Best Practices for Tenable Role-Based Access Control (RBAC)

Last Revised: June 10, 2026

Table of Contents

Welcome to the Tenable Role-Based Access Control Best Practices Guide

This guide explains how to plan, configure, and maintain role-based access control (RBAC) in Tenable Vulnerability Management. It is intended for platform administrators and security team leads who are responsible for managing user access in a shared Tenable One environment.

When multiple users share a Tenable One instance — especially across geographic or business boundaries — controlling who can see and do what becomes critical. Without a deliberate access strategy, users may encounter data they shouldn't see, accidentally modify scan configurations, or submit support tickets for behavior that is working as designed.

This guide walks you through the recommended approach for implementing RBAC effectively: from understanding the core model, to configuring roles and permissions, to applying best practices that keep your access controls secure and maintainable over time.

How to Use This Guide

This guide is organized into three topics. If you are new to RBAC, read them in order. If you are returning to address a specific need, navigate directly to the relevant topic.

Topic	Description
Welcome	You are here. Understand what this guide covers, what RBAC is, and what you need before you begin.
Get Started with Role-Based Access Control	Step-by-step configuration: roles, permissions, groups, tags, and users.
RBAC Best Practices	Recommendations for scan organization, credential management, and ongoing maintenance.
Troubleshooting	Solutions for common access issues, including users seeing unexpected data, scan failures caused by misconfigured groups, and permission configurations that are not behaving as expected.

What Is RBAC?

Role-based access control (RBAC) is a security model in which access to a system is determined by the roles assigned to users, rather than by individually configured permissions for each user. Tenable implements RBAC through three complementary components:

- Roles – Define what actions a user can perform and which product modules they can access. For example, whether a user can create a scan, manage credentials, or administer other users.
- Permissions – Define which data a user can access. Permissions are always scoped to a set of assets identified by a tag. For example, whether a user can view or scan assets tagged `Region:EMEA`.
- Tags – Key-value pairs assigned to assets that define the scope a permission applies to. Tags are the mechanism that drives data segmentation in Tenable One.

A useful shorthand: a role answers “what can this user do?” while a permission answers “which assets can they do it on?”

> Note: Products in the Tenable One platform – such as Tenable Exposure Management and Tenable Identity Exposure – have their own role models, which can also be managed from within Tenable Vulnerability Management. For more information, see Tenable-Provided Roles and Privileges.

Prerequisites

Before you begin configuring RBAC, confirm the following:

- You have an Administrator role in Tenable Vulnerability Management.
- You have a clear understanding of your organization's team structure – which teams exist, which assets they are responsible for, and what actions they need to perform.
- You have reviewed, or are prepared to review, your organization's existing asset tagging strategy. Tags drive permission scoping, so a well-organized tag structure is essential to effective RBAC.

Related Topics

- Get Started with Role-Based Access Control
- RBAC Best Practices
- Tenable-Provided Roles and Privileges
- Custom Role Privilege Application
- Permissions
- User Groups
- Tags

Get Started with Role-Based Access Control

Role-based access control (RBAC) lets administrators define who can access the platform, what data they can see, and what actions they can perform. By combining roles, permissions, and tags, you can logically segment your vulnerability data to match your organization's team structure, geographic boundaries, or regulatory requirements.

This topic explains the RBAC model, describes each component, and walks you through the recommended setup sequence. For guidance on maintaining and optimizing your RBAC configuration over time, see Best Practices for Tenable Role-Based Access Control (RBAC).

How RBAC Works

Roles vs. Permissions: What Is the Difference?

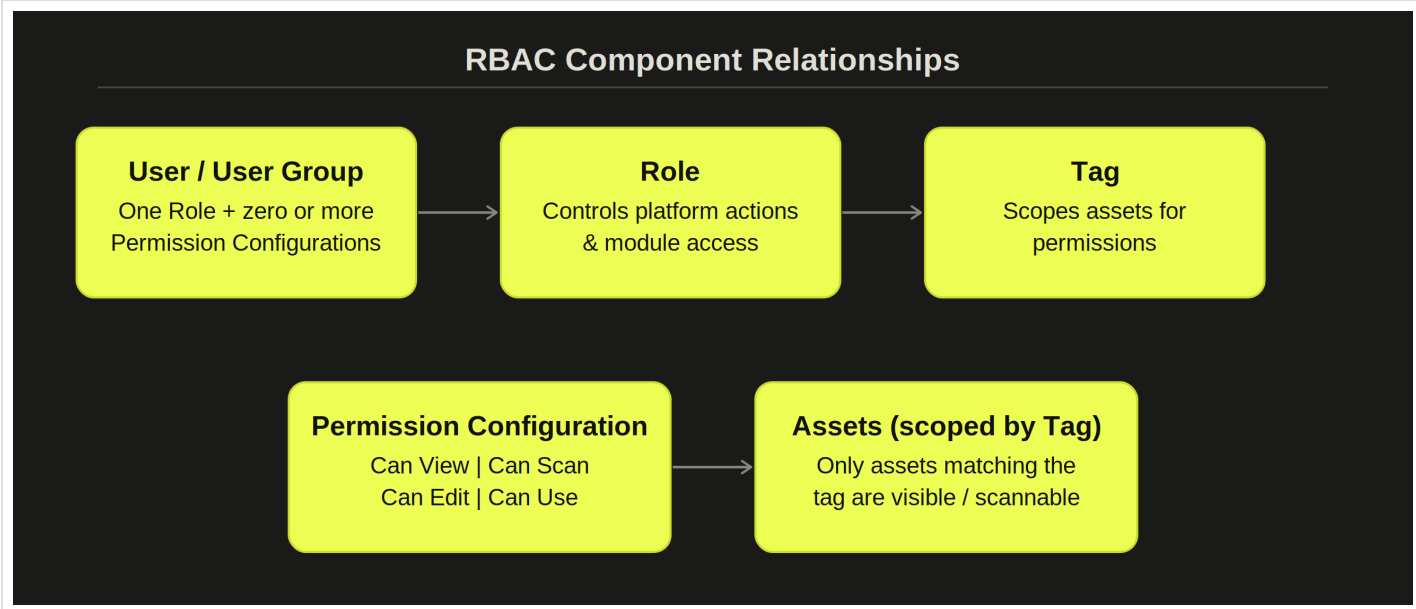
RBAC in Tenable Vulnerability Management is built on three distinct, complementary components:

- Roles — Control what actions a user can perform and which product modules they can access. A role determines whether a user can create a scan, manage credentials, or administer users.
- Permissions — Control which data a user can access. Permissions are always scoped to assets defined by a tag. A permission determines whether a user can view or scan the assets tagged `Region:EMEA`.
- Tags — Define the asset scope that a permission applies to. Tags are key-value pairs assigned to assets and are the mechanism that drives data segmentation.

A useful shorthand: a role answers “what can this user do?” while a permission answers “which assets can they do it on?”

Component Relationships

The following diagram shows how Users, Roles, Groups, Permissions, Tags, and Assets relate to one another:



Tenable-Provided Roles

When you create a user, you must assign exactly one role. This role determines the functions and modules available to that user. The following Tenable-provided roles are available, ordered from least to most privileged:

Role	Typical User	Key Capabilities
Read-Only	Auditors, compliance officers, executives	View dashboards, reports, and findings. Cannot create, edit, delete, or run scans.
Basic	Remediation team members with limited access	Run and view scans assigned to them. Cannot configure the platform or manage users.

Role	Typical User	Key Capabilities
Scan Operator	Network operations staff, junior analysts	Launch, pause, stop, and review scans. Cannot create scan policies or manage global settings.
Standard	Security analysts, vulnerability engineers	Create and manage scans. Generate reports. No administrator-level platform control.
Scan Manager	Senior analysts, scan team leads	Full scan management including scan policies and credentials. No user management.
Administrator	Platform owners, security architects	Full access to all functions, including user management and system configuration. Full and implicit object permissions.

Note: Administrator role users have full platform access and automatically see all assets. Applying tag-based permission configurations to Administrator users has no effect on their data access.

For a complete reference of role privileges, see Tenable-Provided Roles and Privileges.

Custom Roles

When your organization's workflows don't map neatly to a Tenable-provided role, custom roles let you define exactly what a user can and cannot do — for example, create scans but not delete them, or view reports but not modify scan policies. Before creating a custom role, consider:

- Which areas of the product should the user have access to?
- Within each area, which parts of the navigation can the user access?
- Within the navigation, what actions can the user take?

When creating a custom role, you must include Read privileges for the General Settings, License, and My Account sections. Without these, users assigned to the role cannot log in.

Note: You cannot duplicate or delete Tenable-provided roles. Custom roles can be duplicated to accelerate creation of similar roles.

For more information, see Custom Role Privilege Application.

Permission Configurations

A permission configuration defines what a user or group can do with a specific set of assets. It combines a permission type, an asset scope defined by one or more tags, and one or more users or user groups.

The following permission types are available:

Permission	What it allows	Tag interaction	Recommended use
Can View	Read-only visibility into assets, scan results, and reports.	See the assets.	Auditors, compliance staff, remediation stakeholders.
Can Scan	Execute and manage scans. The asset must be discovered and tagged before it can be scanned.	Scan the asset. Asset must be discovered and tagged first.	Teams that need to run scans without managing policies.
Can Edit	Modify and manage objects: scan settings, asset group definitions, report templates.	Edit the tag definition or rule. Change static assignments.	Analysts managing scan configurations. Use with caution.
Can Use	Apply an existing object (scan policy, report template) without	See the tag. Filter by tag.	Users leveraging shared

Permission	What it allows	Tag interaction	Recommended use
	modifying it.		configurations without changing them.

Caution: Adding Can Edit to a permission configuration alongside Can View or Can Scan allows the assigned users to change the scope of the assets they can view and scan. Tenable recommends combining Can Edit with Can View or Can Scan only for administrator users.

Note: You can assign a permission configuration directly to a user or to a group. When a scan runs, Tenable Vulnerability Management evaluates target permissions based on the scan owner's permissions, not the user who launched the scan.

For more information, see Permissions in the *Tenable Vulnerability Management User Guide*.

Tags and Asset Scoping

Tags are the foundation of data segmentation in Tenable Vulnerability Management. Each tag is a key-value pair — for example, `Region:EMEA` or `Team:CloudOps` — that you assign to one or more assets. When you reference a tag in a permission configuration, only assets matching that tag fall within the permission scope.

Tenable recommends using tag automation rules wherever possible to keep tags current as assets are added, modified, or decommissioned.

Note: To edit Tenable Vulnerability Management tags, a user must have the Can Edit permission. To edit Tenable Exposure Management tags, the Can Use permission is sufficient.

User Groups

User groups let you manage permission configurations for multiple users at once. When you assign users to a group, those users inherit all permissions assigned to the group. A group is a collection of permissions — assigning permissions to groups rather than individuals is the recommended approach for managing access at scale.

Common grouping strategies include organizing by geography (for example, US-East, EMEA, APAC), business unit (Finance, Engineering, HR), asset type (Databases, Web Servers, Workstations), or criticality (Production, Development, DMZ).

> Note: Misconfigured user groups can cause scan failures and asset or vulnerability gaps in dashboards and reports. Review group membership and permission configurations regularly.

Recommended Setup Sequence

Complete the following steps in order when configuring RBAC for the first time, or when making significant changes to your access model:

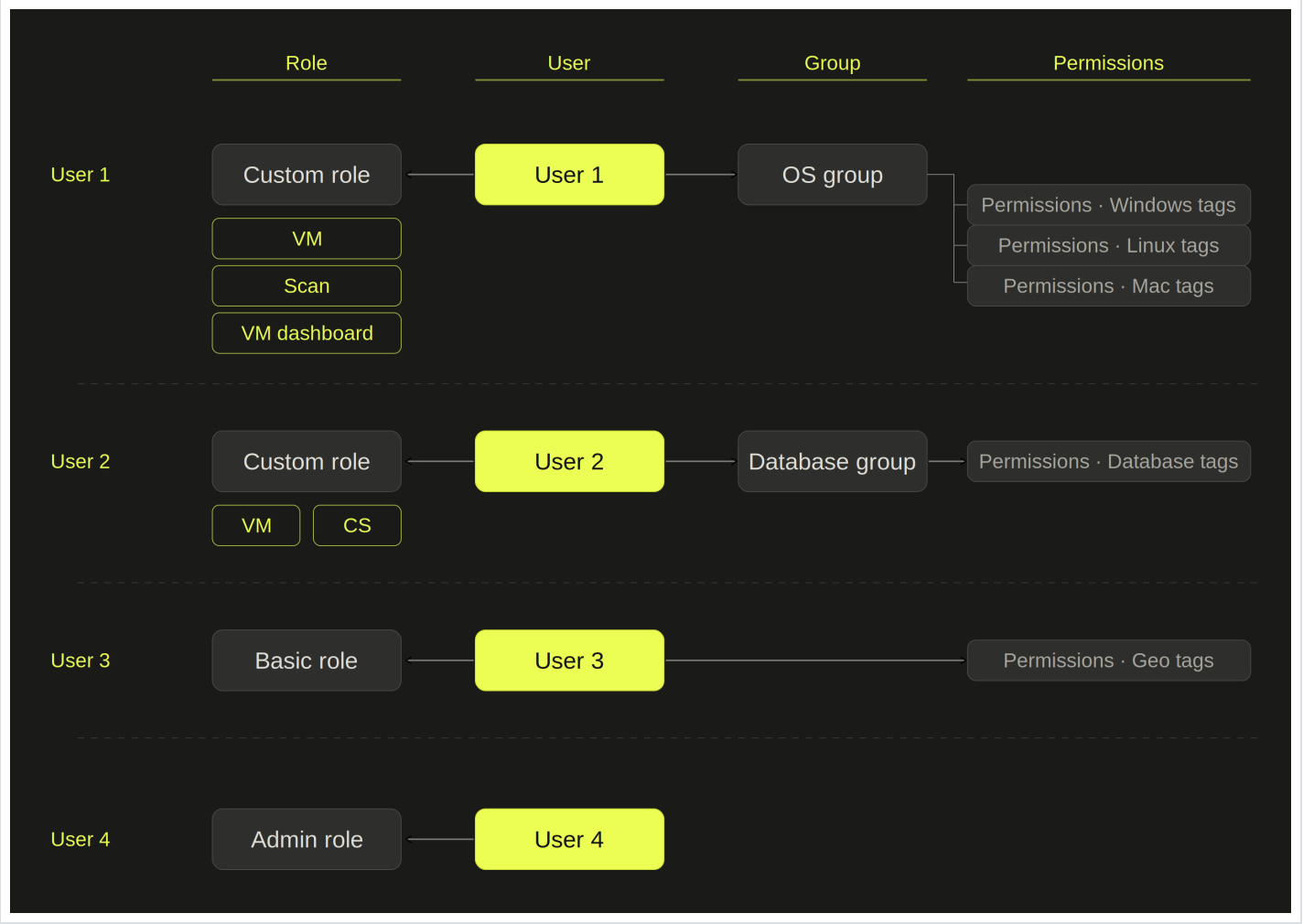
1. Plan your access model — Map your teams and assets. Identify who needs to see what.
2. Create tags — Tag assets to define the scopes your permission configurations will use.
3. Create user groups (optional) — Group users who share the same permission needs.
4. Create users — Add users and assign each one a role (Tenable-provided or custom).
5. Create permission configurations — Combine permission type + tag scope + users/groups.
6. Assign permissions — Associate permission configurations with users or groups.
7. Validate access — Log in as a test user to verify the correct data and functions are available.

Configure RBAC: Step-by-Step

Step 1 — Define User Roles and Responsibilities

The first step in a strong RBAC implementation is deciding what level of access each type of user needs. In Tenable Vulnerability Management, roles broadly determine the actions a user can perform – such as managing users, configuring scans, or viewing vulnerability data. Tenable recommends starting with preconfigured roles where possible, and creating custom roles only when the preconfigured options do not meet your needs.

The following diagram highlights how different users can have a single role, but be part of one, several, or no groups.



Before configuring anything in Tenable Vulnerability Management, define your access model:

- List the teams or personas who need access – for example: security analysts, remediation engineers, auditors, executives.

- Identify which assets each team should be able to see and act on.
- Define the actions each team needs to perform: view only, scan, configure scans, manage users.
- Map each team to a role and a tag-based asset scope.

Use the following table to guide your role and permission choices:

Team / Persona	Suggested Role	Suggested Permissions
CISO / Executive	Read-Only	Can View → All Assets
Compliance officer / Auditor	Read-Only	Can View → relevant tag scope
Remediation engineer	Basic	Can View → assets they own
Junior scanner	Scan Operator	Can Scan → assigned asset tag
Security analyst	Standard	Can Scan + Can View → department tag
Scan team lead	Scan Manager	Can Edit → scan policies; Can Scan → full scope
VM platform owner	Administrator	Full access (no additional permissions required)

Step 2 – Create Tags

Create tags that reflect your asset segmentation strategy – by geography, business unit, criticality, or team ownership.

To create a tag:

1. In the left navigation, click Settings.
2. Click the Tags tile.

3. Click Create Tag and define a key-value pair, for example `Region:EMEA` or `Team:CloudOps`.
4. Add assets to the tag manually, or configure automation logic to dynamically assign assets.

For more information, see Tags in the *Tenable Vulnerability Management User Guide*.

Step 3 – Create User Groups (Recommended)

If multiple users share the same data access requirements, create a user group and assign permissions to the group rather than individual users.

To create a user group:

1. In the top navigation bar, click Settings > Access Control > Groups.
2. Click Create Group, provide a name, and add members.

For more information, see User Groups in the *Tenable Vulnerability Management User Guide*.

Step 4 – Create Users

When you create a user, you must assign a role that broadly determines the platform functions available to that user.

To create a user:

1. In the top navigation bar, click Settings > Access Control > Users.
2. Click Create User and provide the required details.
3. In the Role field, select the appropriate Tenable-provided role, or select a custom role if one has been defined.
4. Click Save.

> Note: If your organization uses SSO or LDAP, users may be provisioned automatically. Ensure that the role assignment logic in your identity provider aligns with your planned access model.

For more information, see Users in the *Tenable Vulnerability Management User Guide*.

Step 5 – Create Permission Configurations

A permission configuration links a permission type to a tag-scoped set of assets, then assigns that configuration to users or groups.

To create a permission configuration:

1. In the left navigation, click Settings.
2. Click the Access Control tile, then click the Permissions tab.
3. Click Create Permission.
4. Provide a name for the permission configuration.
5. In the Objects section, select a tag (or All Assets for unrestricted access).
6. In the Permissions section, select one or more permission types: Can View, Can Scan, Can Edit, or Can Use.
7. In the Users or Groups section, add the users or groups to which this configuration applies.
8. Click Save.

> Caution: If you do not configure a scan policy with the Default: No Access setting, users who can access the scan policy will be able to see all scan results, regardless of their tag-based permission scope. Tenable recommends always setting Default: No Access on scan policies in environments where RBAC is enforced.

Step 6 – Assign Permissions

You can assign permission configurations to users or groups at creation time, or by editing an existing user or group record.

To assign a permission configuration to an existing user:

1. On the Users tab of the Access Control page, click the user to which you want to add a permission configuration.

2. In the Permissions section of the user details, click Add Permission.
3. Select the permission configuration and click Save.

Step 7 – Validate Access

After completing configuration, verify that access is working as intended before communicating the change to your users.

- Log in with a test account that has the role and permissions you have configured.
- Confirm that only the expected assets are visible in the asset inventory and scan results.
- Confirm that the expected actions are available and that prohibited actions are not.
- Check dashboards and reports to confirm that vulnerability data is scoped correctly.

RBAC Best Practices

When multiple users share a Tenable One instance — especially across geographic or business boundaries — controlling who can see and do what becomes critical. Without a deliberate access strategy, users may encounter data they shouldn't see, accidentally modify scan configurations, or open support tickets for behavior that is working as designed.

This topic describes recommended practices for configuring and maintaining RBAC in Tenable Vulnerability Management. It covers how to organize users, structure scan folders to enforce access boundaries, manage credentials securely, and keep your RBAC configuration healthy over time.

If you are new to RBAC and have not yet completed your initial configuration, see Get Started with Role-Based Access Control before continuing.

Use the Least-Privilege Model

Assign the lowest role that enables a user to perform their job. This reduces the impact of a compromised account, limits accidental changes, and simplifies compliance auditing.

- Use Tenable-provided roles wherever possible. The six Tenable-provided roles — Read-Only, Basic, Scan Operator, Standard, Scan Manager, and Administrator — cover the majority of real-world use cases. Evaluate them before reaching for a custom role.
- Create custom roles only when necessary. Custom roles are powerful but require ongoing maintenance. Before creating one, ask: which areas of the product should this user access, which navigation items within each area, and which actions within each item? This three-level check prevents over-provisioning.
- Avoid the Administrator role for routine work. Administrator users have full, implicit access to all assets and platform functions. Assign this role only to users who genuinely need to manage users, system settings, or authentication configuration.

For a complete reference of role privileges, see Tenable-Provided Roles and Privileges and Custom Role Privilege Application.

Use Groups, Not Individual Assignments

Assign permission configurations to user groups rather than to individual users. This makes it significantly easier to onboard new staff, reassign responsibilities when team membership changes, and audit who has access to what.

Structure your groups to reflect your organization. Common strategies include:

- Geography (e.g., US-East, EMEA, APAC)
- Business unit (e.g., Finance, Engineering, HR)
- Asset type (e.g., Databases, Web Servers, Workstations)
- Criticality (e.g., Production, Development, DMZ)

When a new analyst joins the EMEA team, you add them to the EMEA group — their access is already correctly scoped. When they move to a different team, you change their group membership. No individual permission reconfiguration is required.

> Note: Misconfigured user groups can cause scan failures and asset or vulnerability gaps in dashboards and reports. Review group membership and permission configurations periodically, particularly after organizational changes.

For more information, see User Groups in the *Tenable Vulnerability Management User Guide*.

Leverage Tag Automation

Tag automation rules automatically assign assets to tags when they match defined criteria. This keeps your permission scopes accurate without manual intervention as your asset landscape changes.

- Define tag automation rules at deployment time. Manual tag assignment is error-prone at scale. Automation rules ensure that new assets discovered by scans are immediately assigned to the correct tags — and therefore fall within the correct permission scopes.
- Review automation rules when your asset inventory changes significantly. Major changes — such as a cloud migration, acquisition, or decommissioning of an environment — may require updates to your tag criteria.

> Tip: A group is made up of a collection of permissions. The diagram in Get Started with RBAC illustrates how different users can hold a single role while belonging to one, several, or no groups. Well-structured tags and automation rules are what make that group model scale.

For more information, see Tags in the *Tenable Vulnerability Management User Guide*.

Implement a Folder Structure for Scan Organization

A well-organized folder structure does more than keep things tidy — it enforces access control at the scan level. When you assign access groups to folders, users see only the scans in folders their group permits. This prevents accidental cross-contamination of scan data between teams, regions, or business units, and makes it easier to audit who has access to what.

Tenable recommends creating a folder hierarchy that mirrors your access group structure. This makes it intuitive for users to understand why they see what they see, and simplifies administration when groups or responsibilities change.

To create a folder hierarchy:

1. In the top navigation bar, click Scans > Folders.
2. Create folders that match your access groups, for example:
    - Production Assets
        - Web Infrastructure
        - Database Systems
        - Critical Applications

- Development Assets
- Third-Party/Vendors

3. After creating your folders, assign the appropriate access groups to each one.

Users see only the scans in folders that their access group permits.

> Note: Folder-level permissions take precedence over any custom role privileges applied.

Configure Managed Credentials Securely

Authenticated scanning gives you significantly deeper vulnerability visibility than unauthenticated scanning — but it also means storing and managing privileged credentials within Tenable Vulnerability Management. Handling credentials carelessly can introduce serious risk. The following best practices help you get the full benefit of authenticated scanning while keeping your credentials secure.

1. Use managed credentials for authenticated scanning. Managed credentials are stored centrally and can be assigned to scans without exposing the underlying credential values to scan operators. This separates the act of scanning from the act of administering credentials.
2. Organize credentials by category to keep management organized and auditable:
    - Host credentials (SSH, Windows, etc.)
    - Database credentials (Oracle, MySQL, PostgreSQL)
    - Cloud credentials (AWS, Azure, GCP)
3. Apply least-privilege principles to credentials. Scanning does not require write or administrative access to target systems. Credentials should have read access only.
4. Limit credential visibility to authorized users only. Use permissions to ensure that only the users who need to assign or manage credentials can see them. Consider creating a dedicated credential-manager user group.

For more information, see Managed Credentials in the *Tenable Vulnerability Management User Guide*.

Control Scan Result Visibility

Scan policies have their own access controls that are independent of tag-based permission configurations. If a scan policy is shared without a Default: No Access setting, users who can access the policy can see all scan results associated with it — regardless of their tag-based permission scope.

> Caution: Always set Default: No Access on scan policies in environments where RBAC is enforced. This prevents users from viewing scan results for assets outside their permission scope by accessing a shared scan policy.

Additionally, when a scan runs, Tenable Vulnerability Management evaluates target permissions based on the scan owner's permissions, not the user who launched the scan. Ensure that scan ownership is assigned to the appropriate user or service account.

Maintain Your RBAC Configuration

RBAC is not a set-and-forget configuration. As your organization grows and changes, your access controls need to keep pace.

- Audit role and permission assignments regularly. Periodically review who holds which roles and which permission configurations are assigned to which users and groups. Remove access that is no longer required.
- Test before deploying changes at scale. Validate any new permission configurations with a test account before applying them broadly, to avoid unintended access gaps or over-exposure.
- Revisit custom role definitions periodically. As your product usage evolves, verify that custom roles still reflect your organization's least-privilege goals and have not accumulated unnecessary privileges.

- Monitor activity logs. Tenable Vulnerability Management's activity logs (available to Administrators) provide an audit trail of user actions. Review them as part of your regular security hygiene.

Summary Checklist

Use the following checklist to verify your RBAC implementation is complete and aligned with best practices:

- Roles assigned reflect the least privilege required for each user's responsibilities.
- Tenable-provided roles are used where possible; custom roles are used only where necessary.
- The Administrator role is assigned only to users who need full platform control.
- Permissions are assigned to groups, not individual users.
- User groups are organized to reflect your team or asset structure.
- Tags are defined and automated to scope permission configurations accurately.
- Scan folders mirror the access group structure.
- All scan policies are set to Default: No Access.
- Managed credentials are organized by category and restricted to authorized users.
- RBAC configurations are reviewed and updated periodically.

Tenable-Provided Roles and Privileges

Tenable-provided roles are a set of predefined user privileges within Tenable Vulnerability Management that broadly determine the functions a user can access and the actions they can perform. These roles provide a structured, tiered approach to managing access, ensuring users only have the capabilities necessary for their security responsibilities. When you create a user account, you must assign one of these roles, which automatically grants a specific set of privileges.

Roles vs. Permissions: What's the difference?

- Roles – Roles allow you to manage privileges for major functions in Tenable One and control which Tenable One modules and functions users can access.
- Permissions – Permissions allow you to manage access to data, such as Tags, Assets, and their Findings.

Simply put, roles are the actions you can take in a product, and permissions determine the data to which you can perform those actions.

Tenable Vulnerability Management Roles

The primary Tenable-provided roles used for Tenable Vulnerability Management, from most restricted to most privileged, include:

Read-Only

Read-Only users can view information without being able to make changes, run scans, or manage settings. This role is often assigned to auditors, compliance officers, or executives who need visibility into vulnerability data without risk of accidental modifications. Read-only users cannot create, edit, delete, or export any Tenable objects.

Core Capabilities of a Read-Only User

- Viewing Data
    - Access scan results that have been shared with them.
    - View dashboards, reports, and vulnerability findings within their scope.
    - View recast and accept rules.
    - Browse assets and vulnerabilities they are permitted to see.
    - Consume data shared by administrators, scan managers, or basic users.
- Reports and Dashboards

- Generate and view reports from existing scans.
- Use dashboards and filters to analyze vulnerability data.
- Participate in discussions or workflows outside Tenable (e.g., remediation teams) with exported VM data.

Basic

Basic users can run and view scans assigned to them, but they don't have the ability to configure the platform, manage other users, or control system settings. Their role is designed for day-to-day vulnerability assessment tasks within the boundaries set by Administrators or Scan Managers.

Core Capabilities of a Basic User

- Scan Usage
  - Launch scans that have been shared with them or that they own.
  - View results of scans they created or were given access to.
  - Stop or pause scans they are permitted to run.
  - Share their own scans with other users, if allowed.
  - Receive scan assignments from Scan Managers or Administrators.
- Results and Reporting
  - View scan results for their own scans or assigned scans.
  - Generate, filter, and export reports (PDF, CSV, etc.) for those scans.
  - Use dashboards and findings to track vulnerabilities related to their scope.
- Assets and Policies

- Use existing scan policies made available by Scan Managers or Administrators.
- Assign scans to specific assets or asset groups they have permission to see.

Scan Operator

Scan Operators can operate and manage scans within assigned assets, repositories, or networks. These users are generally focused on running and managing vulnerability scans, but not necessarily creating or administering broader system configurations.

Core Capabilities of a Scan Operator

- Run Scans
  - Launch or start scans that have already been created or assigned to them.
  - Pause, resume, or stop scans they have permission to operate.
- View Scan Status and Results
  - View scan status (running, completed, stopped, failed, etc.) and progress metrics during active scans.
  - Access and review scan results for scans they have run or that are shared with them.
  - Export scan data (e.g., as reports in CSV or PDF formats).
- Manage Assigned Scans
  - Clone or modify existing scans if permitted within their access group.
  - Re-run scans using existing configurations or schedules.

Standard

Standard is a built-in role designed for regular users who need to view and work with vulnerability data, but who do not require administrative or configuration privileges. A Standard user has access primarily for viewing, analyzing, and reporting on vulnerability data that has already been collected.

They can see assets, dashboards, and reports shared with them, but they cannot create, modify, or launch scans unless specifically granted additional privileges.

Core Capabilities of a Standard User

- View Vulnerability Data
    - Access vulnerabilities, assets, dashboards, and reports assigned to their access group.
    - Review findings, severity levels, and vulnerability trends.
    - Filter or search vulnerability data to support analysis or remediation tracking.
- Utilize Dashboards and Reporting
    - View and interact with built-in or shared dashboards.
    - Filter or search vulnerability data to support analysis or remediation tracking.
    - Generate vulnerability reports using available templates or saved filters and export results for analysis.
- Collaborate Within Scope
    - Comment on findings or work within remediation workflows if enabled.
    - Access shared data and insights within their assigned access group or assets.

Scan Manager

The Scan Manager’s purpose is to create, manage, and oversee vulnerability scans and scan results without having unrestricted system-wide control. A scan manager user can fully manage scans but does not have administrative powers over the platform or users.

Core Capabilities of a Standard User

- Scan Creation and Management
    - Create, configure, launch, and schedule vulnerability scans.
    - Define targets and asset groups for scans.
    - Edit or delete scans they own or have been granted access to.
    - Share scans with other users or groups (with rights granted by an Administrator).
    - Assign scan permissions.
- Asset and Scanner Usage
    - Use available scanners and scan zones (assigned by an Administrator).
    - Assign scans to specific scanners.
    - Manage scan distribution across scanner resources.
- Results and Reporting
    - View scan results for the scans they own or manage.
    - Generate and export reports (PDF, CSV, etc.).

Administrator

Administrators have the highest level of permissions and can perform both security management and system configuration tasks. Their role is to control the overall deployment, user access, and operational setup of the product environment.

Core Capabilities of an Administrator

- User and Role Management
    - Create, modify, disable, or delete user accounts.
    - Assign roles, permissions, and group memberships.
    - Enforce security policies like password requirements or authentication methods.
- System Configuration
    - Configure global system settings (network settings, logging, notifications, authentication, etc.).
    - Integrate Tenable with external systems (LDAP/AD, SIEMs, ticketing systems, APIs).
    - Set up and manage access controls.
- Scan and Asset Management
    - Create, configure, launch, and schedule vulnerability scans.
    - Manage scanners and scan zones.
    - Define scan policies and templates for other users.
    - Add, organize, and monitor assets or asset groups.
- Plugin and Update Management
    - Control plugin updates for Tenable platforms.
    - Ensure scanners have the latest detection capabilities.
- Data and Reporting

- Access all vulnerability data, scan results, and reports across the environment.
- Configure report templates and dashboards.
- Share or restrict visibility of findings to other users.

- Security and Compliance Oversight
  - Configure compliance scans (CIS, DISA STIG, PCI DSS, etc.).
  - Manage audit files and compliance templates.
  - Review and enforce organization-wide remediation strategies.
- User Management
  - Define user roles and scope of data access.
  - Oversee activity logs and audit trails.
  - Revoke user or system access when necessary.

Tenable Vulnerability Management Role Privileges

The following table describes privileges associated with each Tenable-provided Tenable Vulnerability Management user role, organized by privilege and function.

> Note: You can further refine user access to specific resources by assigning permissions to individual users or groups. For more information, see Permissions.

> Tip: The following roles and privileges apply to commercial and Tenable FedRAMP Moderate environments, where appropriate.

Area	Tenable Vulnerability Management-Provided Roles and Privileges					
	Administrator	**Scan Manager**	**Standard**	**Scan Operator**	**Basic**	Read-Only
Activity Logs	view, export	-	-	-	-	-
Account Settings	view, modify	view, modify	view, modify	view, modify	view, modify	view
Agents	view, delete	view, delete	-	-	-	-
Agent Freeze Windows	view, create, modify, delete	view, create, modify, delete	-	-	-	-
Agent Groups	view, create, modify, delete	view, create, modify, delete	-	-	-	-
Agent Profiles	view, create, modify, delete	view, create, modify, delete	-	-	-	-
Agent Settings	view, modify	view, modify	-	-	-	-
Assets	view, modify,	view,	view,	view,	view,	view

Area	Tenable Vulnerability Management-Provided Roles and Privileges					
	Administrator	**Scan Manager**	**Standard**	**Scan Operator**	**Basic**	Read-Only
	export, delete	modify, export, delete	modify, export, delete	modify, export, delete	export	
Connectors	view, create, modify, delete	-	-	-	-	-
Custom Roles	view, create, modify, delete, export	-	-	-	-	-
Dashboards	view, create, modify, export, delete	view, create, modify, export, delete	view, create, modify, export, delete	view, create, modify, export, delete	view, create, modify, export, delete	view
Exclusions	view, import, export, delete	view, import, export, delete	-	-	-	-
Exports	view, modify, export,	-	-	-	-	-

Area	Tenable Vulnerability Management-Provided Roles and Privileges					
	Administrator	**Scan Manager**	**Standard**	**Scan Operator**	**Basic**	Read-Only
	delete					
Exposure Response	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view
Findings	view, export	view, export	view, export	view, export	view, export	view
General Settings	view, modify	-	-	-	-	-
Managed Credentials	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view
Networks	view, create, modify, delete	view, create, modify, delete	-	-	-	-
Permissions	view, create, modify, delete	-	-	-	-	-
Recast/Accept	view, create,	-	-	-	-	-

Area	Tenable Vulnerability Management-Provided Roles and Privileges					
	Administrator	**Scan Manager**	**Standard**	**Scan Operator**	**Basic**	Read-Only
Rules	modify, delete					
Reports	view, run, create, modify, delete	view, run, create, modify, delete	view, run, create, modify, delete	view, run, create, modify, delete	view	view
SAML Configurations	view, create, modify, delete	-	-	-	-	-
Scan Results	view, export, delete	view, export, delete	view, export, delete	view, export, delete	view, export, delete	view
Scans[1]	view, import, run, create, modify,	view, import, run,	view, import, run,	view, import, run,	view[4], import	view

[1]User roles determine a user's abilities, but the permissions that a user has for a particular scan are dictated by scan permissions.

[4]Can view list of scans, but not scan configuration details.

Area	Tenable Vulnerability Management-Provided Roles and Privileges					
	Administrator	**Scan Manager**	**Standard**	**Scan Operator**	**Basic**	Read-Only
	delete	create, modify, delete	create, modify, delete	create[1], modify[2], delete		
Scanner Groups	view, create, modify, delete	view, create, modify, delete	-	-	-	-
Scanner Profiles	view, create, modify, delete	view, create, modify, delete	-	-	-	-
Sensors	view, add, modify, delete	view, add, modify, delete	-	-	-	-
Shared Collections	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view	view

[1]Can create scans using existing user-defined policies that are shared with the user.

[2]Can manage scans using existing user-defined policies that are shared with the user.

Area	Tenable Vulnerability Management-Provided Roles and Privileges					
	Administrator	**Scan Manager**	**Standard**	**Scan Operator**	**Basic**	Read-Only
Tags[1]	view, create tag category, create tag value, delete, export, assign, unassign	view, create tag value, delete, assign, unassign	view, delete, assign, unassign[2]	view, delete, assign, unassign	view, assign, unassign	view
User-Defined Scan Templates	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view, create, modify	-	-
User Groups	view, create, modify, delete, export	-	-	-	-	-
Users	view, create, modify, delete, generate	-	-	-	-	-

[1]Assigning and Unassigning tags can be done from the Asset Details page.

[2]Standard users must have the Can Use permission to view, delete, assign, and unassign tags.

Area	Tenable Vulnerability Management-Provided Roles and Privileges					
	Administrator	**Scan Manager**	**Standard**	**Scan Operator**	**Basic**	Read-Only
	API key					
Vulnerability Intelligence	view	view	view	view	view	-

Other Tenable One Platform Product Roles and Privileges

Within Tenable Vulnerability Management, you can also apply privileges for other applications within the Tenable One platform. For more information, see Tenable One Product Architecture in the *Tenable One Deployment Guide*.

The following tables describe privileges associated with each product's available user roles, organized by function in their respective product.

> Note: You can further refine user access to specific resources by assigning permissions to individual users or groups. For more information, see Permissions.

> Tip: The following roles and privileges apply to commercial and Tenable FedRAMP Moderate environments, where appropriate.

Tenable Web App Scanning-Provided Roles and Privileges

Area	[[[Undefined variable WebApplicationScanning.WAS]]]-Provided Roles and Privileges					
	Administrator	**Scan Manager**	**Standard**	**Scan Operator**	**WAS Reader**	**Basic**
Dashboards	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view	view
Tenable-Provided Scan Templates	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view	-	-
Scans (also requires scan permissions)	view, import, create, modify, run, delete	view, import, create, modify, run, delete	view, create, modify, run, delete	view, create[1], modify[2], run, delete, move to trash	view	view
Managed Credentials	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete	view, create, modify, delete

[1]Can create scans using existing user-defined policies that are shared with the user.

[2]Can manage scans using existing user-defined policies or user templates that are shared with the user.

Area	[[[Undefined variable WebApplicationScanning.WAS]]]-Provided Roles and Privileges					
	Administrator	**Scan Manager**	**Standard**	**Scan Operator**	**WAS Reader**	**Basic**
Scan Permissions	view, create, modify, delete[1]	view, create, modify, delete[2]	view, create, modify, delete[3]	view, create, modify, delete[4]	-	-
Scan Results (also requires scan permissions)	view, delete	view, delete	view, delete	view, delete	view, delete	view, delete

Tenable Exposure Management-Provided Roles and Privileges

[1]Administrator users can create, modify, and delete permissions for scans that any user on the account owns.

[2]Scan Manager users can create, modify, or delete permissions only on scans they own.

[3]Standard users can create, modify, or delete permissions only on scans they own.

[4]Scan Operator users can create, modify, or delete permissions only on scans they own.

Area	Tenable Exposure Management-Provided Roles and Privileges					
	Administrator	**Scan Manager**	**Standard**	**Scan Operator**	**Basic**	Read-Only
Settings	manage, read	read	read	read	read	read
Access to Asset Type	computing resource (host), cloud resource, web application, identity	computing resource (host), cloud resource, web application, identity	computing resource (host), cloud resource, web application, identity	computing resource (host), cloud resource, web application, identity	computing resource (host), cloud resource, web application, identity	read
Export	manage own	manage own	manage own	manage own	manage own	read
Exposure Card	create, share, read	create, share, read	create, share, read	share, read	read	read
Finding	manage, read	manage, read	read	read	read	read
Query	search, save, read	search, save, read	search, save, read	search, read	search, read	read
Tag	create, edit	create, edit	-	-	-	-
Third-	create,	-	-	-	-	-

Area	Tenable Exposure Management-Provided Roles and Privileges					
	Administrator	**Scan Manager**	**Standard**	**Scan Operator**	**Basic**	Read-Only
Party Connectors	manage, read					

Tenable Identity Exposure-Provided Roles and Privileges

Area	Tenable Identity Exposure-Provided Roles and Privileges	
	Global Administrator	**Custom**
Entire Application	Read, Edit, Create	User roles are defined in the application. For more information, see Roles.

Tenable Attack Surface Management-Provided Roles and Privileges

Area	Tenable Attack Surface Management-Provided Roles and Privileges			
	Business Administrator	Cloud Connector Manager	**Active User**	**View-Only User**
Inventory	manage, add, modify, delete	add, modify, leave	add, modify, leave	view
Suggestions	manage, add, modify, delete	manage, add, modify, delete	manage, add, modify, delete	view

Subscriptions	manage, add, modify, delete	manage, add, modify, delete	manage, add, modify, delete	view
Dashboard	manage, add, modify, delete	manage, add, modify, delete	manage, add, modify, delete	view
Reports	manage, add, modify, delete	manage, add, modify, delete	manage, add, modify, delete	view
Txt Records	manage, modify, delete	manage, modify, delete	manage, modify, delete	view
Activity Logs	view	view	view	view
User Accounts	manage, modify, delete	-	-	-
Business	manage, modify	-	-	-
Cloud Connectors	manage, add, modify, delete	manage, add, modify, delete	view	view

Note: By default, Tenable Attack Surface Management users created within Tenable One are mapped to a user role as documented in the Tenable Attack Surface Management User Guide.

Tenable Cloud Security-Provided Roles and Privileges

Area	Tenable Cloud Security-Provided Roles and Privileges		
	Administrator	**Collaborator**	**Viewer**
Console Tabs	view	view	view
Reports	view, create, schedule, delete	view, create, schedule, delete	view, create

Area	Tenable Cloud Security-Provided Roles and Privileges		
	Administrator	**Collaborator**	**Viewer**
Inventory	view, manage, generate policy	view, manage, generate policy	-
Findings	view, share, manage, disable	view, share, manage	view, share
Administration	view, manage, audit	-	-

Tenable PCI ASV-Provided Roles and Privileges

Area	Tenable PCI ASV-Provided Roles and Privileges	
	Administrator	**Other**
Entire Application	view, import, run, create, modify, delete	-

Custom Role Privilege Application

Custom role privileges affect different areas of the Tenable One platform. The following tables describe the actions each privilege option can perform in their respective platform application.

> Note: When creating a custom role, you must enable the application for use before you can select these privileges. For more information, see Create a Custom Role.
>
> If you disable a user's access to an application:
>
> - Tenable removes the application from the Home page within Tenable Exposure Management.
> - All fields/tabs related to the application are disabled, including in the Inventory, Assets, and Asset Details views in Tenable Exposure Management.

Platform Custom Role Privilege Application

User Interface Section	Privilege Options	Actions Privilege Can Perform
Assets	Read (Enabled by Default) Note: To view Asset Criticality Rating and Asset Exposure Score metrics, a user must also have Lumin application access enabled.	View your assets across the platform, including: • The **Assets** page • Asset details
Findings	Read (Enabled by Default)	View your findings across the platform, including: • The **Findings** page • Finding details
My Account	Read (Enabled by Default)	View your account details on the My Account page, including: • The groups to which you belong • The permissions assigned to your account • The API keys page
	Manage	Manage your account details on the My Account page, including: • Your general account information

		• Your password • Enable two factor authentication • Generate API keys
Access Control	Read	View Access Control data, including: • The Groups page and all data therein • The Permissions page and all data therein • The Roles page and all data therein • The API Access Security page and all data therein

	Manage	Manage Access Control configurations, including:
		• Groups
		  • Create, edit, or delete a group
		  • Export your list of groups
		• Permissions
		  • Create, edit, or delete permission

		configurations • Add or remove a permission configuration from a user or group • Export your list of permission configurations • Roles • Create, duplicate, edit, or delete a custom role • Export your list of roles • Edit allowed IP addresses on the API Access Security page
Access Control Users	Read	View the Users page and all data therein.
Activity Log	Read	View the Activity Logs page and all data therein.
General Settings	Read	View the **General Settings** page and all data therein.
	Manage	Configure options on the **General Settings** page,

		including: • Severity metric • Service-Level Agreement metric • Plugin Language • Default Export Expiration • Plugin Output Search • Email Allow List
License Information	Read	View the **License Information** page and all data therein
Tags	Read	View the Tags page and all data therein, including: • Categories • Values
Target Group	Read	View existing target groups (saved lists of assets/IPs) and select them as a target when configuring a scan.
	Manage	Create, edit, and delete target groups.
Export	Manage Own	Scheduled Exports – Manage your own scheduled exports, including:

		• Edit or delete a scheduled export • Enable or disable a scheduled export Export Activity – Manage your own export activity, including: • Filter your export activity list • Download or export your export activity list • Renew an export expiration date • Stop or delete an export
	Manage All	Scheduled Exports – Manage all scheduled exports within your container, including: • Edit or delete a scheduled export • Enable or disable a scheduled export Export Activity – Manage all export activity within your container, including: • Filter the export activity list

		• Download or export the export activity list • Renew an export expiration date • Stop or delete an export
Hexa AI		
Vulnerability Management	Use	Use the **Hexa AI** assistant

Tenable Exposure Management Custom Role Privilege Application

User Interface Section	Privilege Options	Actions Privilege Can Perform
Exposure Signals	Read (Enabled by Default)	View the **Exposure Signals** page and all data therein
	Write	Manage exposure signals, including: • Add, edit, or duplicate a custom exposure signal • Edit the priority of a built-In exposure signal • Archive or delete a

		custom exposure signal
Inventory	Read (Enabled by Default) Note: To view Asset Criticality Rating and Asset Exposure Score metrics, a user must also have Lumin application access enabled.	View the **Inventory** page, its sub-pages, and all data therein, including: • **Assets** ◦ View Asset Details • **Weaknesses** ◦ View Weakness Details • **Findings** ◦ View Findings Details • **Software** ◦ View Software Details
	Write	Manage data in the Inventory section, including: • Export data from any Inventory sub-page

		• Save bookmarks • Create a tag or exposure signal based off of the asset list
Analytics > Dashboards	Read	• View the **Dashboards** page and all data therein • View the **Dashboard Overview** page
	Write	Manage dashboards, including: • Create, edit, and delete custom dashboards • Make a copy of a dashboard • Change the privacy of a custom dashboard • Export dashboard data
Analytics > Exposure View	Read	View the **Exposure View** page and all data therein

	Write	Manage the Exposure View page, including: • Comment on the Exposure View page and view comment notifications • Export a section or all of the Exposure View page • ConfigureExposure View page settings
	Enable Built-In Card	View the Built-in Cards section of the Exposure Card Library.
Attack Path Important! To access the Attack Path section of Tenable Exposure Management, you must enable the Can View permission for All Assets. Note that this overrides and disables the ability to enforce specific tag permissions for this user in other parts of Tenable Exposure Management. For more information, see Permissions.	Read (Enabled by Default) Note: If a user does not have access to a specific node or asset, they can see it on the page but cannot view or access any of its details.	View the Attack Path page, its sub-pages, and all data therein, including: • **Dashboard** • **Top Attack Paths** • **Top Attack Techniques** ◦ Top Attack Technique Details

		• MITRE ATT&CK Heatmap
	Write	Manage attack techniques, including: • Change the status of an attack technique • Export, archive/un-archive, or bookmark an attack technique • Add and view comments on an attack technique • View the log history for an attack technique • Share an attack technique
Tags	Read (Enabled by Default)	View the **Tags** page and all data therein, including: • View Tag Details
	Write	Manage tags, including: • Create, edit, or

		delete a tag
Connectors	Read (Enabled by Default)	View the **Connectors** page and all data therein
	Write	Manage connectors, including: • Add, edit, or delete a connector • View connector status and logs • Schedule connector sync time • Disable or enable a connector

Tenable Attack Surface Management Custom Role Privilege Application

User Interface Section	Privilege Options	Actions Privilege Can Perform
Business	Manage	Admin Dashboard – View and manage users, inventory, and business details, including: • Add users • Edit Inventory details • Edit Business details

		Subscriptions – View and manage Subscriptions, including: • Add or create subscriptions • Share, copy, or delete subscriptions • Create alerts for subscriptions Suggestions – View and manage Suggestions, including: • Add suggested domains to an inventory • Archive suggested domains • Add suggestion blocklist items • Add source-based suggestions Activity Logs – View and manage Activity Logs. TXT Records – View and manage TXT Records. Reports – View and manage Reports, including: • Add, edit, or delete a report • Run a report • View report details
Cloud Connectors	Manage	View and manage your cloud Integrations, including: • Add, edit, or delete integrations
Inventory	Manage	View and manage your inventory from the Explore > Inventory page and all data therein, including: • View assets and asset details in your inventory • View asset attribution

		• Manage asset tags • Move or copy assets to another inventory • Export or archive assets • Create an Advanced Network Scan • Create Web Application Scan • Create, configure, or leave an inventory • Manage Inventory Sources, Exclusion Rules, or Automation Rules • Search for, filter, copy-to-clipboard, and group assets in your inventory

Tenable Vulnerability Management Custom Role Privilege Application

Note: If you grant the Export privilege within any section, you automatically grant the user access to the Exports page and the related export data.

User Interface Section	Privilege Options	Actions Privilege Can Perform
Dashboards	Read	View your dashboards and their related data.
	Full Write	Fully manage your dashboards, including the privileges associated with Create, Delete, Edit, Export, and Share.

	Create	Create a dashboard.
	Edit	Edit a dashboard.
	Delete	Delete a dashboard.
	Export	Export a dashboard or dashboard widget.
	Share	Share one or more dashboards with other Tenable Vulnerability Management users.
Scans > Nessus/Agent Scan	Read (Enabled by default)	View your Tenable Nessus and Tenable Agent scans.
	Full Write	Fully manage your Tenable Nessus and Tenable Agent scans, including the privileges associated with Create, Delete, Edit, Export, Launch, and Submit PCI.
	Create	Create a Tenable Nessus or Tenable Agent scan.
	Delete	Delete a Tenable Nessus or Tenable Agent scan.
	Edit	Edit a Tenable Nessus or Tenable Agent scan.
	Export	Export a Tenable Nessus or Tenable Agent scan.

	Launch	Launch a Tenable Nessus or Tenable Agent scan.
	Submit PCI	Submit a Tenable Nessus or Tenable Agent scan for PCI ASV validation. Tip: For more information about PCI ASV validation, see the Tenable PCI ASV User Guide.
Scans > Shared Collections	Read (Enabled by default)	View your shared collections.
	Full Write	Fully manage your shared collections, including the privileges associated with Create, Delete, and Edit.
	Create	Create a shared collection.
	Delete	Delete a shared collection.
	Edit	Edit a shared collection.
Scans > Scan Exclusion	Read (Enabled by default)	View your scan exclusions.
	Full Write	Fully manage your shared collections, including the privileges associated with Create, Delete, Edit, and Export.

	Create	Create a scan exclusion.
	Delete	Delete a scan exclusion.
	Edit	Edit a scan exclusion.
	Export	Export a scan exclusion.
Scans > User-Defined Scan Template	Read (Enabled by default)	View your user-defined scan templates.
	Full Write	Fully manage your user-defined scan templates, including the privileges associated with Create, Delete, Edit, and Export.
	Create	Create a user-defined scan template.
	Delete	Delete a user-defined scan template.
	Edit	Edit a user-defined scan template.
	Export	Export a user-defined scan template.
Scans > Tenable-Provided Scan Template	Read (Enabled by default)	View all Tenable-provided scan templates.
Scans > Managed Credential	Read (Enabled by default)	View your managed credentials.

	Full Write	Fully manage your managed credentials, including the privileges associated with Create, Delete, Edit, and Export.
	Create	Create a managed credential.
	Delete	Delete a managed credential.
	Edit	Edit a managed credential.
	Export	Export a managed credential.
Vulnerability Intelligence	Read	View data on the Vulnerability Intelligence page.
	Full Write	Fully manage items in Vulnerability Intelligence, including the privileges associated with Export.
	Export	Export findings or assets from the Vulnerability Intelligence page.
Exposure Response	Read (Enabled by default)	View data on the Exposure Response page and its sub-pages.

	Full Write (Enabled by default)	Fully manage your exposure response initiatives, including the privileges associated with Create, Delete, Edit, and Export.
	Create (Enabled by default)	Create an exposure response initiative, combination, or report card.
	Delete (Enabled by default)	Delete an exposure response initiative.
	Edit (Enabled by default)	Edit an exposure response initiative.
	Export (Enabled by default)	Export exposure response initiative activity.
Explore	Read	View data on the Explore page and its sub-pages.
	Full Write	Fully manage your Explore findings and assets, including the privileges associated with Delete, Edit ACR, and Export.
	Delete	Delete an asset.
	Edit ACR	Edit the ACR of an asset.
	Export	Export data from the Assets and Findings tabs.

Sensors > Nessus Scanner	Read	View Nessus scanner data on the Sensors page and its sub-pages.
	Full Write	Fully manage your Nessus scanners, including the privileges associated with Delete, Edit, and Export.
	Delete	Delete a Nessus scanner.
	Edit	Edit a Nessus scanner.
	Export	Export linked Nessus scanners.
Sensors > Nessus Agent	Read	View Nessus Agent data on the Sensors page and its sub-pages.
	Full Write	Fully manage your Nessus Agents, including the privileges associated with Delete, Edit, and Export.
	Delete	Delete a Nessus Agent.
	Edit	Edit a Nessus Agent.
	Export	Export linked Nessus Agents.
Sensors > Agent Group	Read	View agent group data on the Sensors page and its sub-pages.

	Full Write	Fully manage your agent groups, including the privileges associated with Delete, Edit, and Export.
	Delete	Delete an agent group.
	Edit	Edit an agent group.
	Create	Create an agent group.
Sensors > Web Application Scanner	Read	View Web Application scanner data on the Sensors page and its sub-pages.
	Full Write	Fully manage your Web Application scanners, including the privileges associated with Delete, Edit, and Export.
	Delete	Delete a Web Application scanner.
	Edit	Edit a Web Application scanner.
	Export	Export linked Web Application scanners.
Sensors > Nessus Network Monitor	Read	View Nessus Network Monitor data on the Sensors page and its sub-pages.
	Full Write	Fully manage your Nessus

		Network Monitors, including the privileges associated with Delete, Edit, and Export.
	Delete	Delete a Nessus Network Monitor.
	Edit	Edit a Nessus Network Monitor.
	Export	Export linked Nessus Network Monitors.
Sensors > Scanner Group	Read	View scanner group data on the Sensors page and its sub-pages.
	Full Write	Fully manage your scanner groups, including the privileges associated with Delete, Edit, Export, and Create.
	Delete	Delete a scanner group.
	Edit	Edit a scanner group.
	Export	Export scanner group data.
	Create	Create a scanner group.
Sensors > Network	Read	View your networks and their associated data.
	Full Write	Fully manage your network

		data, including the privileges associated with Delete, Edit, Export, and Create.
	Delete	Delete a network.
	Edit	Edit a network.
	Export	Export network data.
	Create	Create a network.
Sensors > Linking Key	Read	View your linking keys. Important! To view a linking key for a sensor, you must have privileges to view data for that sensor type. For example, to view a Nessus linking key, you must have Sensor > Nessus Scanner permissions enabled for your account.
	Create	Create a linking key. Important! To generate a linking key for a sensor, you must have privileges to manage data for that sensor type. For example, to generate a Nessus linking key, you must have Sensor > Nessus Scanner permissions enabled for your account.
Recast	Read	View your recast and accept

		rules and their associated data.
	Full Write	Fully manage your recast and accept rules, including the privileges associated with Create, Delete, Disable, Edit, and Export.
	Create	Create a recast or accept rule.
	Delete	Delete a recast or accept rule.
	Enable/Disable	Enable/disable a recast or accept rule.
	Edit	Edit a recast or accept rule.
	Export	Export recast or accept rule data.
Reports	Read (Enabled by default)	View your reports and their associated data.
	Full Write	Fully manage your reports, including the privileges associated with Create, Delete, Download, Edit, Generate, Schedule, and Share.
	Create	Create a report.

	Delete	Delete a report.
	Download	Download a generated report.
	Edit	Edit a report.
	Generate	Generate a report.
	Schedule	Schedule a report generation.
	Share	Share one or more reports with other Tenable Vulnerability Management users.
Exports Note: Export (Read, Edit, Disable, Delete) permissions are granted to users either through the `TioBackendExportManageOwn` permission or through the export permissions within the Tenable Vulnerability Management category. For more information, see Permissions.	Read	View your scheduled exports and their associated data.
	Full Write	Fully manage your scheduled exports, including the privileges associated with Delete, Disable, Edit, and Export.
	Delete	Delete a scheduled export.
	Enable/Disable	Enable/disable a scheduled export.
	Edit	Edit a scheduled export.
Remediation	Read	View your remediation projects, remediation goals,

		and their related data.
	Full Write	Fully manage your recast and accept rules, including the privileges associated with Create, Delete, Edit, and Export.
	Create	Create a remediation project or remediation goal.
	Delete	Delete a remediation project or remediation goal.
	Edit	Edit a remediation project or remediation goal.
	Export	Export remediation project or remediation goal data.

User Interface Section	Privilege Options	Actions Privilege Can Perform
Vulnerability Management		
Dashboards	Manage	Manage your dashboards, including: • Create, edit, or delete a dashboard • Filter, rename, duplicate, or set a default dashboard • Manage dashboard exports
	Share	Share one or more dashboards with other Tenable Vulnerability Management users.

Recast/Accept Rule	Read	View the Recast page and all data therein, including: • Recast rule details • Recast columns • Recast filters
	Manage	Manage recast and accept rules, including: • Add or edit recast/accept rules • Disable or delete recast/accept rules
Scan		
Nessus/Agent Scan	Read	View scan configurations and results.
	Manage	Create, edit, delete, and launch Nessus scanner or agent scans.
	Submit PCI	Submit a completed PCI scan to Tenable's ASV (Approved Scanning Vendor) team for validation and attestation.
Scan Exclusion	Read	View targets that are excluded from scans.
	Manage	Create, edit, and delete scan exclusions.
Shared Collections	Read	View shared collections.
	Manage	Manage shared collections, including: • Create, edit, or delete a shared collection • Add or remove scans from a shared collection
Tenable-Provided Scan Template	User	Select and apply a built-in Tenable scan template (for example, "Basic Network Scan") to a new scan they are

		creating. Users cannot modify the Tenable template itself.
User-Defined Scan Template	Read	View the settings of a scan template created by another user.
	Manage	Create, edit, and delete custom scan templates.
Managed Credential	Read	View and select existing managed credentials to use them in a scan. This does not let the user see the actual password or secret.
	Manage	Create, edit, and delete the managed credentials stored in the platform's vault.
Sensors		
Agent	Read	View agents and agent groups. This allows a user to see the list of linked agents and agent groups. They can view details like agent status and linking keys. They cannot edit agent group settings, unlink agents, or use the agent groups in a scan.
Scanner	Read	View scanners and scanner groups. This allows a user to see all linked scanners, cloud scanners, and scanner groups. They can view scanner status, version, and configuration details. They cannot edit scanner settings, delete scanners, or use the scanners in a scan.

Tenable Web App Scanning Custom Role Privilege Application

User Interface	Privilege	Actions Privilege Can Perform

Section	Options	
Assets	Create	Create a web application.
Web Application Scan	Read	View scan configurations and results.
	Manage	Manage web application scans, including: • Create, launch, edit, or delete web application scans • Copy a scan • Export scan results
	Import	Import a web application scan.
	Submit PCI	Submit a completed PCI scan to Tenable's ASV (Approved Scanning Vendor) team for validation and attestation.
Tenable-Provided Scan Template	User	Select and apply a built-in Tenable scan template (for example, "Basic Network Scan") to a new scan they are creating. Users cannot modify the Tenable template itself.
Managed Credential	Read	View and select existing managed credentials to use them in a scan. This does not let the user see the actual password or secret.
	Manage	Create, edit, and delete the managed credentials stored in the platform's vault.
Recast/Accept Rule	Read	View the Recast page and all data therein, including: • Recast rule details • Recast columns • Recast filters

	Manage	Manage recast and accept rules, including: • Add or edit recast/accept rules • Disable or delete recast/accept rules
User-Defined Scan Template	Read	View the settings of a scan template created by another user.
	Manage	Create, edit, and delete custom scan templates.

Tenable AI Exposure Custom Role Privilege Application

User Interface Section	Privilege Options	Actions Privilege Can Perform
AI Exposure Admin	Use	Modify settings within the Tenable AI Exposure application.

Troubleshooting

As you configure and refine your RBAC setup, you may encounter unexpected behavior that points to a gap in permissions rather than a product defect.

Permission-Related 403 HTTP Errors

Even a well-designed RBAC configuration can produce unexpected behavior if permissions are incomplete. One of the most common issues is a 403 HTTP error that appears when a user attempts an action they appear to have access to. Understanding the root cause can save significant troubleshooting time.

Scenario: Empty Share Report Pane

You have permission to share reports but lack the Read permission for users and groups. When you attempt to share a report, the share pane appears empty, often accompanied by a 403 HTTP error.

Corrective action: Grant the Can Read permission for users and groups to the affected user role.

> Note: Similar scenarios occur in other areas where users and groups appear empty. In most cases, the cause is the same – the user lacks read permissions for users and groups.