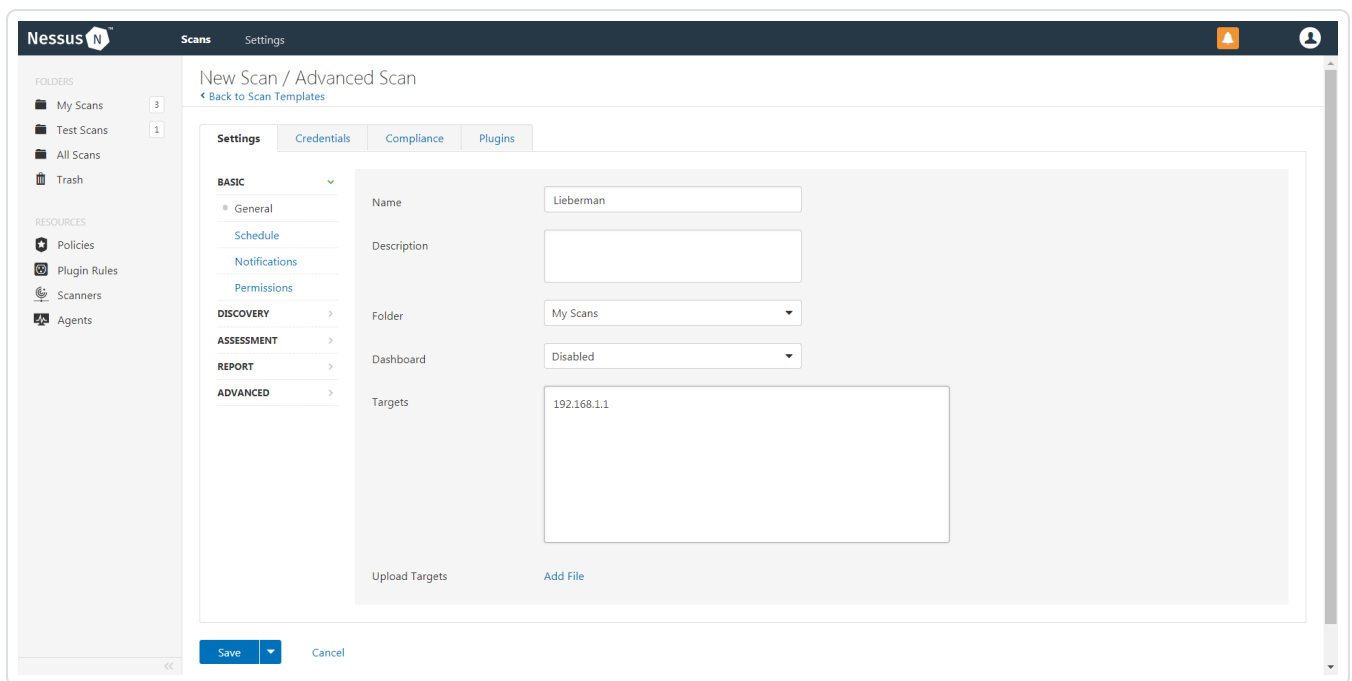
- In a browser, log in to Nessus.
- Navigate to the **Scans** section.
- Click the **+ New Scan** button to configure Nessus for credentialed scans of Windows systems using Lieberman's password management solution.



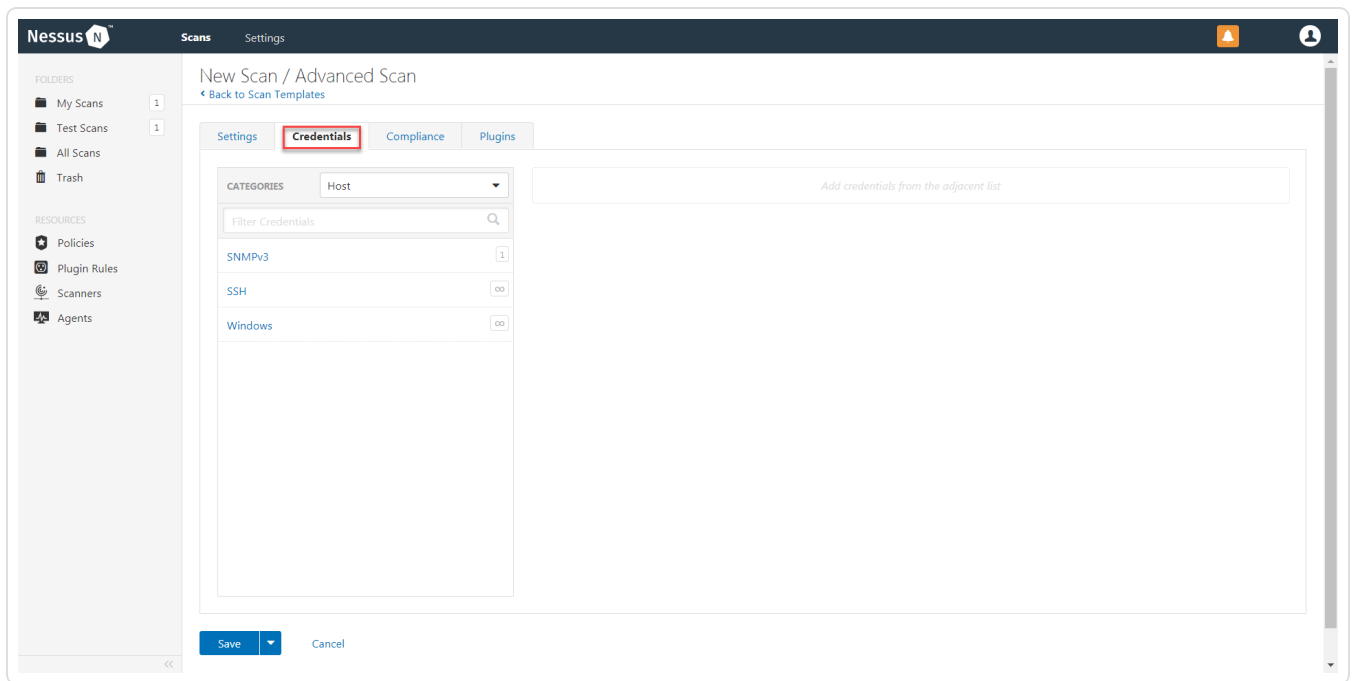
- Select a **Scan Template** for the scan type required for your scan. For demonstration purposes, the **Advanced Network Scan** template is used.



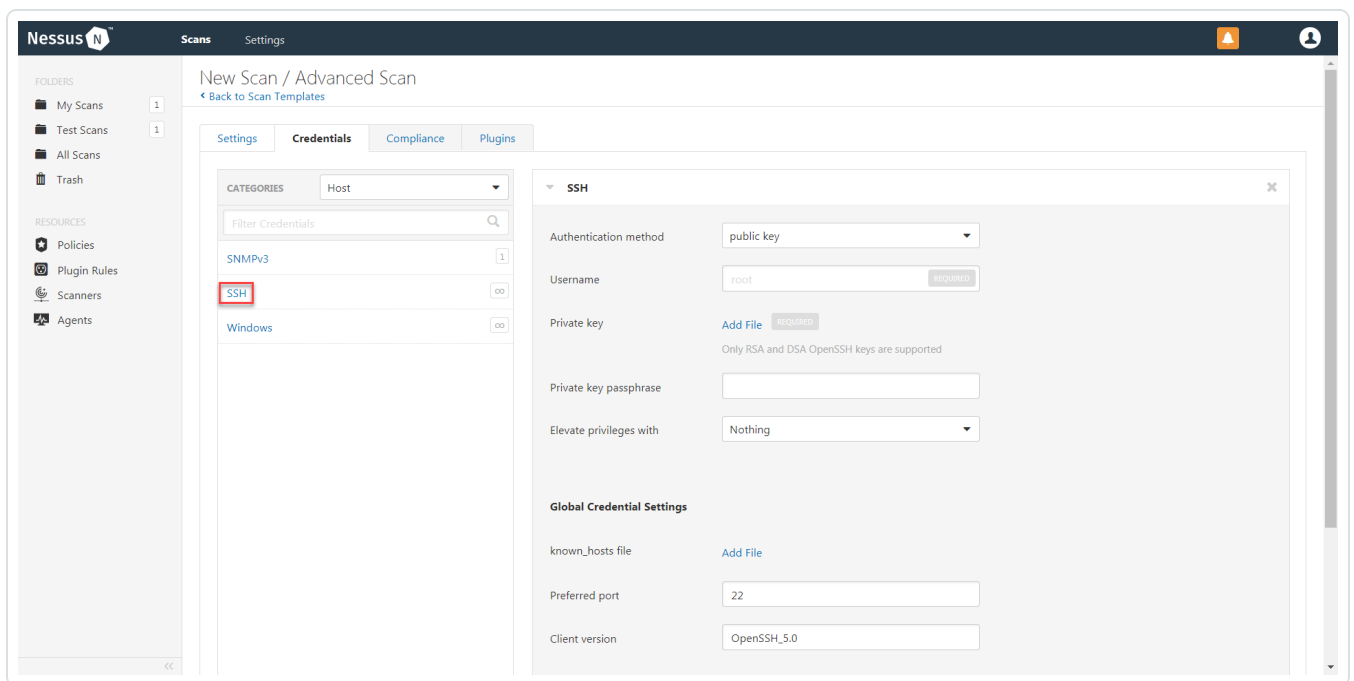
5. Enter a descriptive **Name** and the IP address(es) or hostname(s) of the scan **Targets**.



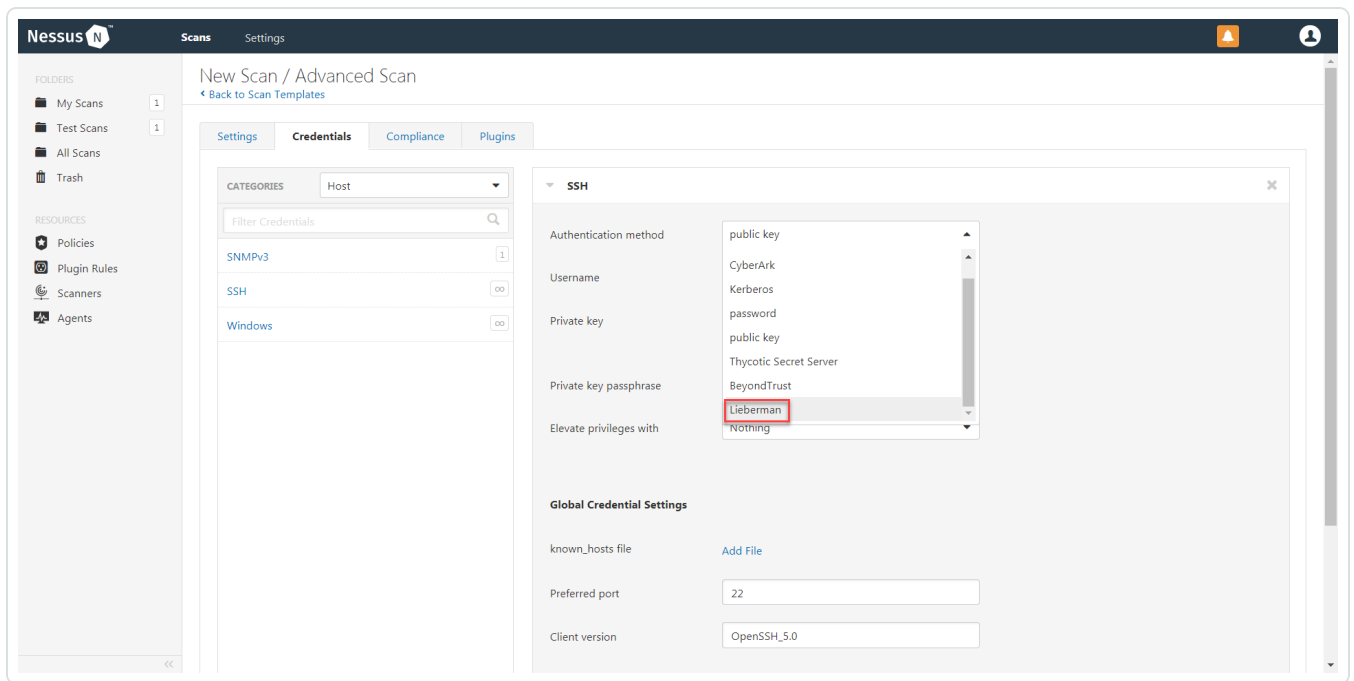
6. Click on the **Credentials** tab.



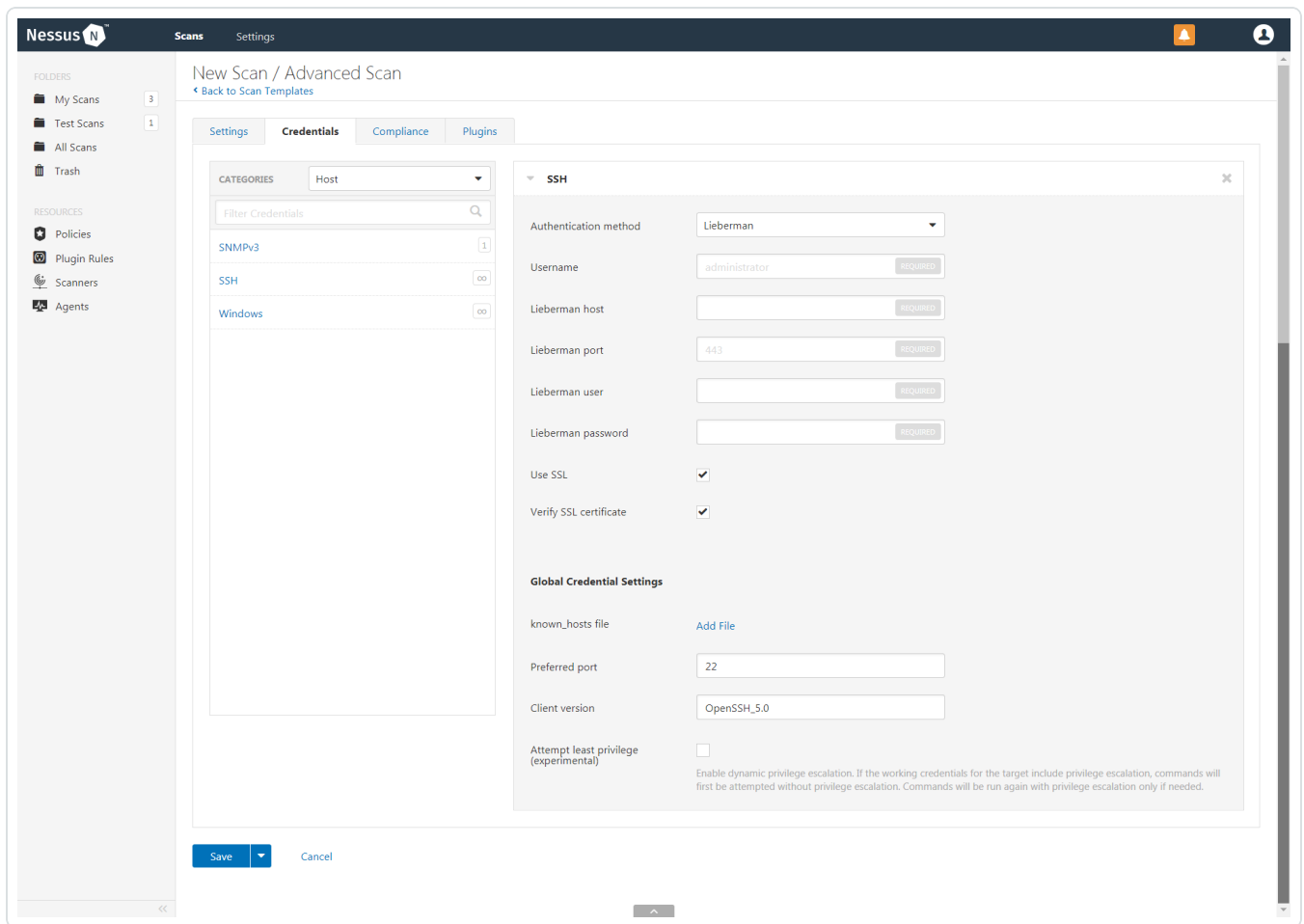
7. In the left-hand menu, select **SSH**.



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



9. Configure each field for SSH authentication. Refer to the table below for a description of each field.



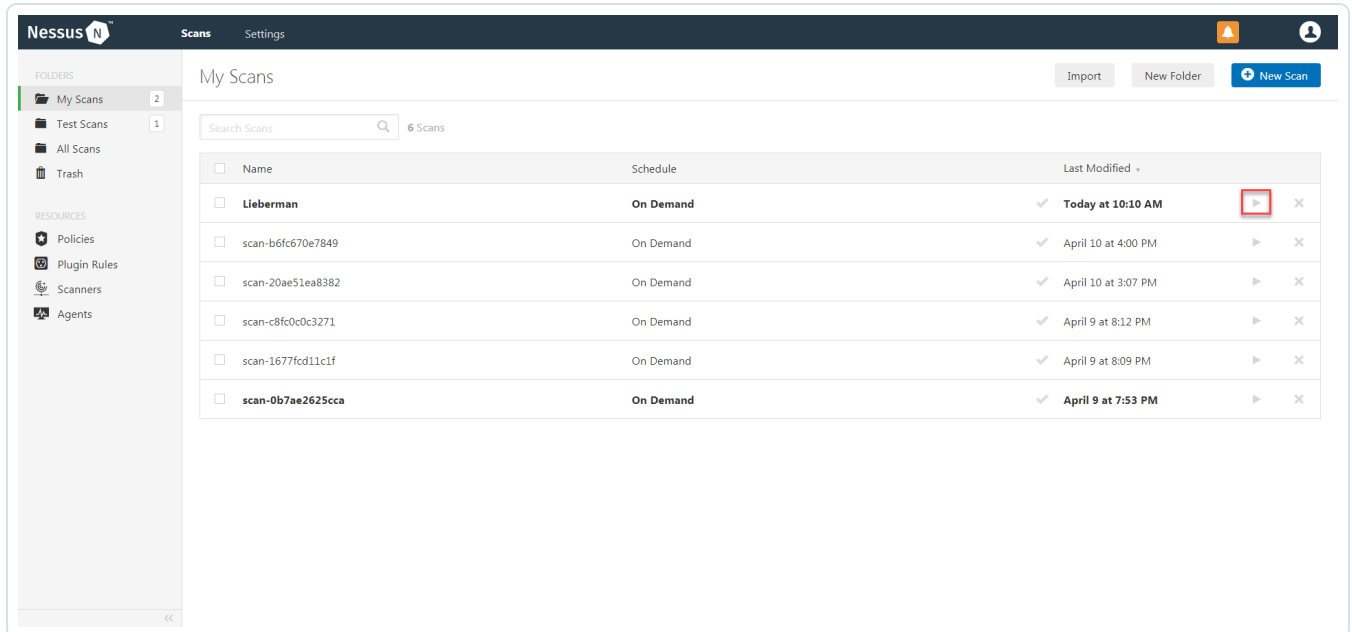
The table below contains a description of each option:

Option	Description
Username	(Required) The target system's username.
Lieberman Host	(Required) The Lieberman IP/DNS address.
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.
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.

10. Once the options to reach Lieberman are set, click **Save**.
11. To verify the integration is working, click the **Launch** button to initiate an on-demand scan.



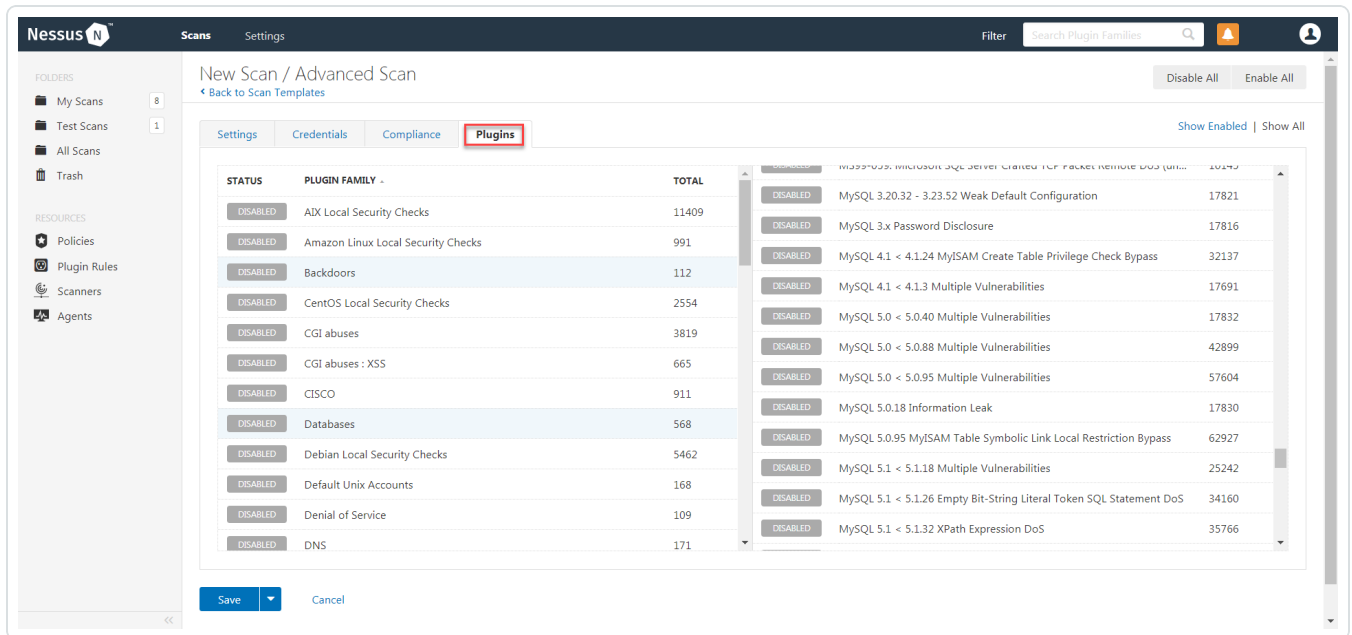
12. Once the scan has completed, select the completed scan and look for **Plugin ID 97993** and the corresponding message - *It was possible to log into the remote host via SSH using 'password' authentication*. This validates that authentication was successful.



# Database Integration

Tenable Nessus 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.

scan-58dc178c3601 / Configuration

Settings | Credentials | Compliance | **Plugins**

STATUS	PLUGIN FAMILY	TOTAL	DISABLED	ENABLED
DISABLED	Oracle WebLogic Server Multiple Vulnerabilities (O...	78541	DISABLED	
DISABLED	AIX Local Security Checks	11409	DISABLED	
DISABLED	Oracle WebLogic Server Multiple Vulnerabilities (O...	94290	DISABLED	
DISABLED	Amazon Linux Local Security Checks	991	DISABLED	
DISABLED	Oracle WebLogic Server Multiple Vulnerabilities (O...	103935	DISABLED	
DISABLED	Backdoors	112	DISABLED	
DISABLED	Oracle WebLogic Server Node Manager Remote C...	44316	DISABLED	
DISABLED	CentOS Local Security Checks	2554	DISABLED	
DISABLED	Oracle WebLogic Server Security Subcomponent ...	73914	DISABLED	
DISABLED	CGI abuses	3819	ENABLED	
DISABLED	OS Identification and Installed Software Enumerati...	97993		ENABLED
DISABLED	CGI abuses : XSS	665	DISABLED	
DISABLED	pam_ssh Login Prompt Remote Username Enume...	38197	DISABLED	
DISABLED	CISCO	909	DISABLED	
DISABLED	Patch Management: Dell KACE K1000 Computer I...	76867	DISABLED	
DISABLED	Databases	568	DISABLED	
DISABLED	Patch Management: Dell KACE K1000 Report	76869	DISABLED	
DISABLED	Debian Local Security Checks	5458	DISABLED	
DISABLED	Patch Management: Get Packages from Symante...	80860	DISABLED	
DISABLED	Default Unix Accounts	168	DISABLED	
DISABLED	Patch Management: Host information from VMwar...	57027	DISABLED	
DISABLED	Denial of Service	109	DISABLED	
DISABLED	Patch Management: Missing updates from Dell KA...	76868	DISABLED	
DISABLED	DNS	171	DISABLED	
DISABLED	Patch Management: Missing updates from SCCM	57030	DISABLED	
DISABLED	F5 Networks Local Security Checks	607	DISABLED	
DISABLED	Patch Management: Missing Updates from Syman...	78012	DISABLED	
DISABLED	Fedora Local Security Checks	12543	DISABLED	
DISABLED	Patch Management: Missing updates from Tivoli E...	62560	DISABLED	

Save Cancel

3. Click **Save**.

**Note:** See the chart for database plugin types and corresponding IDs.

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

---

# Additional Information

---

[Lieberman RED System](#)

[About Tenable](#)

---

# Lieberman RED System

---

For additional information and documentation about the Lieberman RED Identity Management 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](https://tenable.com).