Tenable and Centrify Vault Integration Guide

Last Revised: May 22, 2021

Table of Contents

Welcome to Tenable for Centrify

This document provides information and steps for integrating Tenable applications with Centrify Vault.

Integrating Tenable applications with Centrify provides an effective solution for managing, controlling, and monitoring privileged user activities. Centrify provides technology security teams with centralized policy framework to authorize privileges based on roles and responsibilities.

You can integrate Centrify with Nessus Manager or Tenable.io.

The benefits of integrating Tenable applications with Centrify include:

- A single location for access to super user passwords for all on-premises and cloud-based systems
- Simplified and automated shared account password management
- Centralized control for credentials access and administrator audits

For additional information about Centrify, see the Centrify website.

Requirements

To properly integrate Tenable with Centrify you must meet the following requirements.

Tenable Product

You must have an active account for at least one of the following Tenable products to integrate with Centrify: Tenable.io or Nessus Manager.

Tenable User Role

You must have the appropriate role for your Tenable account as listed below.

- Tenable.io - Standard, Scan Manager, Administrator, or System Administrator
- Nessus Manager - Standard, Administrator, or System Administrator

Centrify Requirements

You must have an active Centrify account with Centrify Privileged Access Service 19.5.195 or higher.

Nessus and Centrify Vault

View the corresponding section to configure your Nessus application with Centrify.

Configure Nessus Manager with Centrify (Windows)

Configure Nessus for Centrify (SSH)

Configure Nessus Manager with Centrify (Windows)

In Nessus Manager, you can integrate with Centrify using Windows credentials. Complete the following steps to configure Nessus Manager with Centrify in Windows.

Requirements

- Nessus Manager account
- Centrify account

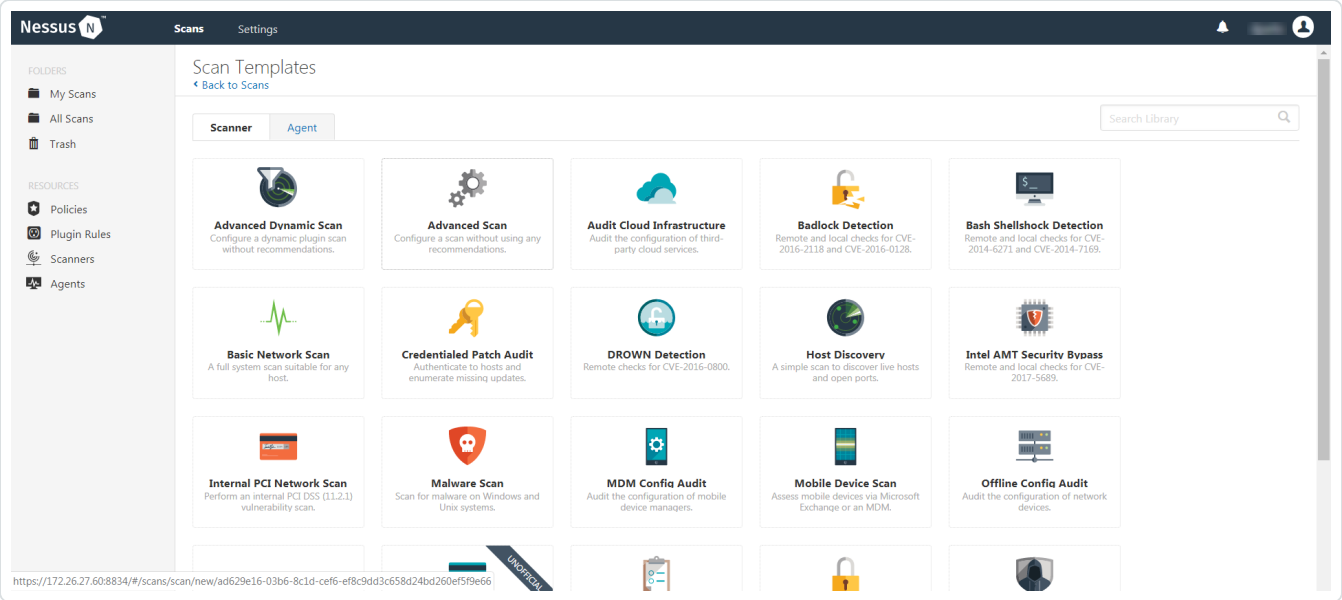
Required User Role: Standard, Administrator, or System Administrator

To integrate with Windows:

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

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

   The **Scan Templates** page appears.



4. Select a scan template.

   The selected scan template **Settings** 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) Add a description, folder location, scanner location, and specify target groups.
8. Click the **Credentials** tab.

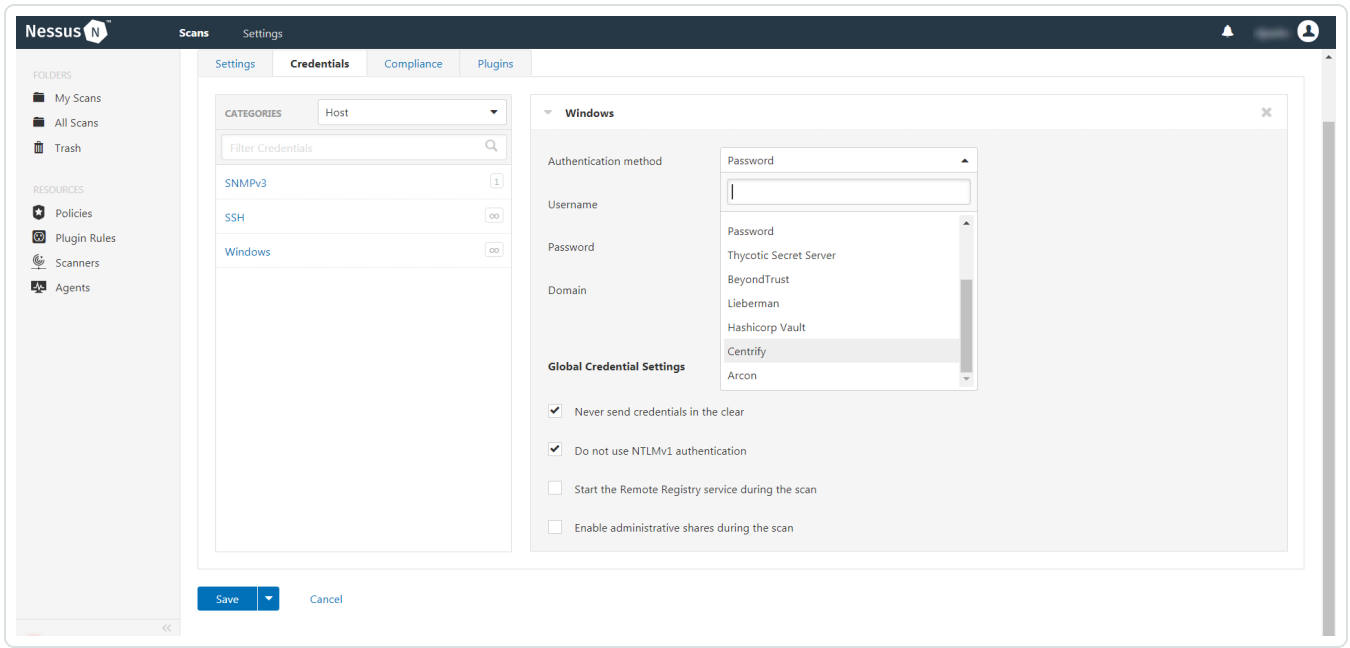
   The **Credentials** options appear. By default, the **Categories** drop-down box displays **Host**.

9. In the left menu, select **Windows**.

   The **Windows** settings appear.

10. In the **Windows** settings, click the **Authentication method** drop-down box.

    The **Authentication method** drop-down box options appear.



11. Select **Centrify**.

    The **Centrify** options appear.

12. Configure the Windows credentials.

Option	Default Value
Centrify Host	(Required) The Centrify IP address or DNS address. **Note:** If your Centrify installation is in a subdirectory, you must include the subdirectory path. For example, type *IP address or hostname/sub-directory path*.
Centrify Port	The port on which Centrify listens.
API User	(Required) The API user provided by Centrify
API Key	(Required) The API key provided by Centrify.
Tenant	The name of a specified team in a multi-team environment.
Authentication URL	The URL Nessus Manager uses to access Centrify.
Password Engine URL	The name of a specified team in a multi-team environment.
Username	(Required) The username to log in to the hosts you want to scan.
Checkout Duration	The length of time, in minutes, that you want to keep credentials checked out in Centrify. Configure the **Checkout Duration** to exceed the typical duration of your Nessus Manager scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in Centrify so that password changes do not disrupt your Nessus Manager scans. If Centrify changes a password during a scan, the scan fails.
Use SSL	When enabled, Nessus Manager uses SSL through IIS for secure communications. You must configure SSL through IIS in Centrify before enabling this option.

Verify SSL	When enabled, Nessus Manager validates the SSL certificate. You must configure SSL through IIS in Centrify before enabling this option.

13. Click **Save**.

    The credential saves and the **My Scans** page appears.

What to do next:

To verify the integration is working:

1. On the **My Scans** page, click the **Launch** button to initiate an on-demand scan.
2. Once the scan completes, select the completed scan and look for the following message - *Microsoft Windows SMB Log In Possible: 10394*. This result validates that authentication was successful.

Configure Nessus for Centrify (SSH)

In Nessus Manager, you can integrate with Centrify using SSH credentials. Complete the following steps to configure Nessus with Centrify using SSH.

Requirements

- Nessus Manager account
- Centrify account

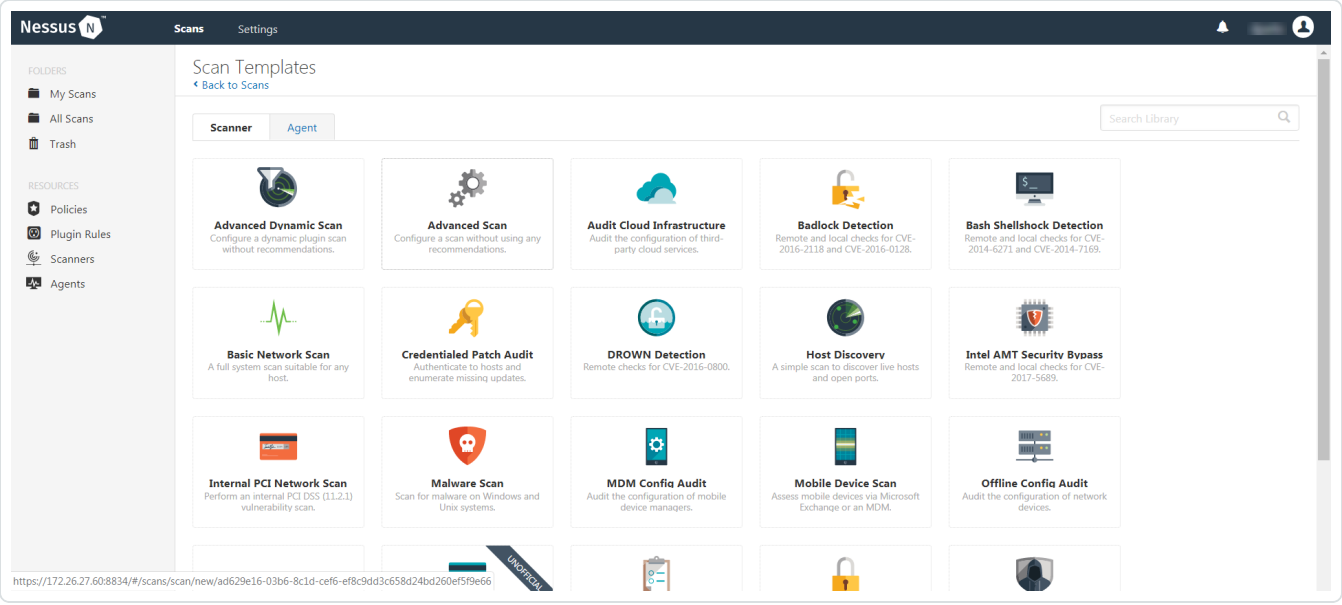
Required User Role: Standard, Administrator, or System administrator

To integrate Nessus with Centrify using SSH credentials:

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

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

   The **Scan Templates** page appears.



4. Select a scan template.

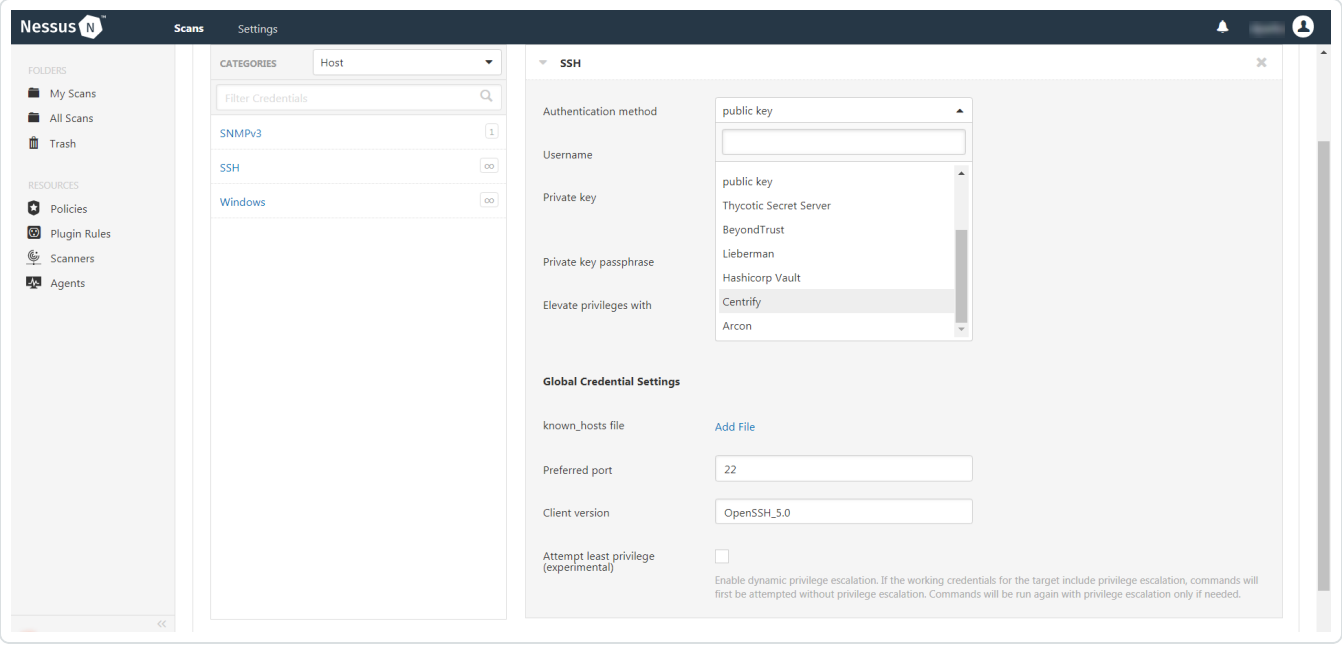
The selected scan template **Settings** page appears.

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) 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 left menu, select **SSH**.

   The **SSH** settings appear.
10. In the **SSH** settings, click the **Authentication method** drop-down box.

    The **Authentication method** drop-down box options appear.



11. Select **Centrify**.

    The **Centrify** options appear.
12. Configure the SSH credentials.

Option	Default Value
Centrify Host	(Required) The Centrify IP address or DNS address. **Note:** If your Centrify installation is in a subdirectory, you must include the subdirectory path. For example, type *`IP address or hostname/sub-directory path`*.
Centrify Port	The port on which Centrify listens.
API User	(Required) The API user provided by Centrify
API Key	(Required) The API key provided by Centrify.
Tenant	The name of a specified team in a multi-team environment.
Authentication URL	The URL Nessus Manager uses to access Centrify.
Password Engine URL	The name of a specified team in a multi-team environment.
Username	(Required) The username to log in to the hosts you want to scan.
Checkout Duration	The length of time, in minutes, that you want to keep credentials checked out in Centrify. Configure the **Checkout Duration** to exceed the typical duration of your Nessus Manager scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in Centrify so that password changes do not disrupt your Nessus Manager scans. If Centrify changes a password during a scan, the scan fails.
Use SSL	When enabled, Nessus Manager uses SSL through IIS for secure communications. You must configure SSL through IIS in Centrify before enabling this option.
Verify SSL	When enabled, Nessus Manager validates the SSL certificate. You must configure SSL through IIS in Centrify before enabling this option.

13. Click **Save**.

What to do next:

To verify the integration is working:

1. On the **My Scans** page, click the **Launch** button to initiate an on-demand scan.
2. Once the scan completes, 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 result validates that authentication was successful.

Tenable.io and Centrify Vault

View the corresponding section to configure your Nessus application with Centrify.

Configure Tenable.io with Centrify (Windows)

Configure Tenable.io for Centrify (SSH)

Configure Tenable.io with Centrify (Windows)

In Tenable.io, you can integrate with Centrify using Windows credentials. Complete the following steps to configure Tenable.io with Centrify using Windows.

Requirements

- Tenable.io account
- Centrify account

Required User Role: Standard, Scan Manager, or Administrator

To integrate Tenable.io with Centrify using Windows credentials:

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 **Centrify**.

The **Centrify** options appear.

8. Configure the **Centrify** credentials.

9.

Option	Default Value
Centrify Host	(Required) The Centrify IP address or DNS address. **Note:** If your Centrify installation is in a subdirectory, you must include the subdirectory path. For example, type *`IP address or hostname/sub-directory path`*.
Centrify Port	The port on which Centrify listens.
API User	(Required) The API user provided by Centrify
API Key	(Required) The API key provided by Centrify.
Tenant	The name of a specified team in a multi-team environment.
Authentication URL	The URL Tenable.io uses to access Centrify.
Password Engine URL	The name of a specified team in a multi-team environment.
Username	(Required) The username to log in to the hosts you want to scan.
Checkout Duration	The length of time, in minutes, that you want to keep credentials checked out in Centrify. Configure the **Checkout Duration** to exceed the typical duration of your Tenable.io scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in Centrify so that password changes do not disrupt your Tenable.io scans. If Centrify changes a password during a scan, the scan fails.
Use SSL	When enabled, Tenable.io uses SSL through IIS for secure communications. You must configure SSL through IIS in Centrify before

	enabling this option.
Verify SSL	When enabled, Tenable.io validates the SSL certificate. You must configure SSL through IIS in Centrify before enabling this option.

10. Click **Save**.

    The credential saves and the **My Scans** page appears.

What to do next:

Verify the integration is working.

1. On the **My Scans** page, click the **Launch** button to initiate an on-demand scan.
2. Once the scan completes, click the completed scan.

   The scan details appear.

   Look for a message similar to the following- *Microsoft Windows SMB Log In Possible: 10394*. This validates that authentication was successful.

Configure Tenable.io for Centrify (SSH)

In Tenable.io, you can integrate with Centrify using SSH credentials. Complete the following steps to configure Tenable.io with Centrify using SSH.

Requirements

- Tenable.io account
- Centrify account

Required User Role: Standard, Scan Manager, or Administrator

To configure Tenable.io for CentrifySSH:

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 **SSH**.

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

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

9.

Option	Default Value
Centrify Host	(Required) The Centrify IP address or DNS address. **Note:** If your Centrify installation is in a subdirectory, you must include the subdirectory path. For example, type *`IP address or hostname/sub-directory path`*.
Centrify Port	The port on which Centrify listens.
API User	(Required) The API user provided by Centrify
API Key	(Required) The API key provided by Centrify.
Tenant	The name of a specified team in a multi-team environment.
Authentication URL	The URL Tenable.io uses to access Centrify.
Password Engine URL	The name of a specified team in a multi-team environment.
Username	(Required) The username to log in to the hosts you want to scan.
Checkout Duration	The length of time, in minutes, that you want to keep credentials checked out in Centrify. Configure the **Checkout Duration** to exceed the typical duration of your Tenable.io scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails. **Note:** Configure the password change interval in Centrify so that password changes do not disrupt your Tenable.io scans. If Centrify changes a password during a scan, the scan fails.
Use SSL	When enabled, Tenable.io uses SSL through IIS for secure communications. You must configure SSL through IIS in Centrify before enabling this option.
Verify SSL	When enabled, Tenable.io validates the SSL certificate. You must configure SSL through IIS in Centrify before enabling this option.

10. Click **Save**.

What to do next:

To verify the integration is working:

1. On the **My Scans** page, 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 result validates that authentication was successful.