Tenable and Delinea Integration Guide

Last Revised: June 02, 2025

Table of Contents

Welcome to Tenable for Delinea

This document provides information and steps for integrating Tenable Vulnerability Management, Tenable Nessus, or Tenable Security Center with Delinea Privileged Access Management (PAM).

The Tenable® integration with Delinea delivers a comprehensive authenticated scanning solution that provides security teams better vulnerability insight in order to protect privileged accounts. This integration supports the storage of privileged credentials in Delinea and their automatic retrieval at scan time by Tenable. This ensures that sensitive passwords are safely stored, controlled, auditable, and easily changed without manual intervention.

For more information about each product integration, see *Delinea* in the Tenable Nessus, Tenable Vulnerability Management, and Tenable Security Center user guides.

Delinea Integrations

View one of the following options for Delinea integration steps:

- Database Integration
- SSH Integration
- Windows Integration

Database Integration

Tenable provides full database support for Delinea.

Required User Role: Standard, Scan Manager, or Administrator

To configure Delinea database for Tenable Vulnerability Management or Tenable Nessus:

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 **Settings** pane appears.

10. Click the **Database** option.

    The **Database** options appear.

11. In the **Database Type** drop-down box, select **Cassandra**, **Oracle**, **DB2**, **MongoDB**, **PostgreSQL**, **MySQL**, **SQL Server**, or **Sybase ASE**.

12. In the **Auth Type** drop-down box, click **Delinea** Secret Server.

    The Delinea Secret Server options appear.

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

Option	Description	Required
Delinea Secret Name	The value of the secret on the Delinea server. The secret is labeled Secret Name on the Delinea server.	yes
Delinea Host	The Delinea Secret Server IP address or DNS address.	yes
Delinea Port	The port on which Delinea Secret Server listens.	yes
Delinea Authentication Method	Indicates whether to use credentials or an API key for authentication. By default, credentials are selected.	yes
Delinea Login Name	The username to authenticate to the Delinea server.	yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the Delinea Login Name you provided.	yes
Delinea API key	The API key provided by Delinea Secret Server.	yes

Use SSL	Enable if the Delinea Secret Server is configured to support SSL.	no
Verify SSL certificate	If enabled, verifies the SSL Certificate on the Delinea server.	no

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.

To configure Delinea database for Tenable Security Center:

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 **Database** authentication.

Option	Description	Required
Delinea Secret Name	The value of the secret on the Delinea server. The secret is labeled Secret Name on the Delinea server.	yes
Delinea Host	The Delinea Secret Server IP address or DNS address.	yes
Delinea Port	The port on which Delinea Secret Server listens.	yes
Delinea Authentication Method	Indicates whether to use credentials or an API key for authentication. By default, credentials are selected.	yes
Delinea Login Name	The username to authenticate to the Delinea server.	yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the Delinea Login Name you provided.	yes
Delinea API key	The API key provided by Delinea Secret Server.	yes
Use SSL	Enable if the Delinea Secret Server is configured to support SSL.	no
Verify SSL certificate	If enabled, verifies the SSL Certificate on the Delinea server.	no

9. Click **Submit**.

   Tenable Security Center saves your configuration.

SSH Integration

To configure Tenable with Delinea using SSH integration:

Required User Role: Standard, Scan Manager, or Administrator

To configure Delinea SSH for Tenable Vulnerability Management or Tenable Nessus:

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 **Delinea** Secret Server.

    The Delinea Secret Server options appear.
13. Configure each option for the **SSH** authentication.

Option	Description	Required
Delinea	Indicates whether to use credentials or an API key	yes

Authentication Method	for authentication. By default, **Credentials** is selected.	
Delinea Login Name	The username to authenticate to the Delinea server.	yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the Delinea Login Name you provided.	yes
Delinea API Key	The API key generated in the Secret Server user interface. This setting is required if the **API Key** authentication method is selected.	yes
Delinea Secret Name	The value of the secret on the Delinea server. The secret is labeled **Secret Name** on the Delinea server.	yes
Delinea Host	The Delinea Secret Server host to pull the secrets from.	yes
Delinea Port	The Delinea Secret Server Port for API requests. By default, Tenable uses 443.	yes
Delinea Login Name	The username to authenticate to the Delinea server.	yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the Delinea Login Name you provided.	yes
Use Private Key	If enabled, uses key-based authentication for SSH connections instead of password authentication.	no
Checkout Duration	The duration Tenable should check out the password from Delinea. Duration time is in hours and should be longer than the scan time.	yes

Use SSL	Enable if the Delinea Secret Server is configured to support SSL.	no
Verify SSL Certificate	If enabled, verifies the SSL Certificate on the Delinea server.	no
Elevate privileges with **Privilege Escalation**	The privilege escalation method you want to use to increase users' privileges after initial authentication. Multiple options for privilege escalation are supported, including su, su+sudo and sudo. Your selection determines the specific options you must configure.	no
Custom password prompt	Some devices are configured to prompt for a password with a non-standard string (for example, "secret-passcode"). This setting allows recognition of these prompts. Leave this blank for most standard password prompts.	no
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.	no

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.

To configure Delinea SSH for Tenable Security Center:

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	Required
Delinea Authentication Method	Indicates whether to use credentials or an API key for authentication. By default, **Credentials** is selected.	yes
Delinea Login Name	The username to authenticate to the Delinea server.	yes

Delinea Password	The password to authenticate to the Delinea server. This is associated with the Delinea Login Name you provided.	yes
Delinea API Key	The API key generated in the Secret Server user interface. This setting is required if the **API Key** authentication method is selected.	yes
Delinea Secret Name	The value of the secret on the Delinea server. The secret is labeled **Secret Name** on the Delinea server.	yes
Delinea Host	The Delinea Secret Server host to pull the secrets from.	yes
Delinea Port	The Delinea Secret Server Port for API requests. By default, Tenable uses 443.	yes
Delinea Login Name	The username to authenticate to the Delinea server.	yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the Delinea Login Name you provided.	yes
Use Private Key	If enabled, uses key-based authentication for SSH connections instead of password authentication.	no
Checkout Duration	The duration Tenable should check out the password from Delinea. Duration time is in hours and should be longer than the scan time.	yes
Use SSL	Enable if the Delinea Secret Server is configured to support SSL.	no
Verify SSL Certificate	If enabled, verifies the SSL Certificate on the Delinea server.	no

Elevate privileges with **Privilege Escalation**	The privilege escalation method you want to use to increase users' privileges after initial authentication. Multiple options for privilege escalation are supported, including su, su+sudo and sudo. Your selection determines the specific options you must configure.	no
Custom password prompt	Some devices are configured to prompt for a password with a non-standard string (for example, "secret-passcode"). This setting allows recognition of these prompts. Leave this blank for most standard password prompts.	no
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.	no

9. Click **Submit**.

   Tenable Security Center saves your configuration.

Windows Integration

To configure Tenable with Delinea using Windows integration:

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

To configure Delinea Windows for Tenable Vulnerability Management or Tenable Nessus:

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 **Delinea** Secret Server.

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

Option	Description	Required
Delinea	Indicates whether to use credentials or an API key	yes

Authentication Method	for authentication. By default, **Credentials** is selected.	
Delinea Login Name	The username to authenticate to the Delinea server.	yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the Delinea Login Name you provided.	yes
Delinea API Key	The API key generated in the Secret Server user interface. This setting is required if the **API Key** authentication method is selected.	yes
Delinea Secret Name	The value of the secret on the Delinea server. The secret is labeled **Secret Name** on the Delinea server.	yes
Delinea Host	The Delinea Secret Server IP address for API requests.	yes
Delinea Port	The Delinea Secret Server Port for API requests. By default, Tenable uses 443.	yes
Delinea Login Name	The username to authenticate to the Delinea server.	yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the Delinea Login Name you provided.	yes
Checkout Duration	The duration Tenable should check out the password from Delinea. Duration time is in hours and should be longer than the scan time.	yes
Use SSL	Enable if the Delinea Secret Server is configured to support SSL.	no

Verify SSL Certificate	If enabled. verifies the SSL Certificate on the Delinea server.	no

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.

To configure Delinea Windows for Tenable Security Center:

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	Required
Delinea	Indicates whether to use credentials or an API key	yes

Authentication Method	for authentication. By default, **Credentials** is selected.	
Delinea Login Name	The username to authenticate to the Delinea server.	yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the Delinea Login Name you provided.	yes
Delinea API Key	The API key generated in the Secret Server user interface. This setting is required if the **API Key** authentication method is selected.	yes
Delinea Secret Name	The value of the secret on the Delinea server. The secret is labeled **Secret Name** on the Delinea server.	yes
Delinea Host	The Delinea Secret Server IP address for API requests.	yes
Delinea Port	The Delinea Secret Server Port for API requests. By default, Tenable uses 443.	yes
Delinea Login Name	The username to authenticate to the Delinea server.	yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the Delinea Login Name you provided.	yes
Checkout Duration	The duration Tenable should check out the password from Delinea. Duration time is in hours and should be longer than the scan time.	yes
Use SSL	Enable if the Delinea Secret Server is configured to support SSL.	no

Verify SSL Certificate	If enabled. verifies the SSL Certificate on the Delinea server.	no

9. Click **Submit**.

   Tenable Security Center saves your configuration.

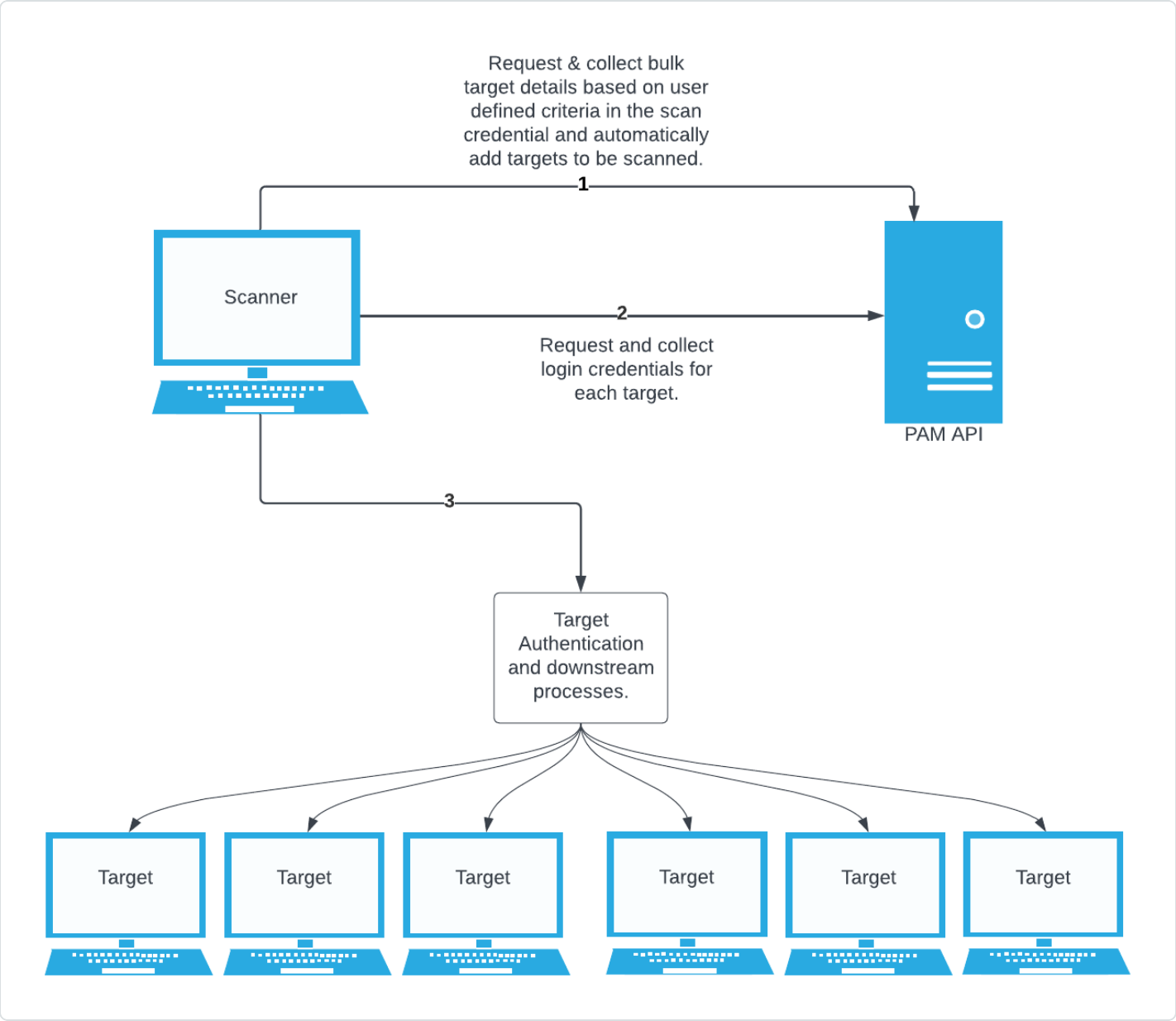
Delinea Secret Server Auto-Discovery

Tenable's Delinea Secret Server integration provides the Auto-Discovery feature with significant advantages. When using Delinea Secret Server Auto-Discovery, the scan automatically adds discovered hosts as scan targets with their respective credentials. With the Auto-Discovery feature, there is no need to enter these scan targets in the target list.

Enter one target in the target list. This target can be any pingable IP address or hostname, such as the IP address of the scanner, 127.0.0.1, or the address of one of the intended targets. This initial target kicks off the collection process. You can configure up to five Delinea Secret Server Auto-Discovery credentials.

The standard Delinea Secret Server integration requires configuring a scan credential with the name of a specific secret. This secret then functions as the authentication credentials for each of the hosts in the target list. You must enter the target list when you begin configuring the scan. You may also need to configure several different credentials in the scan if the various scan targets use different accounts to authenticate.

In contrast, Delinea Secret Server Auto-Discovery allows you to enter a search query to collect multiple accounts. It automatically configures these accounts and their respective machines as scan targets with credentials. It associates the scan targets individually with their respective accounts.



Collection

The initial collection of accounts occurs once on the arbitrary target/host appear in the target settings of the scan policy. Logs for the initial collection are located in the **Debugging Log Report** plugin output on this host in the following logs:

- Database = `pam_database_auto_collect.nbin~Delinea Secret Server Auto-Discovery`

- SSH = `pam_ssh_auto_collect.nbin~Delinea Secret Server Auto-Discovery`
- Windows = `pam_smb_auto_collect.nbin~Delinea Secret Server Auto-Discovery`

Adding targets to the scan with credentials

After the initial collection, the integration automatically adds the hosts and necessary knowledge base (KB) entries for an authenticated scan.

Logs from this stage are located in the Debugging Log Report plugin output on this host in the following logs:

- Database = `pam_database_auto_collect.log`
- SSH = `pam_ssh_auto_collect.log`
- Windows = `pam_smb_auto_collect.log`

To automatically add a target to the scan, the integration must collect an account that includes a **Machine** field containing either an IP address or a resolvable hostname. If a machine is not a valid IP address or resolvable hostname, it does not add the host to the scan. In this case errors from the function `fqdn_resolv()` trigger the creation of separate detailed logs:

- Database = `pam_database_auto_collect_resolv_func.log`
- SSH = `pam_ssh_auto_collect_resolv_func.log`
- Windows = `pam_smb_auto_collect_resolv_func.log`

Querying for Accounts

You must provide a query defining the exact set of accounts to use for the scan. The Delinea Secret Server Auto-Discovery credential gives a flexible set of options for how to select these accounts. It is essential to know how to construct a query for accounts to use Delinea Secret Server Auto-Discovery.

The following table describes the possible combinations of query values and their effects.

Query Values	Effect
Query Mode: Simple **Folder:** 10 **Search Field:** (empty)	Use all accounts contained in the folder with ID 10. GET

Query Values	Effect
Search Text: (empty) **Exact Match:** false	`/v1/secrets/lookup?filter.folderId=10`
Query Mode: Simple **Folder:** (empty) **Search Field:** (empty) **Search Text:** tenable **Exact Match:** false	Use all accounts with “tenable” in the name. GET `/v1/secrets/lookup?filter.searchText=tenable`
Query Mode: Simple **Folder:** (empty) **Search Field:** notes **Search Text:** tenable **Exact Match:** false	Use all accounts that contain “tenable” in the notes. GET `/v1/secrets/lookup?filter.searchText=tenable&filter.searchField=notes`
Query Mode: Simple **Folder:** (empty) **Search Field:** notes **Search Text:** tenable **Exact Match:** true	Use all accounts whose “notes” field ONLY contains “tenable.” GET `/v1/secrets/lookup?filter.searchText=tenable&filter.searchField=notes&exactMatch=true`
Query Mode: Advanced **Query String:** filter.folderId=10&includeInactive=true	Use folder ID 10, and include inactive secrets. GET `/v1/secrets/lookup?filter.folderId=10&includeInactive=true` .

If using the **Advanced** query mode, the documentation on “Lookup Secrets with Search” contains a full list of parameters that can be used in the query string.

> **Note:** Advanced query strings must be URL-encoded (for example, replacing space characters with `%20`).

The initial query uses the “Lookup Secrets with Search” method of the Delinea Secret Server REST API. You can find an exact API reference in the Secret Server web interface under **Administration** > **REST API Guide**, or in the Delinea online help.

Folder ID is the integer ID of the folder within Delinea Secret Server. A folder ID is visible in its URL when the folder is open in a web browser. For example, the folder ID is **10** if its URL displays `https://SECRETSERVER/app/#/secrets/view/folder/10` , then the folder ID is **10**.

Privilege Escalation

The Delinea Secret Server Auto-Discovery integration supports privilege escalation. If login and escalation use two different credentials (for example, using an escalation method of `su`), then you must enter a separate query to collect the escalation accounts. Otherwise, you can leave the escalation query fields empty. For example, with sudo escalation the authenticated user would enter their own password to escalate. In all cases, you may optionally specify a user for escalation.

Limitations

It is only possible to use one account per host. If the search collects multiple accounts with the same machine, the first account that the search returns. Additionally, the **Debugging Log Report** includes a warning in the collection phase logs. Generally, Tenable recommends configuring scans to collect only a single account per machine to reduce the number of unnecessary requests.

A credential is limited to a single target authentication protocol. Delinea Secret Server Auto-Discovery is an authentication method of the SSH, Windows, or Database credential, so it is not possible to configure a single credential that collects both SSH and Windows accounts or targets.

You cannot use secrets with SSH private key authentication in the same credential as secrets with password authentication, because you must select the **Use Private Key** option that applies to the entire credential. To use both private keys and password authentication, configure separate Delinea SSH Auto-Discovery credentials.

For Auto-Discovery to use a secret, it must have a **Machine** or **Server** field defining the secret's associated address or hostname.

Database Auto-Discovery

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

Database authentication requires additional data entries that are specific to the database type that is targeted. For example, to authenticate to an Oracle database, you must specify not only a username and password, but also port, service type, authentication type and database name.

In some cases, these values may be pulled from the Auto-Discovery process. For example, an Oracle Database account created with the **Oracle Account** contains **port** and **database** fields, that do not need to be entered manually. However, the **Auth Type** and **Service Type** fields must entered manually.

Generally, Delinea Secret Server Auto-Discovery can dynamically use **port** and **database** fields defined in the secret, but they can also be entered manually. Fields other than **port** and **database** may need to be entered manually.

> **Note:** All Database Types in Tenable are supported (Oracle, DB2, Cassandra, MySQL, PostgreSQL, Sybase ASE, MongoDB, and SQL Server).

View the following tables for necessary fields and the database types they apply to.

Oracle

Field name	Description	Field value
AuthType	Method to authenticate to database.	SYSDBA or SYSOPER or NORMAL
Database	Instance or database name.	Example: orcl
Port	The port database instance is running on.	Example: 1521
ServiceType	Type of service on database.	SID or SERVICE_NAME

MongoDB

Field name	Description	Field value
Database	Instance or database name.	Example: MongoDB 5
Port	The port database instance is running on.	Example: 27017

PostgreSQL

Field name	Description	Field value
Database	Instance or database name.	Example: Postgres
Port	The port database instance is running on.	Example: 5432

Cassandra

Field name	Description	Field value
Port	The port database instance is running on.	Example: 9042

DB2

Field name	Description	Field value
Database	Instance or database name.	Example: DB2_admin
Port	The port database instance is running on.	Example: 50000

MySQL

Field name	Description	Field value
Port	The port database instance is running on.	Example: 3306

SQL Server

Field name	Description	Field value
AuthType	Method to authenticate to database.	Windows or SQL
Database	Instance or database name.	Example: SQLEXPRESS
Port	The port database instance is running on.	Example: 1433

To configure Database auto-discovery for Tenable Vulnerability Management or Tenable Nessus:

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 **Settings** pane appears.

10. Click the **Database** option.

    The **Database** options appear.

11. In the **Database Type** drop-down box, select **Cassandra**, **Oracle**, **DB2**, **MongoDB**, **PostgreSQL**, **MySQL**, **SQL Server**, or **Sybase ASE**.

12. In the **Auth Type** drop-down box, click **Delinea** Secret Server.

    The Delinea Secret Server options appear.

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

Option	Description	Required
Delinea Host	The Delinea Secret Server host to pull the secrets from.	Yes
Delinea Port	The Delinea Secret Server Port for API requests. By default, Tenable uses 443.	Yes

Option	Description	Required
Delinea Authentication Method	Indicates whether to use credentials or an API key for authentication. By default, **Credentials** is selected.	Yes
Delinea Login Name	The username to authenticate to the Delinea server.	Yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the provided Delinea Login Name.	Yes
Delinea API Key	The API key generated in the Secret Server user interface. This setting is required if the API Key authentication method is selected.	Yes
Query Mode	Choose to query accounts using pre-set fields or by constructing a string of URL query parameters. By default, **Simple** is selected.	Yes
Folder ID	Query accounts with the given folder ID. This option is only available if query mode is set to **Simple**.	No
Search Text	Query accounts matching the given search text. This option is only available if query mode is set to **Simple**.	No
Search Field	The field to search using the given search text. If not specified, the query will search the `name` field. This option is only available if query mode is set to **Simple**.	No
Exact Match	Perform an exact match against the search text. By default, this is unselected. This option is only available if query mode is set to **Simple**.	No

Option	Description	Required
Query String	Provide a string of URL query parameters. This option is only available if query mode is set to **Advanced**, and in that case it is required.	Yes
Use Private Key	Use key-based authentication for SSH connections instead of password authentication.	No
Use SSL	Use SSL for secure communications.	Yes
Verify SSL Certificate	Verify the Delinea Secret Server SSL certificate.	No

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.

SSH Auto-Discovery

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

To configure SSH auto-discovery for Tenable Vulnerability Management or Tenable Nessus:

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.

    The **Host** options appears.

11. Select **SSH**.

    The **Settings** pane appears.

12. In the **Auth Type** drop-down box, click **Tenable for Delinea Secret Server**.

    The **Tenable for Delinea Secret Server** options appear.

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

Option	Description	Required
Delinea Host	The Delinea Secret Server host to pull the secrets from.	Yes
Delinea Port	The Delinea Secret Server Port for API requests. By default, Tenable uses 443.	Yes
Delinea Authentication Method	Indicates whether to use credentials or an API key for authentication. By default, **Credentials** is selected.	Yes
Delinea Login Name	The username to authenticate to the Delinea server.	Yes

Option	Description	Required
Delinea Password	The password to authenticate to the Delinea server. This is associated with the provided Delinea Login Name.	Yes
Delinea API Key	The API key generated in the Secret Server user interface. This setting is required if the API Key authentication method is selected.	Yes
Query Mode	Choose to query accounts using pre-set fields or by constructing a string of URL query parameters. By default, **Simple** is selected.	Yes
Folder ID	Query accounts with the given folder ID. This option is only available if query mode is set to **Simple**.	No
Search Text	Query accounts matching the given search text. This option is only available if query mode is set to **Simple**.	No
Search Field	The field to search using the given search text. If not specified, the query will search the `name` field. This option is only available if query mode is set to **Simple**.	No
Exact Match	Perform an exact match against the search text. By default, this is unselected. This option is only available if query mode is set to **Simple**.	No
Query String	Provide a string of URL query parameters. This option is only available if query mode is set to **Advanced**, and in that case it is required.	Yes
Use Private Key	Use key-based authentication for SSH connections instead of password authentication.	No

Option	Description	Required
Use SSL	Use SSL for secure communications.	Yes
Verify SSL Certificate	Verify the Delinea Secret Server SSL certificate.	No
Delinea Elevate Privileges With	The privilege escalation method to use to increase users' privileges after initial authentication. Multiple options for privilege escalation are supported, including su, su+sudo and sudo. Selecting a privilege escalation method provides options to configure an escalation query, similar to “query mode” and its related options. These fields must only be completed if using a separate account for escalation than initial login (for example, “su”).	Yes

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.

Windows Auto-Discovery

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

To configure Windows auto-discovery for Tenable Vulnerability Management or Tenable Nessus:

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, enter an initial target in the target list. (This is arbitrary and only used to start the initial collection.) Valid options include the IP address of the scanner or the address of just one of the intended targets.

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 **Delinea** Secret Server.

    The Delinea Secret Server options appear.

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

Option	Description	Required
Delinea Host	The Delinea Secret Server host to pull the secrets from.	Yes
Delinea Port	The Delinea Secret Server Port for API requests. By default, Tenable uses 443.	Yes

Option	Description	Required
Delinea Authentication Method	Indicates whether to use credentials or an API key for authentication. By default, **Credentials** is selected.	Yes
Delinea Login Name	The username to authenticate to the Delinea server.	Yes
Delinea Password	The password to authenticate to the Delinea server. This is associated with the provided Delinea Login Name.	Yes
Delinea API Key	The API key generated in the Secret Server user interface. This setting is required if the API Key authentication method is selected.	Yes
Query Mode	Choose to query accounts using pre-set fields or by constructing a string of URL query parameters. By default, **Simple** is selected.	Yes
Folder ID	Query accounts with the given folder ID. This option is only available if query mode is set to **Simple**.	No
Search Text	Query accounts matching the given search text. This option is only available if query mode is set to **Simple**.	No
Search Field	The field to search using the given search text. If not specified, the query will search the `name` field. This option is only available if query mode is set to **Simple**.	No
Exact Match	Perform an exact match against the search text. By default, this is unselected. This option is only available if query mode is set to **Simple**.	No

Option	Description	Required
Query String	Provide a string of URL query parameters. This option is only available if query mode is set to **Advanced**, and in that case it is required.	Yes
Use Private Key	Use key-based authentication for SSH connections instead of password authentication.	No
Use SSL	Use SSL for secure communications.	Yes
Verify SSL Certificate	Verify the Delinea Secret Server SSL certificate.	No

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.