



# Tenable Vulnerability Management Security Best Practices Guide

---

Last Revised: October 16, 2024



## Table of Contents

<b>Overview</b> .....	<b>3</b>
<b>Administrator Accounts</b> .....	<b>4</b>
<b>Credentials Used By Tenable</b> .....	<b>5</b>
<b>Multi-Factor Authentication</b> .....	<b>6</b>
<b>SAML Single Sign-On (SSO)</b> .....	<b>7</b>
<b>Linking Keys</b> .....	<b>8</b>
<b>API Keys</b> .....	<b>9</b>
<b>Activity Logs</b> .....	<b>10</b>
<b>Service Level Agreement</b> .....	<b>11</b>
<b>Account Lockout and Unlocking Accounts</b> .....	<b>12</b>
<b>Vulnerability Priority Rating</b> .....	<b>13</b>
<b>Vulnerability Management KPIs</b> .....	<b>14</b>

# Overview

---

This document contains guidelines for securely configuring Tenable Vulnerability Management. If you have any questions or concerns related to this document, contact [security@tenable.com](mailto:security@tenable.com).

The following sections include guidelines and best practices for securing Tenable Vulnerability Management:

- [Administrator Accounts](#)
- [Credentials Used By Tenable](#)
- [Multi-Factor Authentication](#)
- [SAML Single Sign-On \(SSO\)](#)
- [Linking Keys](#)
- [API Keys](#)
- [Activity Logs](#)
- [Service Level Agreement](#)
- [Account Lockout and Unlocking Accounts](#)
- [Vulnerability Priority Rating](#)
- [Vulnerability Management KPIs](#)

# Administrator Accounts

---

Tenable provides several default [roles](#) by default. Administrators have the highest level of access to an organization's systems and data. An administrator can perform a wide range of tasks such as create new user accounts, modify system configurations, and delete data. As a result, administrators have potentially destructive capabilities and pose a significant security risk if their credentials are compromised. Administrator accounts that are not Single Sign-on enabled must be protected with a strong password that is kept in a password vault and Multi-Factor Authentication (MFA) must be enforced.

To mitigate this risk, it is important to limit the number of users who have admin privileges to only those who truly need it to perform their job responsibilities. This typically includes IT staff, system administrators, and senior management. By limiting the number of users with admin access, organizations can reduce the likelihood of insider threats or accidental misuse of admin privileges.

## Credentials Used By Tenable

---

Many Tenable sensors (for example, Tenable Nessus and Tenable Web App Scanning) require the usage of various types of system and application credentials to perform assessments to the deepest possible levels.

Your organization is responsible for securing the credentials kept within your environment. Best practices apply in these cases, and must correlate to your organization's appropriate risk appetite. For example:

- Many customers utilize Privileged Access Management (PAM) solutions, which automatically rotate and secure credentials used by the Tenable Nessus scanner. Those without that capability, or a geographically and logically segmented network, may opt for other Tenable Nessus Agent solutions.
- Tenable Web App Scanning supports uploading of Selenium Files for authentication replay. These files are plaintext at rest and, when not stored in Tenable, you must secure them by some method of local encryption or stored in a secure vault.

Tenable encrypts scan credentials when they are stored within the platform. For more information, see <https://www.tenable.com/trust/assurance>.

## Multi-Factor Authentication

---

Multi-factor Authentication (MFA) offers enhanced security by requiring users to provide multiple forms of identification before accessing their accounts. It reduces the risk of unauthorized access, protects against phishing and brute force attacks, and ensures compliance with security regulations. MFA is easy to set up, making it an essential measure for safeguarding online accounts and sensitive data. For information about how to configure MFA, see [Configure Two-Factor Authentication](#) on the Tenable documentation portal.

## SAML Single Sign-On (SSO)

---

SAML offers single sign-on capability, improved security, and centralized identity management. It reduces password fatigue, improves user experience, and simplifies compliance auditing. You can configure Tenable Vulnerability Management to accept credentials from your SAML identity provider (IdP). Once SAML is enabled for a user, they can log in to Tenable Vulnerability Management directly through their identity provider, which automatically signs the user in and redirects them to the Tenable Vulnerability Management landing page.

**Note:** Once SAML is configured, an administrator must enable it for each user for whom they want to enforce SAML. The administrator must also disable the password login option to force the user to use SSO.

**Note:** Once SAML is configured for a user, they must log in using the IdP Tile or the URL provided in the SP metadata file (for example, cloud.tenable.com/SAML/XXXXXX) and log back out before they can access the **Sign in via SSO** link on the Tenable Vulnerability Management login page.

For more information about [adding](#), [editing](#), or [deleting](#) a SAML configuration, see the Tenable documentation portal.

For information about configuring SAML for Tenable products with specific IdPs, see the [Tenable SAML Quick Reference Guide](#).

## Linking Keys

---

Linking keys are secure tokens used to associate a Tenable Nessus Agent with a Tenable Nessus Manager or Tenable Vulnerability Management account. Traditional active scans originate from a Tenable Nessus scanner that reaches out to the hosts targeted for scanning, while agent scans run on hosts regardless of network location or connectivity and then report the results back to the manager (for example, Tenable Nessus Manager or Tenable Vulnerability Management) when network connectivity resumes.

Agents use linking keys to associate to the customer instance when the agent is first configured. Once the agent is associated with a customer, it maintains that association throughout the life of the agent. Therefore, if a linking key is regenerated, it does not affect agents that are already linked. If a linking key is regenerated, the old linking key can no longer be used to set up agents and you must use the new linking key.

For more information, see [Retrieve the Nessus Agent Linking Key](#).

To secure your linking key, there are several sensor settings that you can enable to suit specific use cases such as FIPS mode, SSL ciphers, and local encryption requirements. For more information, see the [Tenable Nessus User Guide](#).

# API Keys

---

API keys are associated with accounts on a customer instance and enable API access for all licensed Tenable Vulnerability Management products. API keys interact with licensed Tenable products and customer data within an instance. You must protect these keys by storing them in a secure password vault. API keys are scoped to the user's [role](#) and permission for which they are generated. Users with the Basic, Scan Operator, Standard, Scan Manager, or Administrator role can generate their own API keys. Users with Custom Roles can be prevented from generating or updating API keys and administrators can disable API access for any specific user who does not have the ability to manage User Access Control. Administrators can [generate API keys](#) for any user in the instance. For instructions on how to generate API Keys, see the [Generate API Keys](#) documentation.

Regenerating API keys replaces any existing API keys generated for a given account. If an API key is ever exposed, regenerate the key to revoke the exposed key and obtain new credentials. Be sure to copy the access and secret keys as soon as they are generated and store them in a password vault. After closing the browser tab, you cannot retrieve the keys from Tenable Vulnerability Management. Tenable recommends that your organization periodically rotates API keys in a manner that aligns with your organization's risk tolerance and operational requirements. Regular key rotation helps mitigate potential security risks and must be conducted as part of ongoing security hygiene practices.

# Activity Logs

---

In Tenable Vulnerability Management, user events are recorded in the activity log. To view the activity log, you must have the Administrator role.

Activity log events may include the following (subject to change):

Action	Description
<b>audit.log.view</b>	The system received and processed an audit-log request.
<b>session.create</b>	The system created a session for the user. A user login triggers this event.
<b>session.delete</b>	The session aged out, or the user ended a session.
<b>session.impersonation.end</b>	An administrator ended a session where they impersonated another user.
<b>session.impersonation.start</b>	An administrator started a session where they impersonated another user.
<b>user.authenticate.mfa</b>	Two-factor authentication was successful, and login was allowed.
<b>user.authenticate.password</b>	The user authenticated a session start using a password.
<b>user.create</b>	An administrator created a new user account.
<b>user.delete</b>	An administrator deleted a user account.
<b>user.impersonation.end</b>	An administrator stopped impersonating another user.
<b>user.impersonation.start</b>	An administrator started impersonating another user.
<b>user.logout</b>	The user logged out of their session.
<b>user.update</b>	Either an administrator or the user updated a user account.

You can use the [Activity Log API endpoint](#) to view audit events programmatically within an instance. You can also use [PyTenable](#) to interact with the audit log.

# Service Level Agreement

---

Service Level Agreements (SLAs) define an expected level of service by which measurements, metrics, or penalties can be established. SLA compliance is a critical component of a vulnerability management program. Your company's Information Security Policy must drive this SLA definition.

The Department of Homeland Security provides [10 resource guides](#) to help organizations implement business practices to reduce cyber risk. [Volume 4: Vulnerability Management](#) provides guidance for organizations to work with stakeholders to develop remediation timeframes that align with business goals.

## Account Lockout and Unlocking Accounts

---

Tenable Vulnerability Management locks you out if you attempt to log in and fail five consecutive times. Lockouts affect the user interface. If a user has the `api_permitted` authorization, API requests are still permitted. Users can unlock their account by resetting their password. For more information, see [Unlock your Account](#) on the Tenable documentation portal.

## Vulnerability Priority Rating

---

Vulnerability Priority Rating (VPR), the output of [Tenable Predictive Prioritization](#), helps organizations improve their remediation efficiency and effectiveness by rating vulnerabilities based on severity level – Critical, High, Medium, and Low – determined by two components: technical impact and threat. Technical impact measures the impact on confidentiality, integrity, and availability following exploitation of a vulnerability. It is equivalent to the CVSSv3 impact subscore.

The threat component reflects both recent and potential future threat activity against a vulnerability. Some examples of threat sources that influence VPR are public proof-of-concept (PoC) research, reports of exploitation on social media, emergence of exploit code in exploit kits and frameworks, references to exploitation on the dark web and hacker forums, and detection of malware hashes in the wild. Such threat intelligence is key in prioritizing those vulnerabilities that pose the most risk to an organization.

## Vulnerability Management KPIs

---

As with any good security project, one of the best ways to start is by establishing reasonable Key Performance Indicators (KPIs) to guide the security team and create realistic goals. Tenable recommends these five KPIs to get you started:

- Scan frequency: How often does your enterprise conduct assessments?
- Scan intensity: How many different scans are launched on a given scan day?
- Asset authentication: How does your enterprise measure assessment depth?
- Asset coverage: What proportion of the licensed assets are scanned in a 90-day period?
- Vulnerability coverage: What proportion of total vulnerability plugins are used in a 90-day period?

Once these KPIs are established, here are three ways security teams can start applying Predictive Prioritization and Vulnerability Priority Ratings (VPR) to their vulnerability management process:

- In the discovery phase, VPR can assist in classifying assets within the network by improving accuracy and helping to discover new IP addresses that are added.
- When scanning, VPR can be applied automatically. As the security team scans the network more frequently, the threat intelligence improves because there's more data to analyze in real time.
- During the patching process, VPR helps security teams provide a much-needed context to the IT professionals responsible for patching. As a result, the security teams can improve their ability to prioritize and allocate resources based on real-world risk.