

CREDENTIALLED SCANS

OVERVIEW

This document describes credentialed scans in Tenable.io. Tenable.io allows for multiple scan settings, among them are the ability to run credentialed scans. Credentialed scans, also called authenticated scans, grant a Tenable.io scanner local access through the use of credentials to log into devices and examine them for vulnerabilities and misconfigurations from the inside out. Credentialed scans can perform any operation that a local user can perform with the level of scanning dependent upon the privileges granted to the user account (for example, root or administrator access). The more privileges the account has, the more thorough the scan results.

BENEFITS OF CREDENTIALLED SCANS

- More vulnerability detections: Discover many more vulnerabilities that can't be discovered without authenticating to the target(s).
- More accuracy: Credentialed scanning provides more detailed information about remotely-discovered vulnerabilities.
- Less false positives: The high accuracy of credentialed scans reduces the amount of false positives, meaning you spend less time chasing down issues that might not be relevant.
- Find localized vulnerabilities: Some vulnerabilities are not accessible over the network, but present themselves in end-user software ranging from web browsers, PDF readers and office suites. With a credentialed scan, Tenable.io can find vulnerabilities that require user interaction to enumerate vulnerabilities in local software.
- Understand risk: With visibility into more vulnerabilities, misconfigurations and missing patches than uncredentialed scans you can make better vulnerability prioritization decisions based on all available information.

ADDITIONAL RESOURCES

[Documentation](#)

[Tenable.io Scanning Best Practices](#)

Blog:
[How to protect scanning credentials](#)

Blog:
[5 Ways to protect scanning credentials for Windows Hosts](#)

Blog:
[5 Ways to protect scanning credentials for Linux, macOS and Unix hosts](#)

Webinar:
[Overcoming the Challenges of Credentialed Scanning](#)

Video:
[Launch a Credentialed Scan in Tenable.io](#)


Tenable.io also integrates with leading Privileged Access Management (PAM) solutions to streamline privileged access to use in credentialed vulnerability scans. Integrations are available with [CyberArk](#), [BeyondTrust](#), [Thycotic](#), [HashiCorp](#), [Centrify](#) and [Arcon](#).



CREDENTIALLED SCANS IN TENABLE.IO

Review [Add a Credential to a Scan](#) or [Create a Managed Credential](#) in the [Tenable.io user guide](#).

CREATE A MANAGED CREDENTIAL

1. In the upper-left corner, click the  button. The left navigation pane appears.
2. Click Settings.
3. Click the Credentials widget
4. Click the "+ Create Credentials" button to the right of the Credentials title. The credential form plan appears
5. Select the type of Credentials you want to create (Window, SSH, etc.)
6. Type your credentials and then select the appropriate permissions for the group/user that you want to allow access to.
7. Click Create.

ADD CREDENTIALS TO A SCAN

1. [Create](#) or [edit](#) a scan
2. In the left navigation menu, click Credentials. The Credentials pane appears.
3. Next to add credentials, click the + button. The Select Credential pane appears.
4. Do one of the following: Add an existing managed credential, Add a scan specific credential, Add a new managed credential.
5. Click Save to save your credential changes. Tenable.io will close the Settings plane and adds credentials to the credential table for the scan.
6. Do one of the following:
 - a. If you want to save without launching the scan, click Save. Tenable.io saves the scan.
 - b. If you want to save and launch a scan immediately, click Save & Launch. Tenable.io saves and launches the scan.