Tenable and Centrify Vault Integration Guide

Last Revised: April 09, 2025

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 Tenable Nessus Manager, Tenable Vulnerability Management, or Tenable Security Center.

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 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 Vulnerability Management, Tenable Nessus Manager, or Tenable Security Center.

Tenable User Role

You must have the appropriate role for your Tenable account.

- Tenable Vulnerability Management - Standard, Scan Manager, Administrator, or System Administrator
- Tenable Security Center - Any
- Tenable 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 sections to configure your Tenable Nessus application with Centrify.

Configure Tenable Nessus Manager with Centrify (Windows)

Configure Tenable Nessus for Centrify (SSH)

Configure Tenable Nessus Manager with Centrify (Windows)

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

Required User Role: Standard, Administrator, or System Administrator

To integrate with Windows:

1. Log in to your Tenable user interface.
2. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.
3. In the left navigation plane, click **Scans**.

   The **Scans** page appears.
4. In the upper-right corner of the page, click the **Create a Scan** button.

   The **Select a Scan Template** page appears.
5. Select a scan template.

   The scan configuration page appears.
6. In the **Name** box, type a name for the scan.
7. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
8. (Optional) Add a description, folder location, scanner location, and specify target groups.
9. Click the **Credentials** tab.

   The **Credentials** pane appears.

10. In the **Select a Credential** menu, select the **Host** drop-down.
11. Select **Windows**.

    The **Settings** pane appears.
12. In the **Auth Type** drop-down box, click **Centrify**.

    The Centrify options appear.
13. Configure each option for the **Windows** authentication.

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/subdirectory 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 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 Tenable Nessus Manager scans. If a password from a previous scan is still checked out when a new scan begins, the new scan

Option	Default Value
	fails. **Note:** Configure the password change interval in Centrify so that password changes do not disrupt your Tenable Nessus Manager scans. If Centrify changes a password during a scan, the scan fails.
Use SSL	When enabled, Tenable 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, Tenable Nessus Manager validates the SSL certificate. You must configure SSL through IIS in Centrify before enabling this option.
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.

14. Do one of the following:

    - If you want to save without launching the scan, click **Save**.
    - If you want to save and launch the scan immediately, click **Save & Launch**.

      Note: If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

What to do next:

To verify the integration is working:

1. On the **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 Tenable Nessus for Centrify (SSH)

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

> **Required User Role:** Standard, Administrator, or System administrator

To integrate Tenable Nessus with Centrify using SSH credentials:

1. Log in to your Tenable user interface.
2. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.
3. In the left navigation plane, click **Scans**.

   The **Scans** page appears.
4. In the upper-right corner of the page, click the **Create a Scan** button.

   The **Select a Scan Template** page appears.
5. Select a scan template.

   The scan configuration page appears.
6. In the **Name** box, type a name for the scan.
7. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
8. (Optional) Add a description, folder location, scanner location, and specify target groups.
9. Click the **Credentials** tab.

   The **Credentials** pane appears.
10. In the **Select a Credential** menu, select the **Host** drop-down.

11. Select **SSH**.

    The **Settings** pane appears.

12. In the **Auth Type** drop-down box, click **Centrify**.

    The Centrify options appear.

13. Configure each option for the **SSH** authentication.

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/subdirectory 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 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 Tenable Nessus Manager scans. If a password from a previous scan is still checked out when a new scan begins, the new scan fails.

Option	Default Value
	Note: Configure the password change interval in Centrify so that password changes do not disrupt your Tenable Nessus Manager scans. If Centrify changes a password during a scan, the scan fails.
Use SSL	When enabled, Tenable 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, Tenable Nessus Manager validates the SSL certificate. You must configure SSL through IIS in Centrify before enabling this option.
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.

14. Do one of the following:

    - If you want to save without launching the scan, click **Save**.
    - If you want to save and launch the scan immediately, click **Save & Launch**.

      Note: If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

What to do next:

To verify the integration is working:

1. On the **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 Security Center and Centrify Vault

View the corresponding sections to configure your Tenable Security Center application with Centrify.

Configure Tenable Security Center with Centrify (Windows)

Configure Tenable Security Center for Centrify (SSH)

Configure Tenable Security Center with Centrify (Windows)

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

Required User Role: Standard, Administrator, or System Administrator

To integrate with Windows:

1. Log in to Tenable Security Center.
2. Click **Scanning** > **Credentials** (administrator users) or **Scans** > **Credentials** (organizational users).

   The **Credentials** page appears.
3. Click **Add**.

   The **Credential Templates** page appears.
4. In the **Miscellaneous**, **API Gateway**, **Database**, **SNMP**, **SSH**, or **Windows**, or **Web Authentication** sections, click the tile for the specific method you want to configure.

   The **Add Credentials** configuration page appears.
5. In the **Name** box, type a name for the credentials.
6. In the **Description** box, type a description for the credentials.
7. (Optional) Type or select a **Tag**. For more information, see Tags in the *Tenable Security Center User Guide*.
8. Configure each option for the **Windows** authentication.

Option	Description
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/subdirectory path*.
Centrify Port	(Required) The port on which Centrify listens. By default, Tenable Security CenterTenable Vulnerability Management uses port 443.
API User	(Required) The API user provided by Centrify.
API Key	(Required) The API key provided by Centrify.
Tenant	(Required) The Centrify tenant associated with the API. By default, Tenable Security CenterTenable Vulnerability Management uses *centrify*.
Authentication URL	(Required) The URL Tenable Security CenterTenable Vulnerability Management uses to access Centrify. By default, Tenable Security CenterTenable Vulnerability Management uses */Security*.
Password Query URL	(Required) The URL Tenable Security CenterTenable Vulnerability Management uses to query the passwords in Centrify. By default, Tenable Security Center uses */RedRock*.
Password Engine URL	(Required) The URL Tenable Security CenterTenable Vulnerability Management uses to access the passwords in Centrify. By default, Tenable Security CenterTenable Vulnerability Management uses */ServerManage*.
Username	(Required) The username to log in to the hosts you want to scan.
Checkout Duration	(Required) 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 Security Center scans so that password changes do

	not disrupt your Tenable Security CenterTenable Vulnerability Management scans. If Centrify changes a password during a scan, the scan fails. If a password from a previous scan is still checked out when a new scan begins, the new scan fails.
Use SSL	When enabled, Tenable Security CenterTenable Vulnerability Management uses SSL through IIS for secure communications. You must configure SSL through IIS in Centrify before enabling this option.
Verify SSL Certificate	When enabled, Tenable Security CenterTenable Vulnerability Management validates the SSL certificate. You must configure SSL through IIS in Centrify before enabling this option.

9. Click **Submit**.

   Tenable Security Center saves your configuration.

What to do next:

To verify the integration is working:

1. On the **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 Tenable Security Center for Centrify (SSH)

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

Required User Role: Standard, Administrator, or System administrator

To integrate Tenable Security Center with Centrify using SSH credentials:

1. Log in to Tenable Security Center.
2. Click **Scanning** > **Credentials** (administrator users) or **Scans** > **Credentials** (organizational users).

   The **Credentials** page appears.
3. Click **Add**.

   The **Credential Templates** page appears.
4. In the **Miscellaneous**, **API Gateway**, **Database**, **SNMP**, **SSH**, or **Windows**, or **Web Authentication** sections, click the tile for the specific method you want to configure.

   The **Add Credentials** configuration page appears.
5. In the **Name** box, type a name for the credentials.
6. In the **Description** box, type a description for the credentials.
7. (Optional) Type or select a **Tag**. For more information, see Tags in the *Tenable Security Center User Guide*.
8. Configure each option for the **SSH** authentication.

Option	Description
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/subdirectory path*.
Centrify Port	(Required) The port on which Centrify listens. By default, Tenable Security CenterTenable Vulnerability Management uses port 443.
API User	(Required) The API user provided by Centrify.
API Key	(Required) The API key provided by Centrify.
Tenant	(Required) The Centrify tenant associated with the API. By default, Tenable Security CenterTenable Vulnerability Management uses

	centrify.
Authentication URL	(Required) The URL Tenable Security CenterTenable Vulnerability Management uses to access Centrify. By default, Tenable Security CenterTenable Vulnerability Management uses */Security*.
Password Query URL	(Required) The URL Tenable Security CenterTenable Vulnerability Management uses to query the passwords in Centrify. By default, Tenable Security Center uses */RedRock*.
Password Engine URL	(Required) The URL Tenable Security CenterTenable Vulnerability Management uses to access the passwords in Centrify. By default, Tenable Security CenterTenable Vulnerability Management uses */ServerManage*.
Username	(Required) The username to log in to the hosts you want to scan.
Checkout Duration	(Required) 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 Security Center scans so that password changes do not disrupt your Tenable Security CenterTenable Vulnerability Management scans. If Centrify changes a password during a scan, the scan fails. If a password from a previous scan is still checked out when a new scan begins, the new scan fails.
Use SSL	When enabled, Tenable Security CenterTenable Vulnerability Management uses SSL through IIS for secure communications. You must configure SSL through IIS in Centrify before enabling this option.
Verify SSL Certificate	When enabled, Tenable Security CenterTenable Vulnerability Management validates the SSL certificate. You must configure SSL through IIS in Centrify before enabling this option.

9. Click **Submit**.

   Tenable Security Center saves your configuration.

What to do next:

To verify the integration is working:

1. On the **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 Vulnerability Management and Centrify Vault

View the corresponding sections to configure your Tenable Nessus application with Centrify.

Configure Tenable Vulnerability Management with Centrify (Windows)

Configure Tenable Vulnerability Management for Centrify (SSH)

Configure Tenable Vulnerability Management with Centrify (Windows)

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

> **Required User Role:** Standard, Scan Manager, or Administrator

To integrate Tenable Vulnerability Management with Centrify using Windows credentials:

1. Log in to your Tenable user interface.
2. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.
3. In the left navigation plane, click **Scans**.

   The **Scans** page appears.
4. In the upper-right corner of the page, click the **Create a Scan** button.

   The **Select a Scan Template** page appears.
5. Select a scan template.

   The scan configuration page appears.
6. In the **Name** box, type a name for the scan.
7. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
8. (Optional) Add a description, folder location, scanner location, and specify target groups.
9. Click the **Credentials** tab.

The **Credentials** pane appears.

10. In the **Select a Credential** menu, select the **Host** drop-down.
11. Select **Windows**.

    The **Settings** pane appears.
12. In the **Auth Type** drop-down box, click **Centrify** Secret Server.

    The Centrify Secret Server options appear.
13. Configure each option for the **Windows** authentication.

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/subdirectory 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 Vulnerability Management 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

Option	Default Value
	your Tenable Vulnerability Management 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 Vulnerability Management scans. If Centrify changes a password during a scan, the scan fails.
Use SSL	When enabled, Tenable Vulnerability Management uses SSL through IIS for secure communications. You must configure SSL through IIS in Centrify before enabling this option.
Verify SSL	When enabled, Tenable Vulnerability Management validates the SSL certificate. You must configure SSL through IIS in Centrify before enabling this option.
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.

14. Do one of the following:

    - If you want to save without launching the scan, click **Save**.
    - If you want to save and launch the scan immediately, click **Save & Launch**.

> **Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

What to do next:

Verify the integration is working.

1. On the **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 Vulnerability Management for Centrify (SSH)

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

> **Required User Role:** Standard, Scan Manager, or Administrator

To configure Tenable Vulnerability Management for Centrify SSH:

1. Log in to your Tenable user interface.
2. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.
3. In the left navigation plane, click **Scans**.

   The **Scans** page appears.
4. In the upper-right corner of the page, click the **Create a Scan** button.

   The **Select a Scan Template** page appears.
5. Select a scan template.

   The scan configuration page appears.

6. In the **Name** box, type a name for the scan.
7. In the **Targets** box, type an IP address, hostname, or range of IP addresses.
8. (Optional) Add a description, folder location, scanner location, and specify target groups.
9. Click the **Credentials** tab.

   The **Credentials** pane appears.
10. In the **Select a Credential** menu, select the **Host** drop-down.
11. Select **SSH**.

    The **Settings** pane appears.
12. In the **Auth Type** drop-down box, click **Centrify**.

    The Centrify options appear.
13. Configure each option for the **SSH** authentication.

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/subdirectory 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 Vulnerability Management uses to access Centrify.
Password Engine URL	The name of a specified team in a multi-team environment.

Option	Default Value
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 Vulnerability Management 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 Vulnerability Management scans. If Centrify changes a password during a scan, the scan fails.
Use SSL	When enabled, Tenable Vulnerability Management uses SSL through IIS for secure communications. You must configure SSL through IIS in Centrify before enabling this option.
Verify SSL	When enabled, Tenable Vulnerability Management validates the SSL certificate. You must configure SSL through IIS in Centrify before enabling this option.
Targets to Prioritize Credentials	Specify IPs or CIDR blocks on which this credential is attempted before any other credential. To specify multiple IPs or CIDR blocks, use a comma or space-separated list. Using this setting can decrease scan times by prioritizing a credential that you know works against your selected targets. For example, if your scan specifies 100 credentials, and the successful credential is the 59th credential out of 100, the first 58 credentials have to fail before the 59th credential succeeds. If you use **Targets To Prioritize Credentials**, you configure the scan to use the successful credential first, which allows the scan to access the target faster.

14. Do one of the following:

- If you want to save without launching the scan, click **Save**.
- If you want to save and launch the scan immediately, click **Save & Launch**.

> **Note:** If you scheduled the scan to run at a later time, the **Save & Launch** option is not available.

What to do next:

To verify the integration is working:

1. On the **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.