Tenable.sc for Thycotic Integration Guide

Last Revised: August 19, 2019

Table of Contents

Introduction

This document describes how to deploy Tenable™ Tenable.sc for integration with Thycotic Secret Server. Please email any comments and suggestions to 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 Thycotic Secret Server with Tenable.sc, administrators now have even more choice and flexibility for reducing the credentials headache.

The combined Tenable-Thycotic solution works when a Tenable.sc scan policy is configured to query a Thycotic Secret Server for privileged credentials. At the time of the scan, Tenable.sc requests the privileged account credentials from Thycotic. Thycotic sends the privileged account credentials to Tenable.sc and the provided credentials are then used to log in to the target system to identify vulnerabilities and misconfigurations.

By integrating Tenable.sc with Thycotic Secret Server, you can:

- Store credentials in Thycotic Secret Server instead of managing and updating the credentials directly within a Tenable solution.
- Reduce the time and effort needed to document credential storage within the organizational environment.
- Automatically enforce security policies within specific departments or for specific business unit requirements, simplifying your compliance process.
- Reduce the risk of unsecured privileged accounts and credentials across the enterprise.

Integration Requirements

You must meet the following minimum version requirements to integrate Tenable Tenable.sc with Thycotic Secret Server:

- Thycotic Secret Sever version 8.9 or later
- Tenable.sc 5.3.2 or later

Note: The integration requires enabling the Thycotic Secret Server web services API, which is available in Secret Server Professional and the hosted version of Secret Server.

Integrate with Thycotic Secret Server

You can configure Tenable.sc to perform credentialed network scans of Windows and Linux systems using Thycotic's password management solution. Credentials are configured similarly to other credentialed network scans.

Configure Windows Credentials

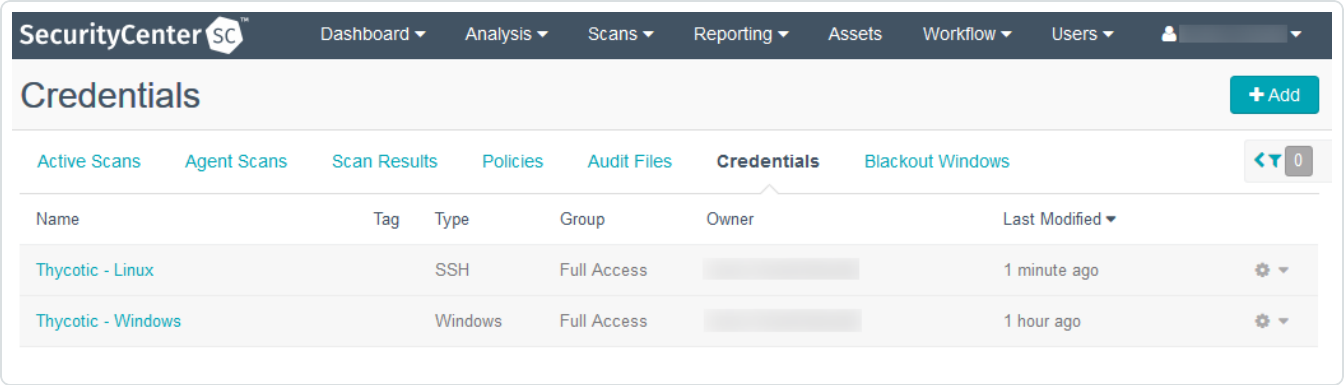
Configure SSH/Linux Credentials

Configure a Credentialed Scan

Configure Windows Credentials

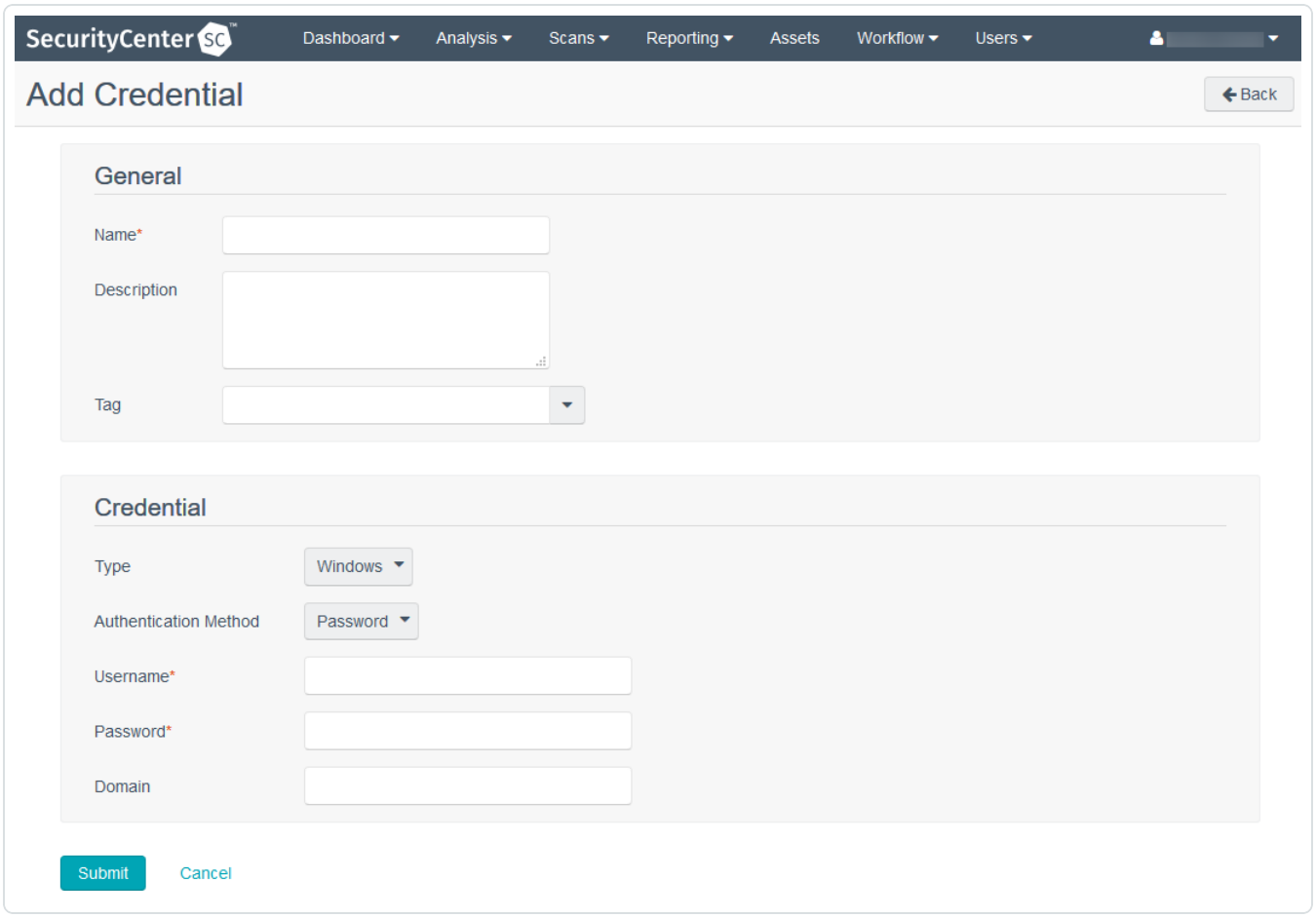
1. Log in to Tenable.sc.
2. In the top navigation bar, click **Scanning > Credentials** (administrator users) or **Scans > Credentials** (organizational users).

   The Credentials page appears.

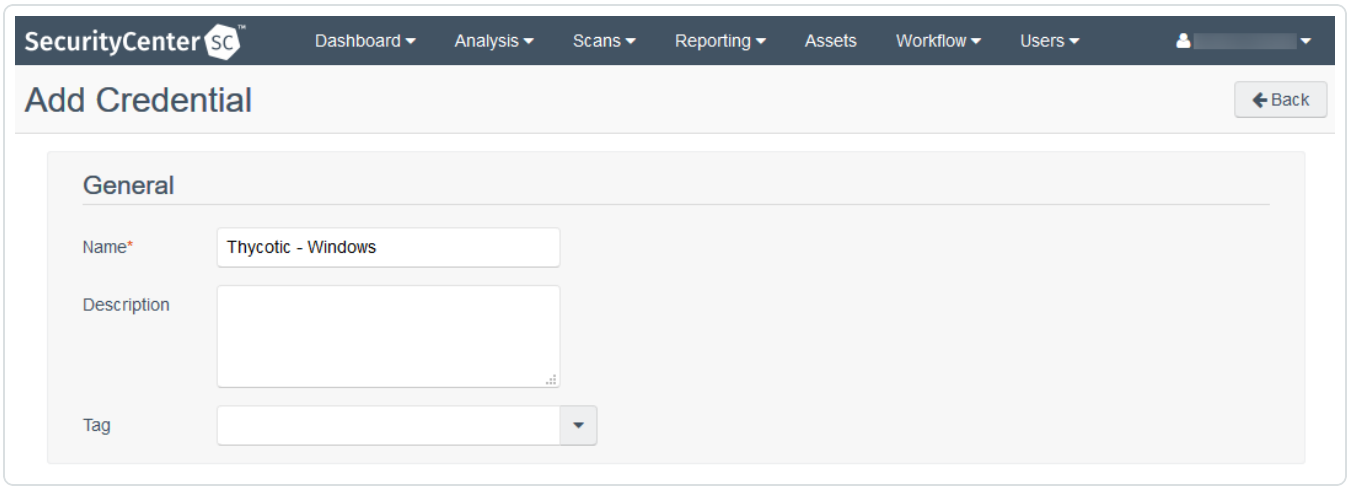


3. Click **Add**.

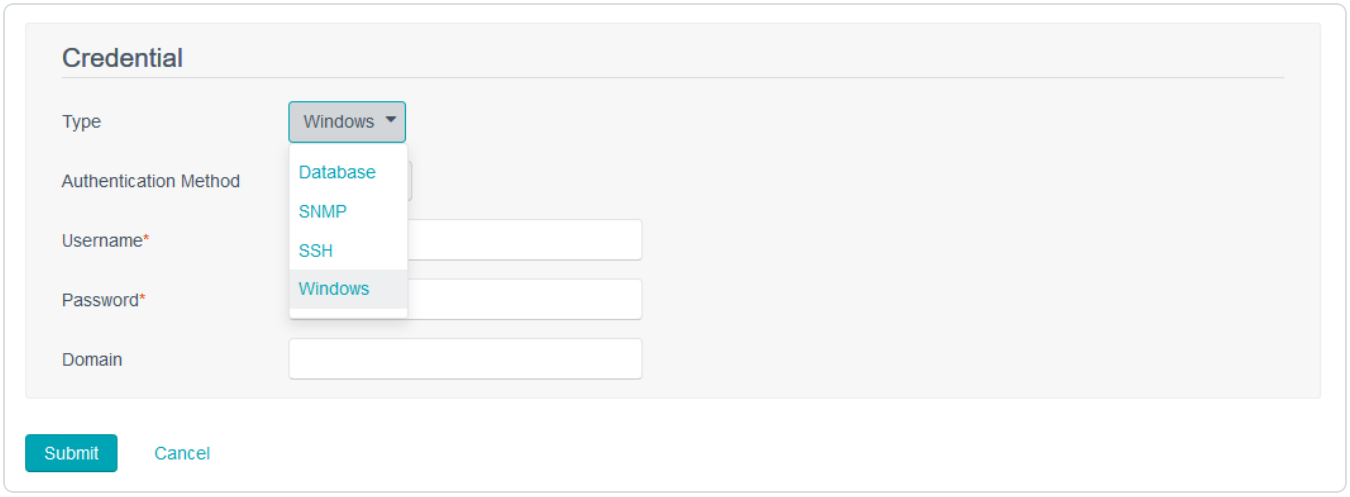
   The Add Credential page appears.



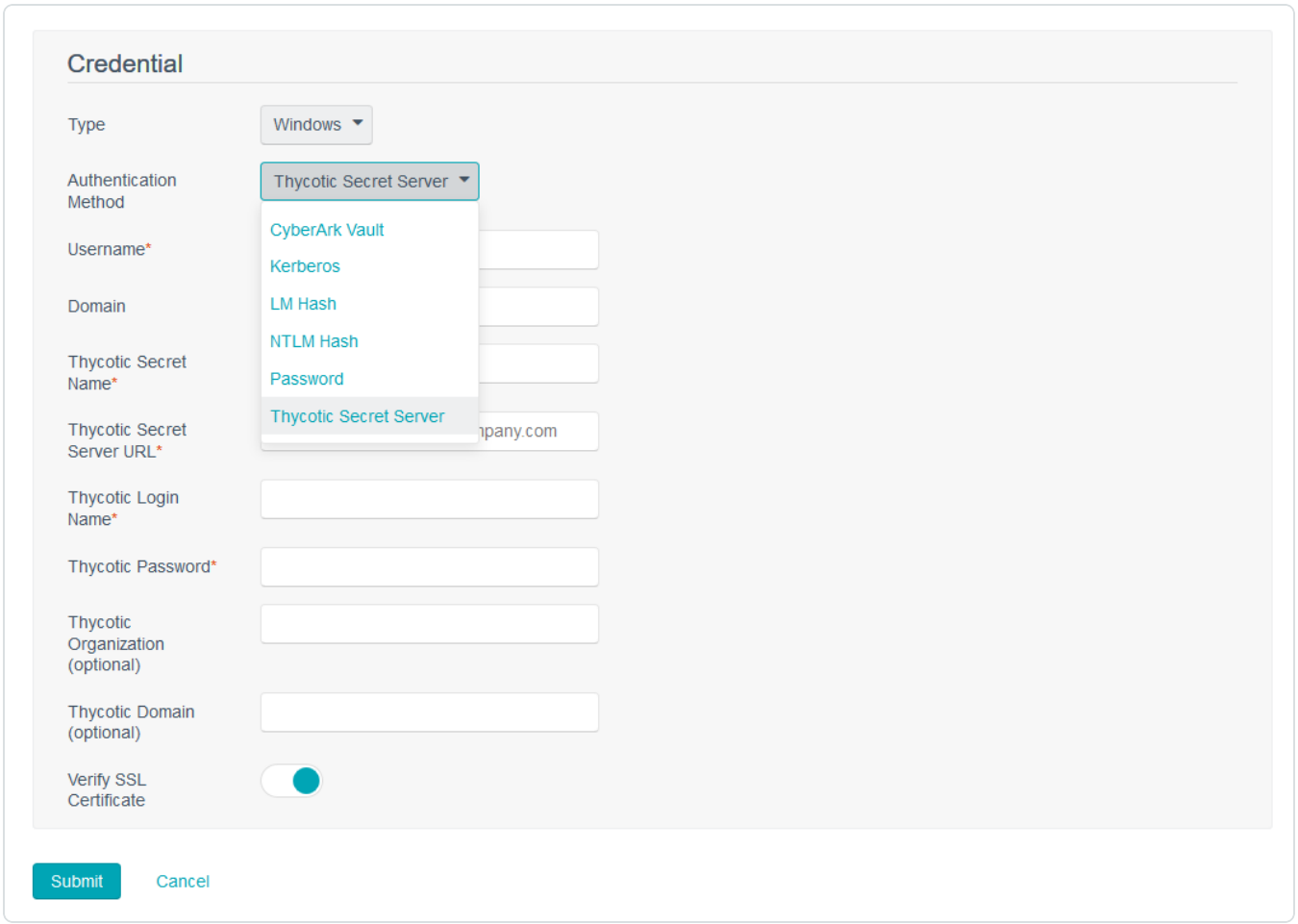
4. In the **General** section, type a **Name** and **Description** for the credentials.
5. (Optional) Select a **Tag**.



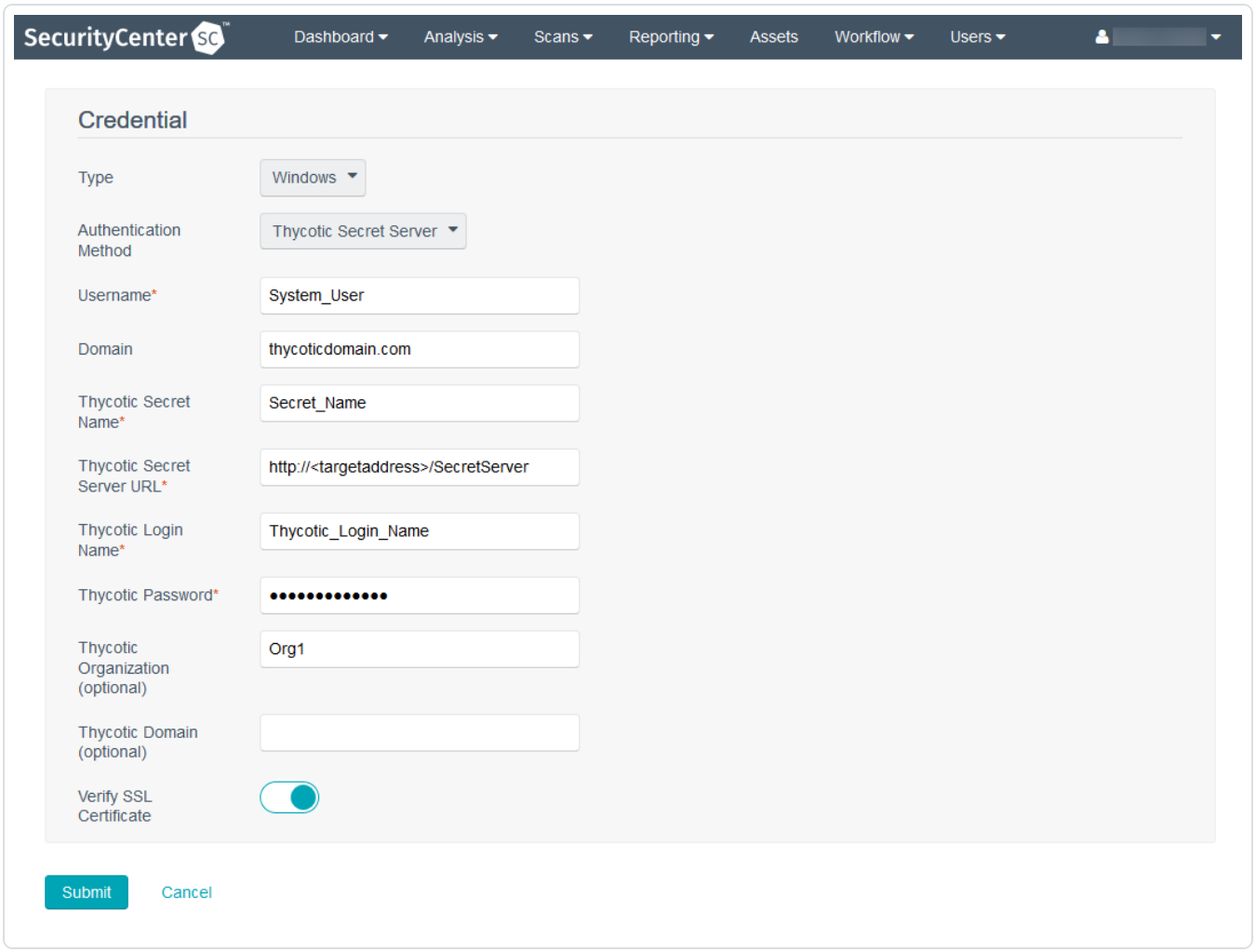
6. In the **Credential** section, in the **Type** drop-down box, select **Windows**.



7. In the **Authentication Method** drop-down box, select **Thycotic Secret Server**.



8. Configure each option for Windows configuration. Refer to Thycotic Secret Server Windows Options for a description of each option.



9. Click **Submit** to finalize the changes.

Thycotic Secret Server Windows Options

The following table describes the options to configure when using Thycotic Secret Server as the **Authentication Method** for Windows credentials.

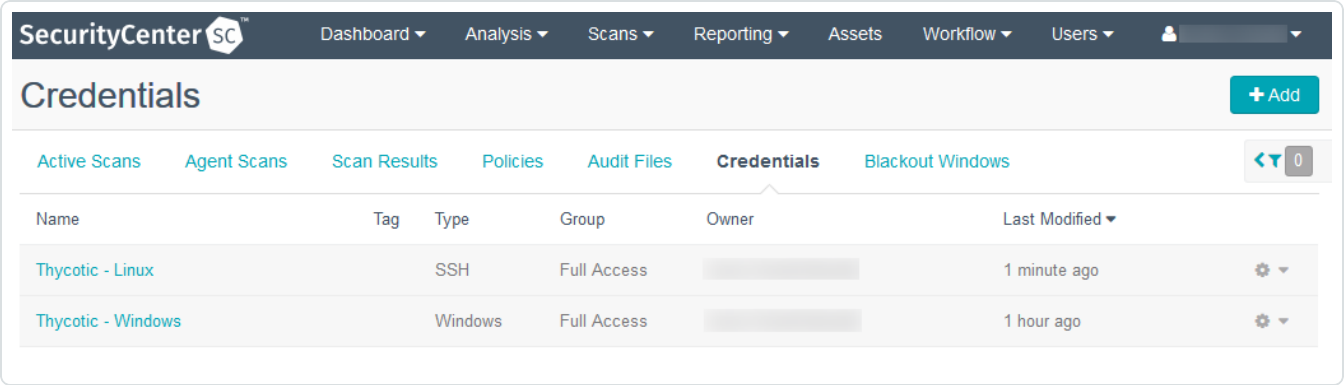
Option	Description
Username	(Required) The username for a user on the target system.
Domain	(Optional) The domain of the username, if set on the Thycotic server.

Thycotic Secret Name	(Required) The Secret Name value on the Thycotic server.
Thycotic Secret Server URL	(Required) The value you want Tenable.sc to use when setting the transfer method, target, and target directory for the scanner. Find the value on the Thycotic server, in **Admin > Configuration > Application Settings > Secret Server URL**. For example, if you type *https://pw.mydomain.com/SecretServer*, Tenable.sc determines it is an SSL connection, that *pw.mydomain.com* is the target address, and that */SecretServer* is the root directory.
Thycotic Login Name	(Required) The username used to authenticate to the Thycotic server.
Thycotic Password	(Required) The password associated with the **Thycotic Login Name** you provided.
Thycotic Organization	(Optional) In cloud instances of Thycotic, the value that identifies which organization the Tenable.sc query should target.
Thycotic Domain	(Optional) The domain, if set for the Thycotic server.
Verify SSL Certificate	If enabled, Tenable.sc verifies the SSL Certificate on the Thycotic server.

Configure SSH/Linux Credentials

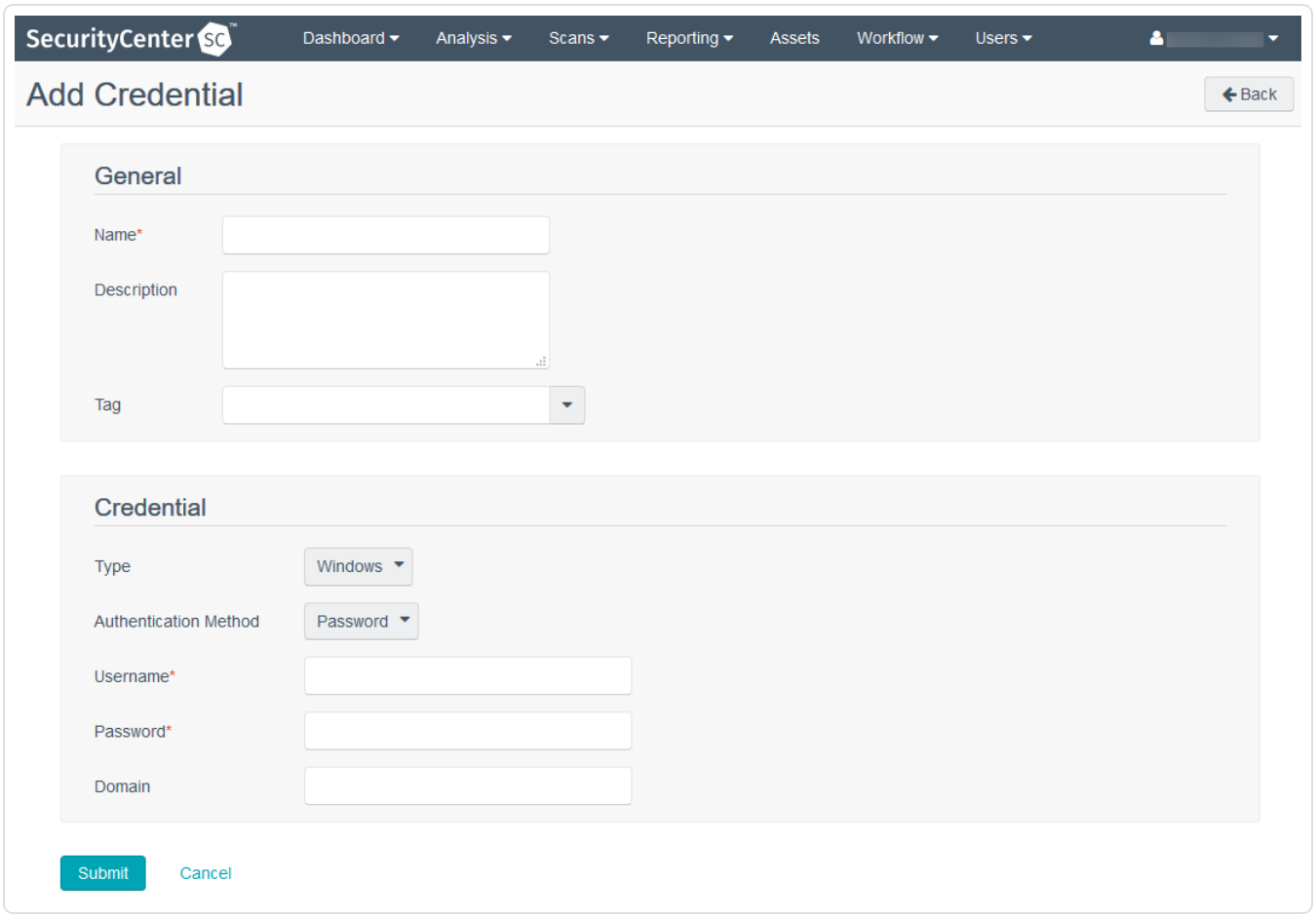
1. Log in to Tenable.sc.
2. In the top navigation bar, click **Scanning > Credentials** (administrator users) or **Scans > Credentials** (organizational users).

   The Credentials page appears.

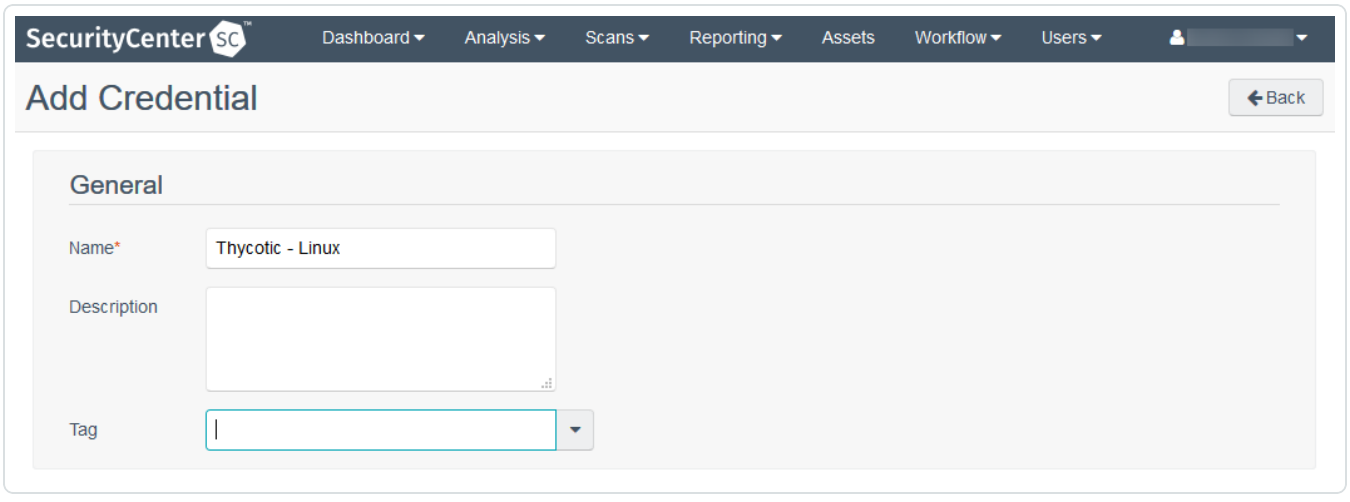


3. Click **Add**.

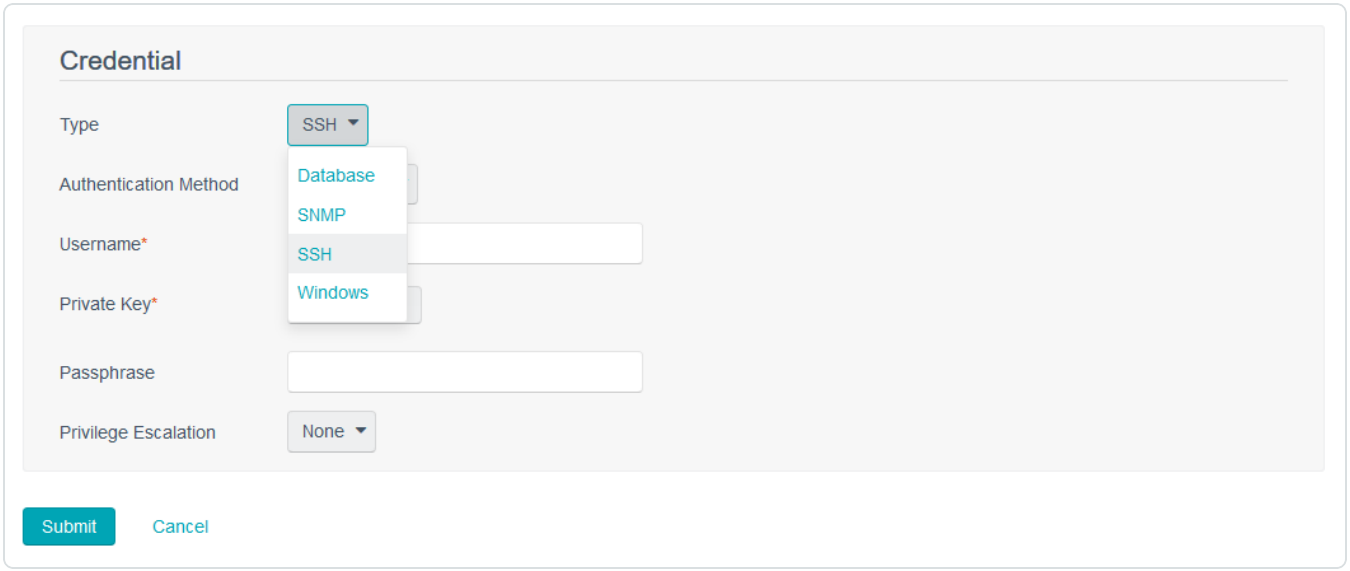
   The Add Credential page appears.



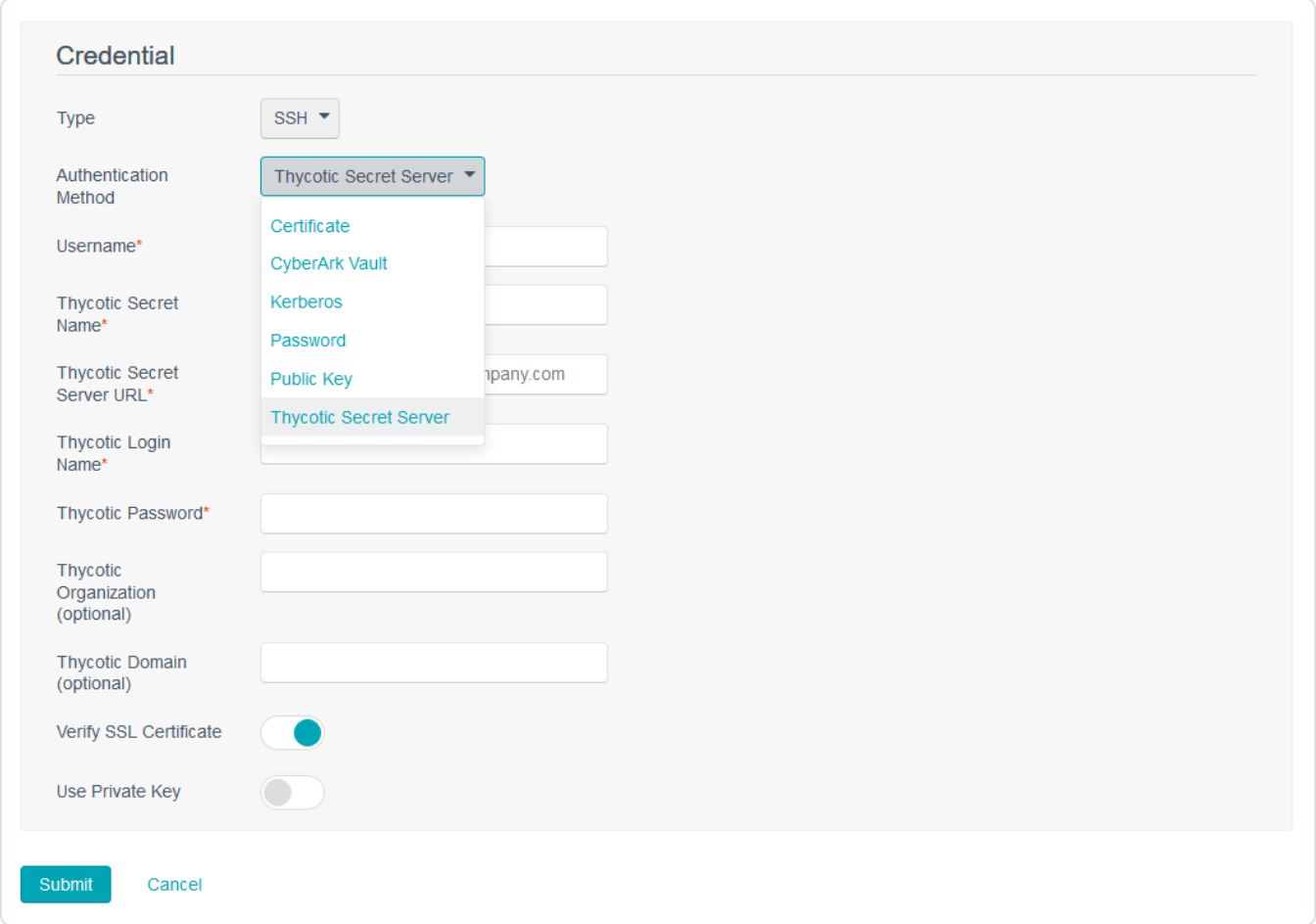
4. In the **General** section, type a **Name** and **Description** for the credentials.
5. (Optional) Select a **Tag**.



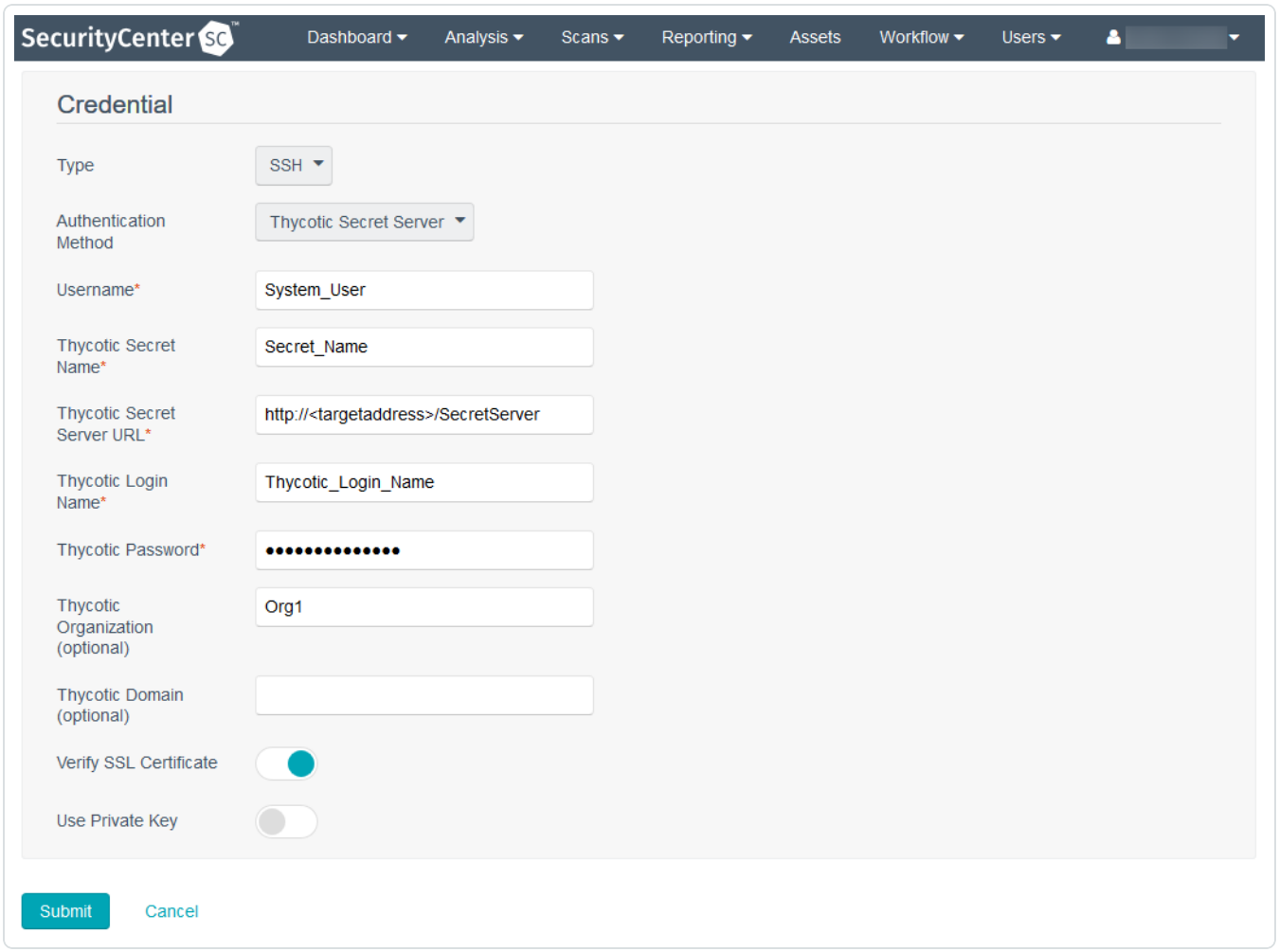
6. In the **Credential** section, in the **Type** drop-down box, select **SSH**.



7. In the **Authentication Method** drop-down box, select **Thycotic Secret Server**.



8. Configure each option for SSH configuration. Refer to Thycotic Secret Server SSH Options for a description of each option.



9. Click **Submit** to finalize the changes.

Thycotic Secret Server SSH Options

The following table describes the options to configure when using Thycotic Secret Server as the **Authentication Method** for SSH credentials.

Option	Description
Username	The username that is used to authenticate via ssh to the system.
Thycotic Secret Name	This is the value that the secret is stored as on the Thycotic server. It is referred to as the “Secret Name” on the Thycotic server.
Thycotic Secret Server URL	The value you want Tenable.sc to use when setting the transfer method, target, and target directory for the scanner. Find the value

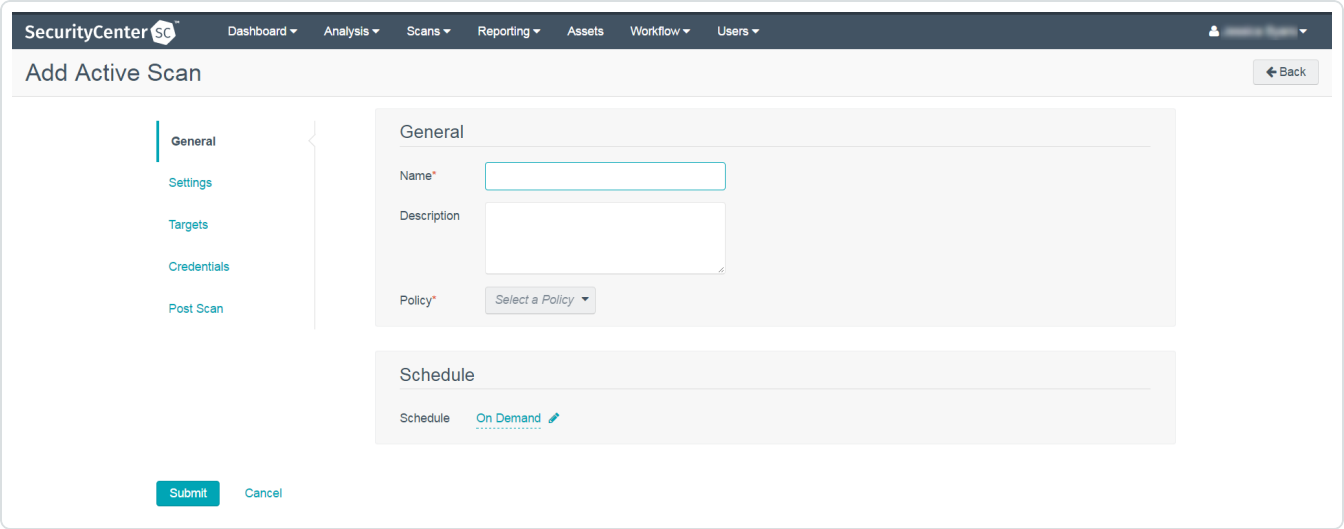
	on the Thycotic server, in **Admin > Configuration > Application Settings > Secret Server URL**. For example, if you type *https://pw.mydomain.com/SecretServer*, Tenable.sc determines it is an SSL connection, that *pw.mydomain.com* is the target address, and that */SecretServer* is the root directory.
Thycotic Login Name	The username used to authenticate to the Thycotic server.
Thycotic Password	The password associated with the **Thycotic Login Name** you provided.
Thycotic Organization (optional)	In cloud instances of Thycotic, the value that identifies which organization the Tenable.sc query should target.
Thycotic Domain (optional)	This is an optional value set if the domain value is set for the Thycotic server.
Use Private Key	If enabled, Tenable.sc uses key-based authentication for SSH connections instead of password authentication.
Verify SSL Certificate	If enabled, Tenable.sc verifies the SSL Certificate on the Thycotic server.
Thycotic elevate privileges with	The privilege escalation method you want to use to increase the user's 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. **Note:** For additional information about all of the supported privilege escalation types and their accompanying fields, see SSH in the Nessus User Guide.

Configure a Credentialed Scan

1. Log in to Tenable.sc.
2. In the top navigation bar, click **Scans > Active Scans**.

   The Active Scans page appears.
3. Click **Add**.

   The Add Active Scan page appears.



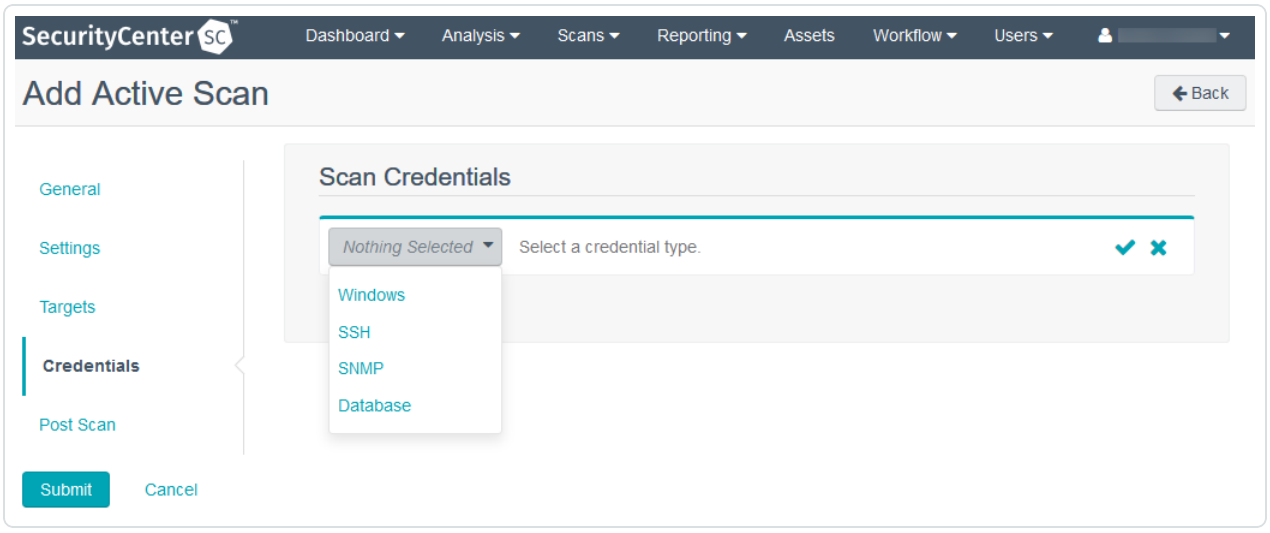
4. In the **General** section:
   1. Type a **Name** for the scan.
   2. (Optional) Type a **Description** for the scan.
   3. Select a **Policy** for the scan.
   4. (Optional) Select a **Schedule** for the scan.
5. In the **Settings** section:
   1. If prompted, select a **Scan Zone** for the scan.
   2. Select an **Import Repository** for the scan.
   3. Select a **Scan Timeout Action** for the scan.

4. Select a **Rollover Schedule** for the scan.
5. Enable or disable the **Advanced** options.

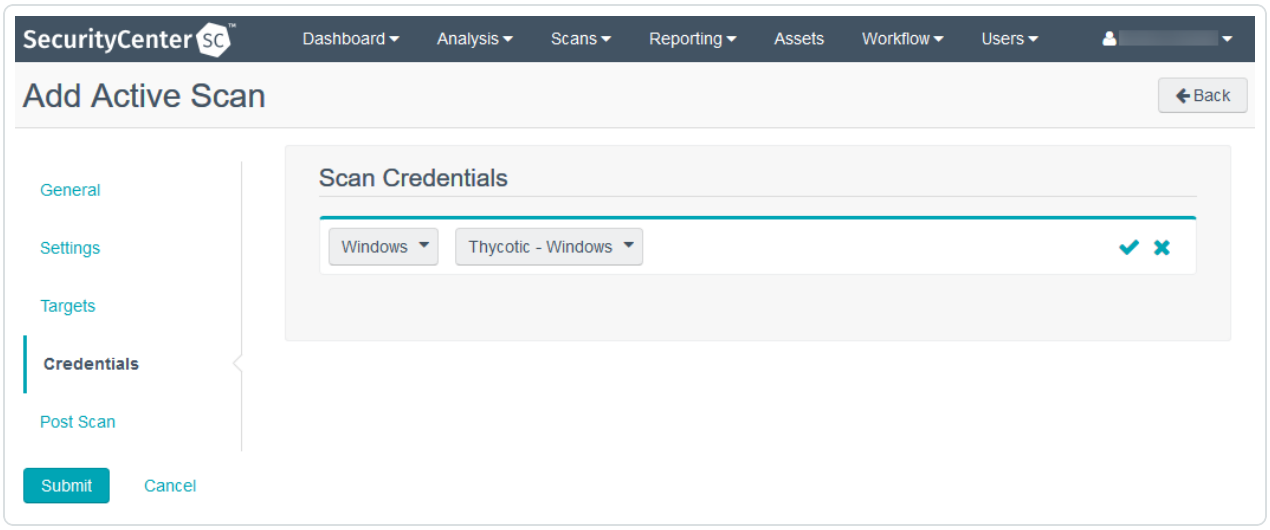
6. In the **Targets** section:
    1. Select a **Target Type** for the scan.

       The page updates to show the required options for that target type.
    2. Select one or more **Assets** and/or **IPs / DNS Names** for the scan.

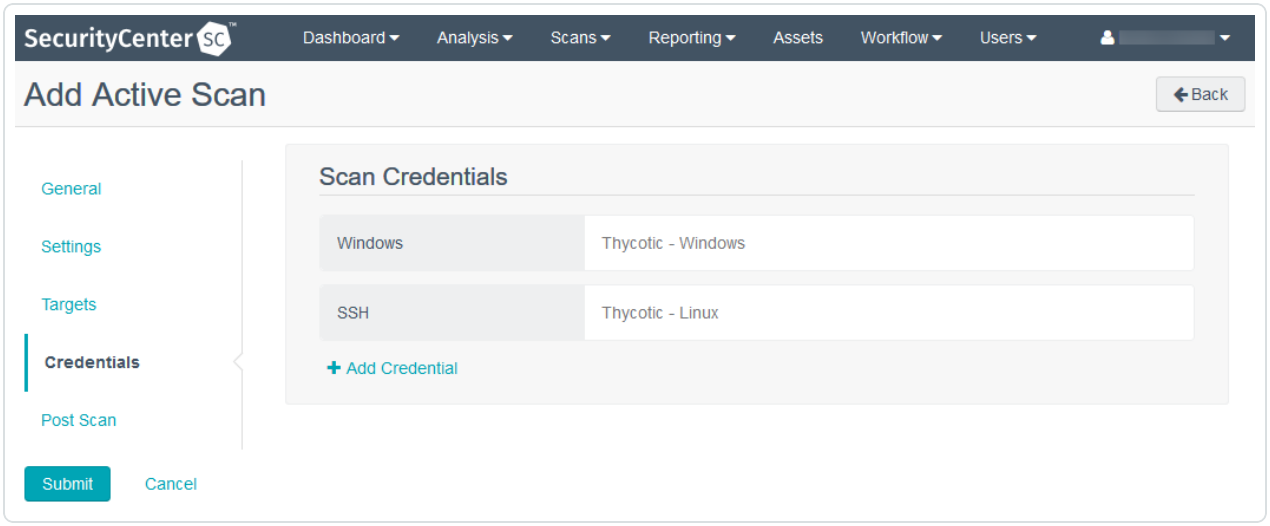
7. In the **Credentials** section, to configure credentialed scanning using your Thycotic credentials, click **Add Credential**.
    1. In the drop-down box, select **Windows** to use Windows credentials or **SSH** to use Linux credentials.



    2. In the drop-down box that appears to the right of the drop-down box in the previous step, select the name of the Thycotic credentials configured in step 4 of Configure Windows Credentials or step 4 of Configure SSH/Linux Credentials.



3. Click the check mark to save the credentials.
4. (Optional) Repeat step 7 to configure additional credentials.



8. In the **Post Scan** section:
    1. (Optional) If you previously added an email address to your account profile and you want to configure email notifications, enable or disable **E-Mail Me on Launch** or **E-Mail Me on Completion**.
    2. (Optional) If you want to configure automatic report generation, click Add Report. For more information, see Add a Report to a Scan.
9. Click **Submit**.

Verify Integration

To verify the integration succeeded, you can initiate a scan using a custom policy containing only plugins that validate access to Windows and Linux targets. This policy is known as a Quick Credential Debug (QCD) scan. QCD enables administrators to perform quick credential tests without performing a full a vulnerability scan.

A QCD scan policy for Windows and Linux includes the following plugins (plugin ID numbers are in parentheses):

- (10394) Microsoft Windows SMB Log In Possible
- (12634) Authenticated Check: OS Name and Installed Package Enumeration
- (21745) Authentication Failure - Local Checks Not Run

Plugin 10394 verifies authentication to Windows targets, plugin 12634 verifies authentication to Linux targets by attempting to authenticate via SSH and enumerate a list of installed packages, and plugin 21745 reports authentication failures along with an audit trail useful for debugging.

Refer to the Tenable.sc User Guide for information on how to create a custom scan policy containing only these three plugins.

- Add a Scan Policy
- Configure Plugin Options
- Start or Pause a Scan

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 21,000 customers worldwide, organizations trust Tenable for proven security innovation. Tenable customers range from Fortune Global 500 companies, to the global public sector, to mid-sized enterprises 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.