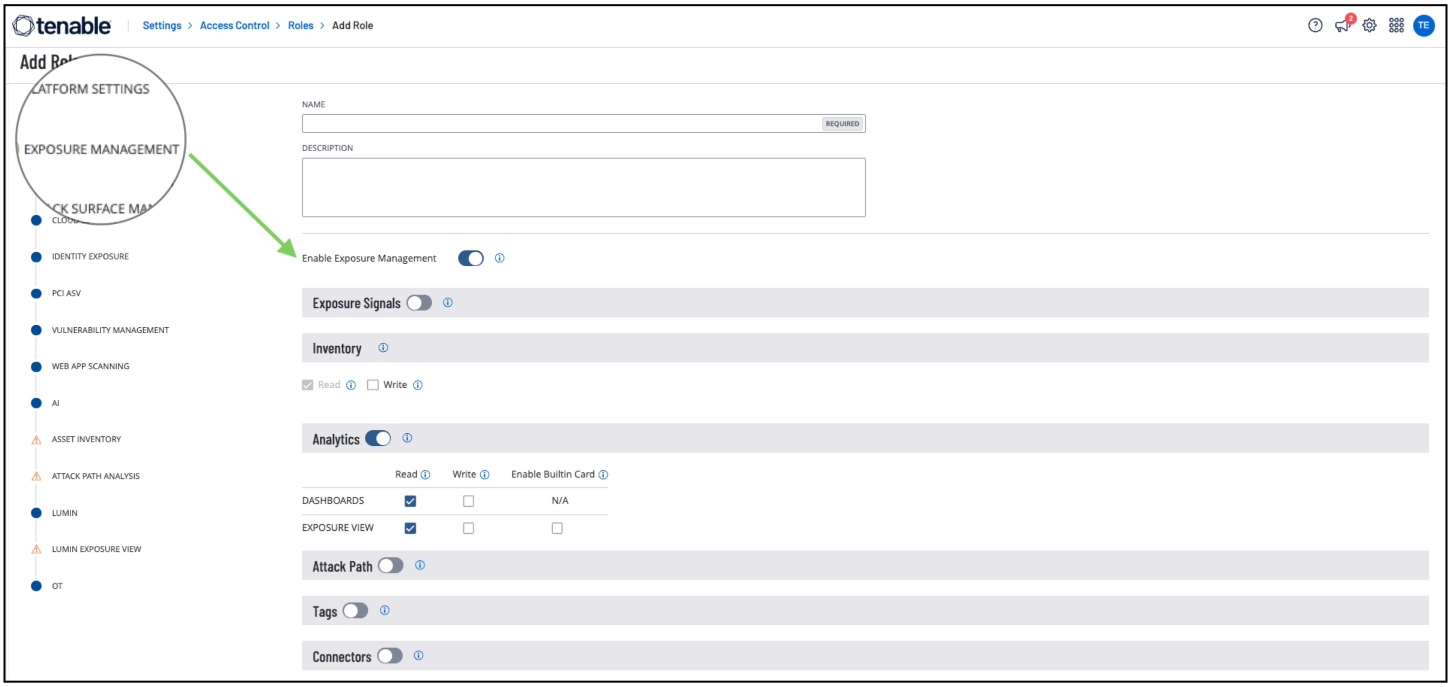
Customer FAQ: RBAC updates and parallel support

Summary

Please follow along in this document to understand the changes, view our FAQ, explainer video and review our documentation.

Tenable is excited to announce the release of the following new roles and updates:

1. ✅ **A new custom role for Exposure Management** that consolidates access into a single place. This allows for more granular access and control for the following areas:
    - Exposure Signals
    - Inventory
    - Analytics
        - Exposure View
        - Dashboards
    - Attack Path Analysis
    - Tags
    - Connectors
    - Identity



NAME REQUIRED

DESCRIPTION

Enable Exposure Management ●

Exposure Signals ○

Inventory

☑ Read ☐ Write

Analytics ●

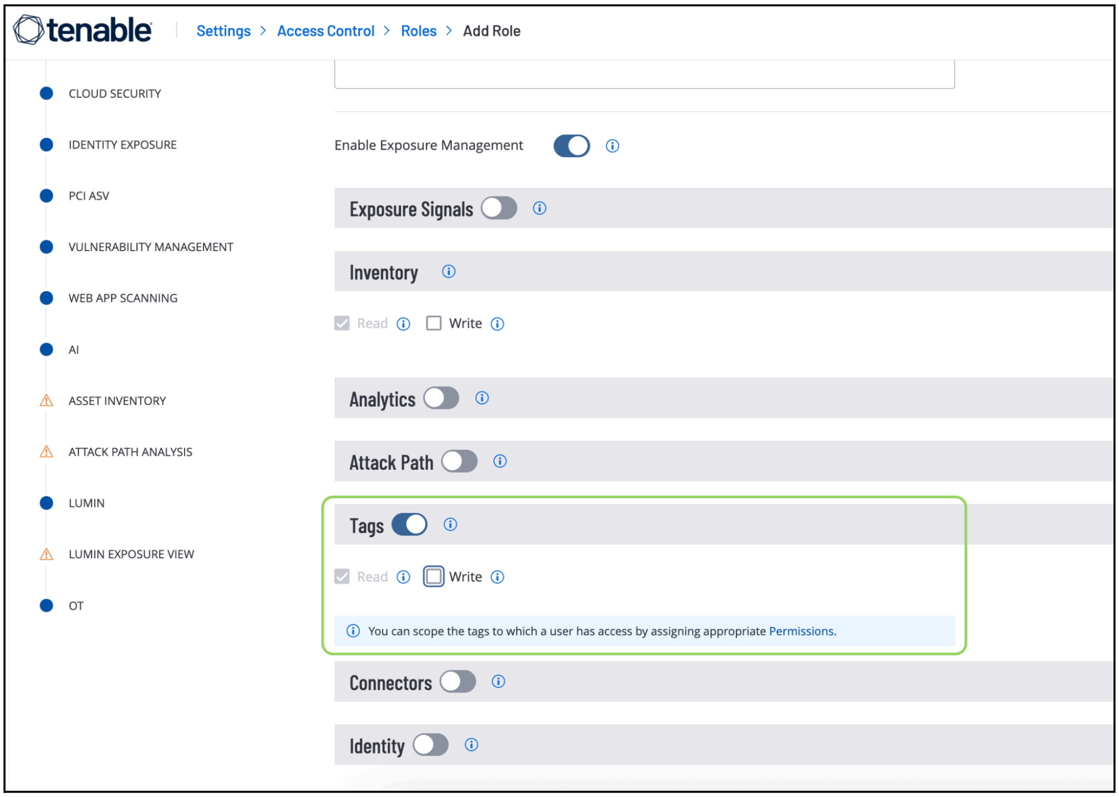
	Read	Write	Enable Builtin Card
DASHBOARDS	☑	☐	N/A
EXPOSURE VIEW	☑	☐	☐

Attack Path ○

Tags ○

Connectors ○

2. ✅ **New tag enforcement for Exposure Management**



Settings > Access Control > Roles > Add Role

- CLOUD SECURITY
- IDENTITY EXPOSURE
- PCI ASV
- VULNERABILITY MANAGEMENT
- WEB APP SCANNING
- AI
- ⚠ ASSET INVENTORY
- ⚠ ATTACK PATH ANALYSIS
- LUMIN
- ⚠ LUMIN EXPOSURE VIEW
- OT

Enable Exposure Management ●

Exposure Signals ○

Inventory

☑ Read □ Write

Analytics ○

Attack Path ○

Tags ●

☑ Read □ Write

You can scope the tags to which a user has access by assigning appropriate Permissions.

Connectors ○

Identity ○

3. ✅ **A new Read-Only role for Exposure Management and Vulnerability Management** which allows users to view and drill down into data only. This role cannot perform actions like creating, updating, deleting or exporting data. The read only access is configured per product area under the Exposure Management and Vulnerability Management role.

Action Required: Updating existing roles

Since we have introduced this new EM role, any previously custom role with access to *Attack Path Analysis*, *Exposure View* or *Asset Inventory* will need to be updated using the new EM role.

*Admins will need to **update** these custom roles by January 31st, 2026. If the new roles aren't updated and assigned to the appropriate users by admins, those existing roles will no longer have access to the EM workspace and will need to request access starting February 1st, 2026.*

Please view the FAQ below for additional information on the required actions and RBAC functionality.

Frequently Asked Questions

Q: Why did I receive an email from Tenable about the new RBAC updates?
A: You have been contacted because your organization has one or more custom role(s) assigned to users/groups involving access to *Lumin Exposure View*, *Attack Path Analysis*, and/or *Asset Inventory* that will require your admin to take action.

Q: What is the immediate action that I need to take?
A: Please work with your administrator to update those existing roles *using the new exposure management role* that is now available and assign to the appropriate users. More detailed instructions are listed below.

Q: Why does my administrator need to update my role when I already have a custom role assigned to me?
A: We are introducing new logic with the new Exposure Management role. This will supersede all custom roles with access to *Lumin Exposure View*, *Attack Path Analysis*, and/or *Asset Inventory.*

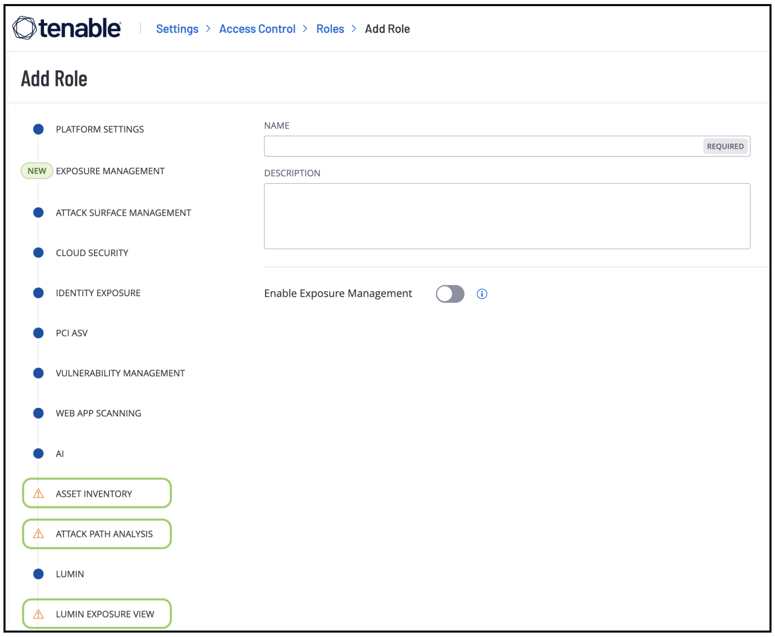
Q: When must users have their roles updated to the new Exposure Management role?
A: New roles need to be updated and assigned to those users/groups by *January 31st, 2026*.

Q: What happens if all of the roles aren't updated by January 31st?
A: Users who have not had their role updated will no longer be able to access the Exposure Management workspace and will need to reach out to an administrator.

Q: How do I update those roles?
A: You will need to work with your administrator to update your role using the new Exposure Management role. Please see our explainer video that outlines the steps needed to update the role. For any questions, please reach out to your Customer Success Manager.

Q: What's happening to the individual roles for *Lumin Exposure View, Attack Path Analysis, or Asset Inventory?*

A: The individual legacy roles for *Lumin Exposure View, Attack Path Analysis, and Asset Inventory* will remain available until January 31st, 2026. There is a period of time where the legacy roles and new exposure management role exist at the same time. We are referring to this as *parallel support* to provide access to both as you navigate the transition over.



Q: What happens if an admin updates permissions to *existing custom roles* only and does not update with the new Exposure Management role?

A: Updating the current role is not a viable solution and users will no longer be able to access the Exposure Management workspace on February 1st, 2026. You will need to reach out to an administrator to regain the proper access.