Tenable One AI Exposure User Guide

Last Revised: November 12, 2026

Copyright © 2026 Tenable, Inc. All rights reserved. Tenable, Tenable Nessus, Tenable Lumin, Assure, and the Tenable logo are registered trademarks of Tenable, Inc. or its affiliates. All other products or services are trademarks of their respective owners.

Table of Contents

Welcome to Tenable One AI Exposure **26**

Console (Using the UI) **27**

Overview 27

Get Started with Tenable One AI Exposure 27

Overview 27

Prerequisites 27

License 27

Log In and Configure 28

Analyze and Assess 28

Navigate the Console 29

Log In to Tenable One AI Exposure 29

Left-Hand Navigation Menu 29

In-Product Help 30

Help Tools 31

User Profile 32

Search across the Console 33

At-a-Glance Resource Profile View 34

Color-Coded Risk Severity 36

Filter Data 37

Filter Data in Tables 38
Filter Data by Account Scope 39
FAQ: Tenable One AI Exposure 40
Supported AI Tools and Applications 41
AI Conversations Viewer Role Requirements 41
Data Retention 41
File and Prompt Size Limits 42
Tenable One Data in Tenable One AI Exposure 42
Explore 44
Inventory 44
View Your AI Asset Inventory 44
Filter the Asset Inventory 46
Export Inventory Data 48
Search across Your Inventory 49
Supported Cloud Resources 50
View Resource Details 52
View Resources in AI Provider Console 52
Mark Sensitive Resources 53
Apply Labels to Resources 54
Get More Details about a Resource 54
View and Manage Associated Risks 55

Explorer 55
Saved Queries 56
Create a New Query 56
Choose an Object 57
Native vs Generic Objects 57
Filter Results 58
Filter by Object Property 58
Filter by Multiple Values 59
Filter by Entity Traits 59
Query Property for Blank Values 60
Filter by Raw Cloud Provider Source Data 60
Filter by Multiple Object Properties 62
Filter by Relations 63
Hide/Show a Query Group 63
Combine Filters with Operators 63
Add Relationships 65
Use Relationship Filters 66
Create a Join 66
Aggregate Results with Group By 67
Save a Query 68
Query Widgets 69

Edit a Query 69
Create a Custom Policy from Query 70
Supported Objects 71
Create a Report from Query Data 72
Create a Finding Automation from a Query 72
Export Query Data 75
Display Query Results 75
Table View 75
Graph View 76
Sample Queries 77
Query for Findings That Violate Compliance Standards 77
Query for Public-Facing Virtual Machines 77
Query for Resources with Inactive Owners 78
Reference: Finding Properties 79
FAQ 80
Queries 81
Queries Table 81
Open a Query in Explorer 82
Monitor a Query 82
Query Widgets 83
Duplicate a Query 83

Delete Custom Queries 84
AI Conversations 84
Conversations Column Data 84
View Conversation Details 85
Software 86
View AI-Related Software Packages 86
Software Packages Column Data 87
Risks 89
AI Posture Findings 89
Navigate the Findings Page 89
Export Finding Data 92
Manually Close a Finding 93
Reopen a Finding 94
Trigger Actions Based on Findings 94
Trigger an Action for a Single Finding 95
Trigger an Action for Multiple Findings 96
Track Jira and ServiceNow Tickets 98
View Finding Details 99
View Finding Activity 99
Remediate Findings 100
Manually Remediate Findings 100

Remediate with One-Time Credentials 100
AI Activity Detections 101
Navigate the Activity Detections Page 102
Export Finding Data 103
Comment on an AI Activity 104
Trigger Actions Based on Detections 104
Trigger an Action for a Single Activity 104
View Activity Detection Details 106
View Activity 106
AI Activity Issues 107
Navigate the Activity Detections Page 108
Export Activities Data 109
Comment on an Activity Issue 110
Close an Activity Issue Manually 110
Reopen an Activity Issue 111
Trigger Actions on AI Activity Issues 111
Trigger an Action for a Single Activity Issue 112
Trigger an Action for Multiple Issues 113
View Activity Details 115
View Activity Issue Details 115
Add a Comment for an Activity Issue 116

Supported Languages for AI-Powered Features 116
Policies 117
AI Policies 117
Manage Policies 117
Policy Column Data 118
Enable and Disable Policies 118
AI Activity Rules 119
Activity Rules Column Data 120
View Activity Rule Details 121
Manage Activity Rules 122
Enable and Disable Activity Rules 122
Classification Rules 123
Reports 124
Reports 124
Create a Report 124
Duplicate a Report 125
Report Types 126
View and Edit Scheduled Reports 127
Access Historical Reports 127
Other Ways to Export Data 128
Settings 128

Audit 128
Access Management 129
Users and Groups 129
Add a New User 130
Add a New Group 133
Inherited Users 136
Built-in Roles and Permissions 137
Single Sign-On 143
Enable Login via Tenable One 144
Enable Login via AWS Identity Center (SAML 2.0) 144
Enable Login via Google 147
Enable Login via Google Using OIDC 147
Enable Login via Google Using SAML 147
Add Support for Google Groups 148
Enable Login via Microsoft Entra ID 149
Enable Login via Microsoft Entra ID Using OIDC 149
Enable Login via Microsoft Entra ID Using SAML 150
Add Support for Microsoft Entra ID Groups 152
Add Support for Microsoft Entra ID Groups Using OIDC 152
Add Support for Microsoft Entra ID Groups Using SAML 153
Enable Login via Okta 154

Add Support for Okta Groups 155
Enable Login via OneLogin 155
Add Support for OneLogin Roles 157
Enable Login via Ping Identity 159
Add Support for Ping Identity Groups 160
Enable Login via JumpCloud 161
Add Support for JumpCloud Groups 163
Enable Login via Custom SAML 2.0 Provider 164
Add Support for Groups 165
Console Timeout Settings 166
Inactivity Timeout 166
Session Timeout 166
Roles 167
Common Use Cases 167
Create a Custom Role 168
Edit a Custom Role 169
Duplicate a Role 169
Delete a Custom Role 169
Available Permissions 170
Permission Dependencies 173
Organization 173

Projects 173
Who Can Create a Project? 174
Supported Features 175
Add a Project Folder 175
Add a Project 176
Grant Access to a Project Scope 179
Move a Project 180
Delete a Project 181
Filter Console Data by Projects 181
View Projects 182
Export Project Data 183
Accounts 183
Manage Your Accounts 184
Accounts Column Data 184
Manage Code Accounts 185
View Account Details 186
Account Management Options 187
Troubleshoot Onboarding Issues 188
Account Status 188
Security 189
Configure Data Masking 189

Integrations 191
View Integration Details 191
Integrations Table 191
Add a New Integration 192
Core Concepts 194
Product Security and Privacy 194
Hosting Regions 194
Tenable Console URL 195
Data Segregation 195
Data Encryption 195
High Availability and Disaster Recovery 195
Compliance and Certifications 195
Annual Penetration Tests 196
Key Management 196
Authentication 196
Password Policy 197
Timeout Settings 197
Account Hierarchy and Folders 197
Automatically Update Folder Structure 200
Account Moves and Parent Folder Dependencies 200
Custom Policies and Exclusions 201

Automations, Scheduled Reports, and Other Dependencies 202
Advanced Use Case Examples 203
FAQ 204
Create Account Folders 204
Account Scopes 206
Filter Console Data and Configure Features by Account Scope 207
Supported Features 208
Account Inheritance 209
How Projects Work 209
How Projects Work 210
When to Use Projects 211
Common Project Use Cases 211
Create Projects for Product Groups 212
Create Projects for Business Functions 212
Create Projects for Development and Production Accounts 213
Create Projects for Application and Service Boundaries (Azure) 215
Supported Features 216
Project Permissions and Capabilities 216
Project Permissions 217
Propagation 217
Effective Permissions 218

Finding Lifecycle 218
Finding Lifecycle Example 218
Finding Status 219
Open Findings 220
Ignored Findings 221
Closed Findings 221
Connect **223**
AI Platforms 223
Connect Microsoft Copilot 223
Set Up Microsoft Entra Graph API Access 223
Configure Power Platform Security Roles and Application User 224
Create a Custom Security Role 224
Create an Application User 226
Connect Microsoft Copilot 228
Connect OpenAI ChatGPT 228
Create an Admin Key 229
Locate Your Organization ID and Workspace ID 230
Connect ChatGPT Enterprise 230
Connect Google Gemini 231
Data Synchronization Limitations 235
Gems 236

Conversations 236
Connect Anthropic Claude 236
Create the Compliance API Key 237
Connect Anthropic Claude 238
Connect Homegrown AI Applications 238
Prerequisites 239
Step 1: Create an Integration for a Homegrown AI Application 239
Step 2: Authenticate API Requests 240
Step 3: Send Conversation Data from Your AI Application 240
Request Parameters 240
Message Object Fields 241
Example Request (GraphQL) 242
Step 4: Retrieve Analysis Results (Optional) 243
Request Parameters 243
Response Fields 243
Example Request (GraphQL) 244
Step 5: Verify the Integration 244
View Analysis Results in the Console 245
AWS 245
AWS Overview 245
Considerations for Connecting an Organization versus Individual Accounts 246

Account Architecture 246
Accounts with Monitoring/Remediation Permissions 247
CloudTrail Connected 247
No CloudTrail Connected 247
Accounts with CloudTrail Permissions 248
AWS Required Permissions 249
Appendix I: AWS IAM Policies 250
Tenable Monitoring Policy (Read-Only) 250
Tenable Remediation Policy (Read-Write) 254
CloudTrail Policy 256
Data Resources Scanning Policy (Data Protection) 257
EC2 Instance Scanning (Workload Protection) 258
ECR Scanning Workload Protection Policy 260
Terraform Policy 261
Amazon Bedrock Invocation Logging 261
JIT Policy for AWS Account Access 262
Management Account for Account Access 262
Delegated Administrator Account for Account Access 264
JIT Policy for Application Access 264
Management Account for Application Access 264
Delegated Administrator Account for Application Access 265

AWS CloudTrail 265
Benefits of Granting CloudTrail Access 267
Enable Granular Recommendations Based on Data Events 267
CloudTrail Deployment 268
KMS Key in Different Account 270
Connect an AWS Account 271
Onboard an AWS China Account 278
Connect an AWS Organization 280
Connect an AWS Organization 281
Prerequisite 281
Connect an Organization 281
Next Steps 285
AWS FAQ and Troubleshooting 286
Access to Us-East-1 Region 286
AWS Console Access to Account 286
Exclude an OU or Account from Organization 287
GetObject Permission for Elastic Beanstalk Buckets 287
Need for Both Custom Policy and SecurityAudit Policy 287
New AWS Services and Permissions 288
Update the Integration Name for the Organization 288
ECS Task Definitions in Inventory 288

Multi-Region CloudTrail 289
Account Status and Troubleshooting 289
CloudTrail Status 291
Enable Amazon Bedrock Activity Monitoring 292
Supported APIs and Models 292
Prerequisites 293
Step 1: Enable Amazon Bedrock Model Invocation Logging 293
Step 2: Grant AI Exposure Access to the Amazon S3 Bucket 294
KMS Key in Different Account 296
Step 3: Verify Logging 297
Troubleshoot Missing Data 297
View Logging Details in the Console 298
Azure 298
Azure Overview 298
Connection Considerations 299
Azure Required Permissions 299
Microsoft Entra ID Permissions 300
Update Permissions for Tenable App 301
Azure Permissions 301
Connect a Microsoft Entra ID Tenant 310
Connect a Microsoft Entra ID Tenant 311

Manual App Registration (China Only) 312
Next Steps 313
Connect an Azure Organization 314
Prerequisites 314
Connect an Organization 314
Manually Deploy an Azure Organization 317
Next Steps 319
Connect an Azure Subscription 319
Prerequisites 319
Connect a Subscription 320
Manually Deploy an Azure Subscription 322
Next Steps 323
Azure FAQ and Troubleshooting 324
Azure Subscription and Organization FAQs 324
Pair Organization with Microsoft Entra ID 324
Exclude a Folder or Subscription from Organization 324
Minimum Permissions for Microsoft Entra ID User 325
Key Vault Reader Role Assignment 325
Update the Integration Name for the Organization 325
Microsoft Entra ID FAQs 326
Handling Unused PII 326

Required User Permissions for Authorizing App 326
Connecting Public vs. China Microsoft Entra ID Tenants 327
Just-in-Time (JIT) Access Support 327
Subscription Status and Troubleshooting 327
Google 328
GCP Overview 328
Cloud Events Data 330
Add VPC Service Control Exceptions 330
Google Required Permissions 332
Google Workspace Permissions 332
Required Permissions 332
GCP Project and Organization Permissions 335
Org-Level Custom Role for Single-Project Connections 338
Connect a Google Workspace 339
Prerequisites 339
Add a Workspace 340
Grant Permissions via Custom Role (Recommended) 342
Grant Permissions via Domain-Wide Delegation (Advanced) 343
Manually Deploy a Google Workspace 344
Add Tenable as an Allowed Domain 345
Added IAM Capabilities with Domain-Wide Delegation 346

Update the Integration Name 347
Connect a GCP Organization 347
Prerequisites 347
Connect an Organization 348
Manually Deploy a GCP Organization 351
Create a Service Account for Tenable 352
Authorize the Service Account at the Org Level 353
Configure Audit Logs 353
Connect a GCP Project 356
Prerequisites 356
Connect a Project 356
Manually Deploy a GCP Project 359
Create a Service Account for Tenable 359
Authorize the Service Account at the Org Level 360
Authorize the Service Account at the Project Level 361
Configure Audit Logs 362
Create a Custom Role with Org-Level Permissions 363
Google FAQ and Troubleshooting 364
GCP FAQs 364
Exclude a Folder or Project from an Organization 365
Grant Organization-Level Permissions 365

Project Is Pending Deletion 365
User in Domain Considered External 365
Update the Integration Name for the Organization 366
Terraform Deployment 366
Google Workspace FAQs 366
Service Account Token Creator Role 366
Service Account Impersonation vs. Service Account Key 367
Super Administrator User (Advanced) 367
Domain-Wide Delegation (Advanced) 368
Quota Administrator Role (Legacy) 369
Project Status and Troubleshooting 370
Workspace Status and Troubleshooting 371
Ticketing and ITSM 372
Jira 372
Before You Begin 373
Set Up an OAuth 2.0 Credential 373
Set Up a Jira User 374
Add a Jira Instance 375
Add a Jira Space 376
Allow Jira Issue Transitions 377
Sample Jira Issue 379

ServiceNow 380
Before You Begin 380
Add an Instance 381
Sync Incident States with Finding Statuses 383
Use Additional Fields in Incidents 384
Supported Fields 386
Sample ServiceNow Incident 386
SIEM 387
Datadog 387
Add a Datadog Organization 387
View Tenable Findings in Datadog 388
Sample JSON 389
QRadar 390
Add a QRadar Server 390
View Tenable Findings in QRadar 393
Sample JSON 395
Splunk 396
Add a Splunk Instance 396
View Tenable Findings in Splunk 398
Sample JSON 398
SQS Queue 400

Add an SQS Queue 400
Sample JSON 404
Offboarding Cloud Accounts 404
Offboard AWS Accounts 405
Offboard Azure Subscriptions 406
Offboard GCP Projects 407
Offboard OCI Tenancy 407
Webhooks 408
Webhooks 408
Add a Webhook 408
Microsoft Sentinel (via Webhook) 409
Prerequisites 410
Create a Custom Table 410
Copy the DCR and DCE Values 412
Create a Logic App with Managed Identity 413
Grant the Logic App Access to the DCR 414
Create a Sentinel Webhook Integration in Tenable 415
View Data in Microsoft Sentinel 415
Sumo Logic (via Webhook) 416
Send Data to Sumo Logic 416
Sample JSON 418

Telegram (via Webhook) 419
Create a New Telegram Bot with BotFather 419
Use AWS to Create a CloudFormation Stack 421
Configure the SSM Parameter 421
Create a CloudFormation Stack 422
Create a Telegram Webhook Integration in Tenable 424
Configure In-Account Scanning 425
Required Alibaba Cloud Permissions 426
Disk Securing for Scanning 434
Trust Policy 435
Permissions 435
Required AWS Permissions 436
Required Azure Permissions 440
Required GCP Permissions 442
Required OCI Permissions 443
Resources Provisioned per Region 443
Alibaba Cloud 444
AWS 445
Azure 447
GCP 449
OCI 450

Welcome to Tenable One AI Exposure

About Tenable One AI Exposure

AI Exposure extends attack surface protection into the AI landscape, giving you continuous visibility into AI tool usage across your organization. It detects unmanaged shadow AI and tracks user activity across platforms such as ChatGPT Enterprise, Microsoft Copilot, Anthropic Claude, and Google Gemini.

Console (Using the UI)

Overview

Get Started with Tenable One AI Exposure

Overview

AI Exposure extends attack surface protection into the AI landscape, giving you continuous visibility into AI tool usage across your organization. It detects unmanaged shadow AI and tracks user activity across platforms such as ChatGPT Enterprise, Microsoft Copilot, Anthropic Claude, and Google Gemini.

AI Exposure provides visibility into sensitive data within AI prompts, responses, and files. This visibility enables you to enforce policies and prevent data leakage. AI Exposure also identifies misconfigurations in AI models and applications, detects malicious behavior, and risks for runtime interactions with AI.

Tenable recommends following these steps to get started with AI Exposure data and functionality.

Prerequisites

Before you begin configuring and using AI Exposure:

- Review the Tenable One Deployment Guide.
- Ensure access to at least one supported AI application, for example, ChatGPT Enterprise or Microsoft Copilot.

License

To use AI Exposure, you purchase licenses for assets. These are resources identified by or managed in your Tenable products. Each product has a different asset type. For more information, see the Tenable One Licensing Quick-Reference Guide.

Tenable offers two versions of Tenable One: **Tenable One Foundation** and **Tenable One Advanced**. Both versions include AI Exposure.

- **Tenable One Foundation** includes AI Inventory.
- **Tenable One Advanced** includes AI Inventory + Posture findings.
- The **Tenable One AI Governance** add-on is available for both Foundation/Advanced at an additional cost and includes runtime monitoring (activity detections).

Log In and Configure

To log in and configure AI Exposure:

1. Log in to the AI Exposure.
2. Integrate AI applications with AI Exposure.
3. Connect cloud providers to create resource and software inventories and view posture risk.
4. Assign the AI Conversations role to view user activity.
5. Configure predefined Policies to control how AI Exposure monitors your environment.
6. Configure Activity Rules to detect all AI activities within your environment.

Analyze and Assess

Perform analysis on your data within AI Exposure:

- Access the AI Dashboard page for a unified view of AI usage and risk, surfaced through key KPIs.
- Review the Inventory page for a complete list of AI tools, agents, and models discovered across your organization's cloud and SaaS environments.

- Review the Findings page to resolve posture gaps and misconfigurations detected by evaluating your AI services against configured policies.
- Review the Activity Detections page to view specific events or activities, such as messages or responses that triggered an activity rule.
- Review the Activity Issues page to view related detections grouped into a single activity issue for critical and high-severity cases.
- Review your users' AI Conversations to enforce AI security.

These processes help protect your AI attack surface and ensure your organization's AI use stays within approved policies and standards.

Navigate the Console

The Console is the central control panel for Tenable. The Console provides a comprehensive interface for managing and assessing the security posture of your entire cloud environment. This article guides you through the primary navigation elements to help you find what you need.

Log In to Tenable One AI Exposure

To log in to AI Exposure:

1. In a supported browser, navigate to https://cloud.tenable.com/. The login page appears.
2. Type your Username and Password credentials.
3. Click **Login**. The Workspace page appears.
4. Click the AI Exposure tile.

   The AI Exposure interface appears.

Left-Hand Navigation Menu

When you log into the Console, the Dashboard page appears. From here, you can investigate potential risks in your environment via Dashboard widgets, or use the left-hand navigation menu to go to relevant areas of the product.

If you're an Administrator user, you will also see the Settings menu.

> **Note:** The menu items listed below may be filtered by your selected Focus View.

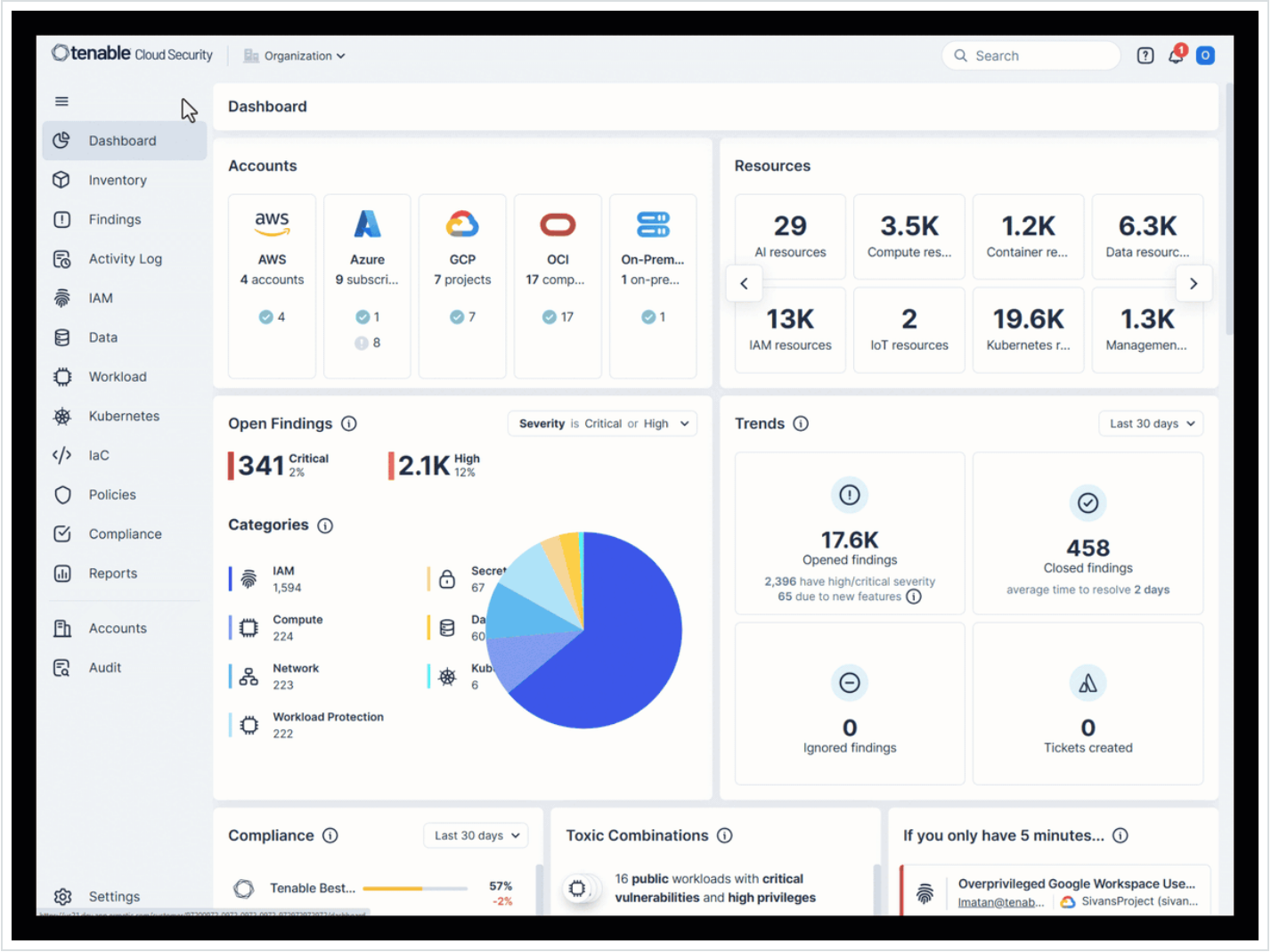
Menu Item	Description
Dashboards	Comprehensive overview of AI activity across your organization. It lists the active users, AI agents, a trend of AI activity and findings.
Explore	Centralized asset view of all cloud resources identified by AI Exposure, along with additional tools to analyze and investigate security data, query permissions, review activity logs, and identify anomalous behavior.
Risks	Assess and prioritize security risks, including findings, activity detections, and activity issues.
Policies	Define and enforce automated guardrails for identities, resources, preventing unauthorized AI activity across your environment.

In-Product Help

Access in-app help directly from the Console. Product documentation is accessible both via:

- Search
- Contextual help links
  

To access the full documentation site, click the **Docs portal** link at the top of the slideout panel.



Help Tools

Click the question mark icon at the top right of the Console to access various help tools.

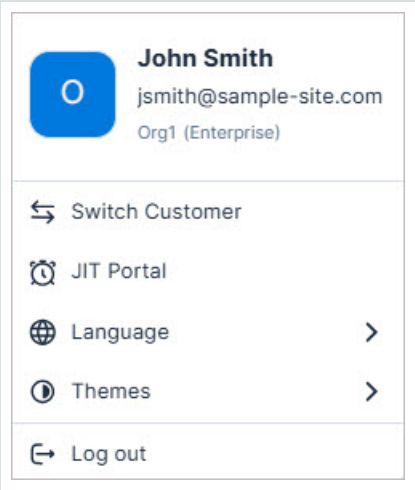
- **Release Notes** – Descriptions of the latest features and improvements added to AI Exposure in the last release. Check this frequently for updates. See Release Notes.
- **Documentation** – Comprehensive product documentation that helps you find answers to your technical questions and learn how to use AI Exposure.
- **API Explorer** – Use GraphiQL, an in-browser tool, to write, validate, and test GraphQL queries. See API to learn more.

- **Feedback** – Submit feedback to the AI Exposure product team directly from the Console.
- **Contact Us** – See Contact Support.

User Profile

Click the icon at the top right of the Console to open your user profile. From here you can perform a variety of actions:

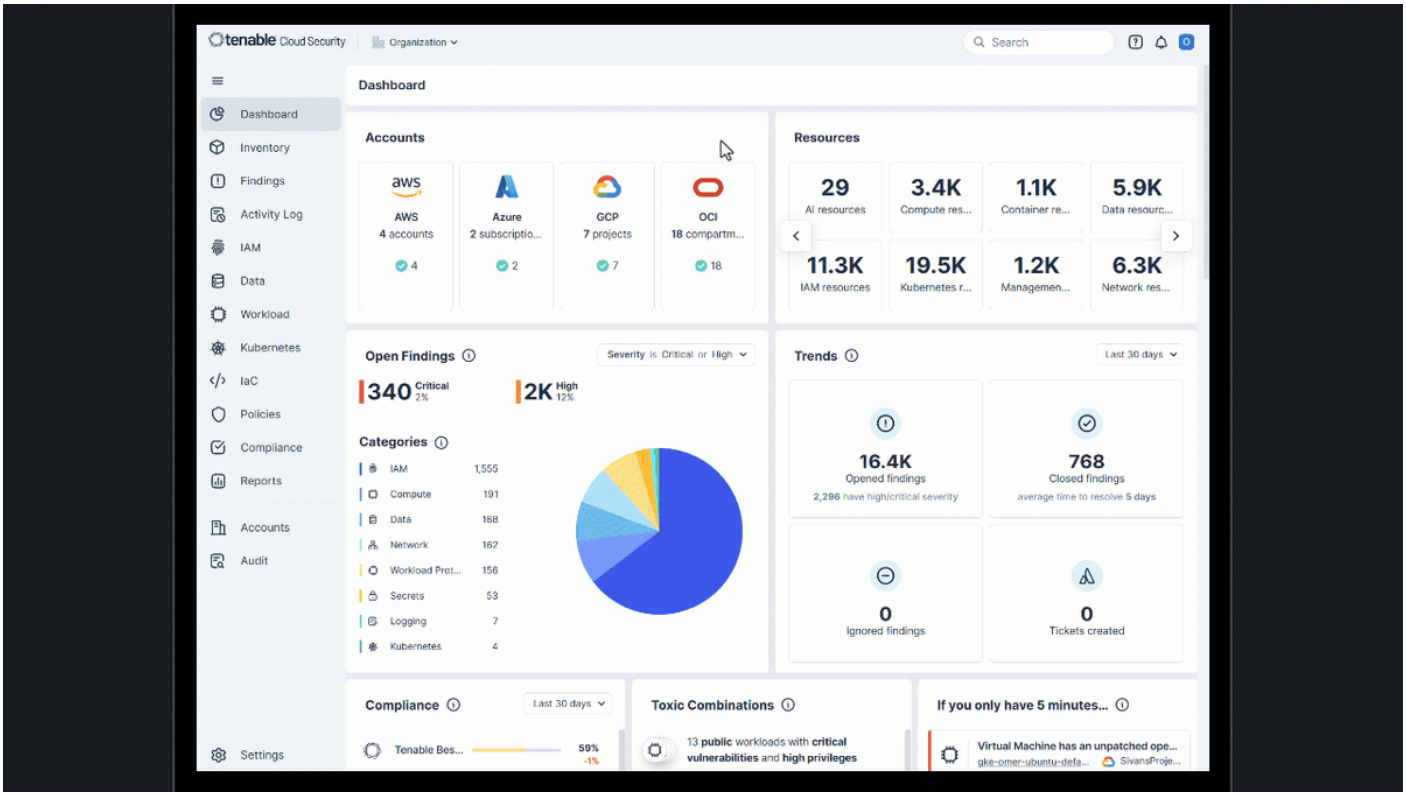
- *See user details*:
  - User name / email address
  - Company/organization name
  - License type
  - Customer ID. Used to register to the Tenable Community. See Contact Support for more information.
- *Navigation*:
  - [JIT users only] Go to **JIT Portal** / **Console**. If you have access to both the AI Exposure Console and the JIT Portal, you can easily navigate back and forth between them.
  - [Multi-tenant only] **Switch Customer** to view data for a different organization.
- *Language*
  - English
  - Japanese
- *Themes*
  - Light Mode
  - Dark Mode
  - System
- *Log out*



Search across the Console

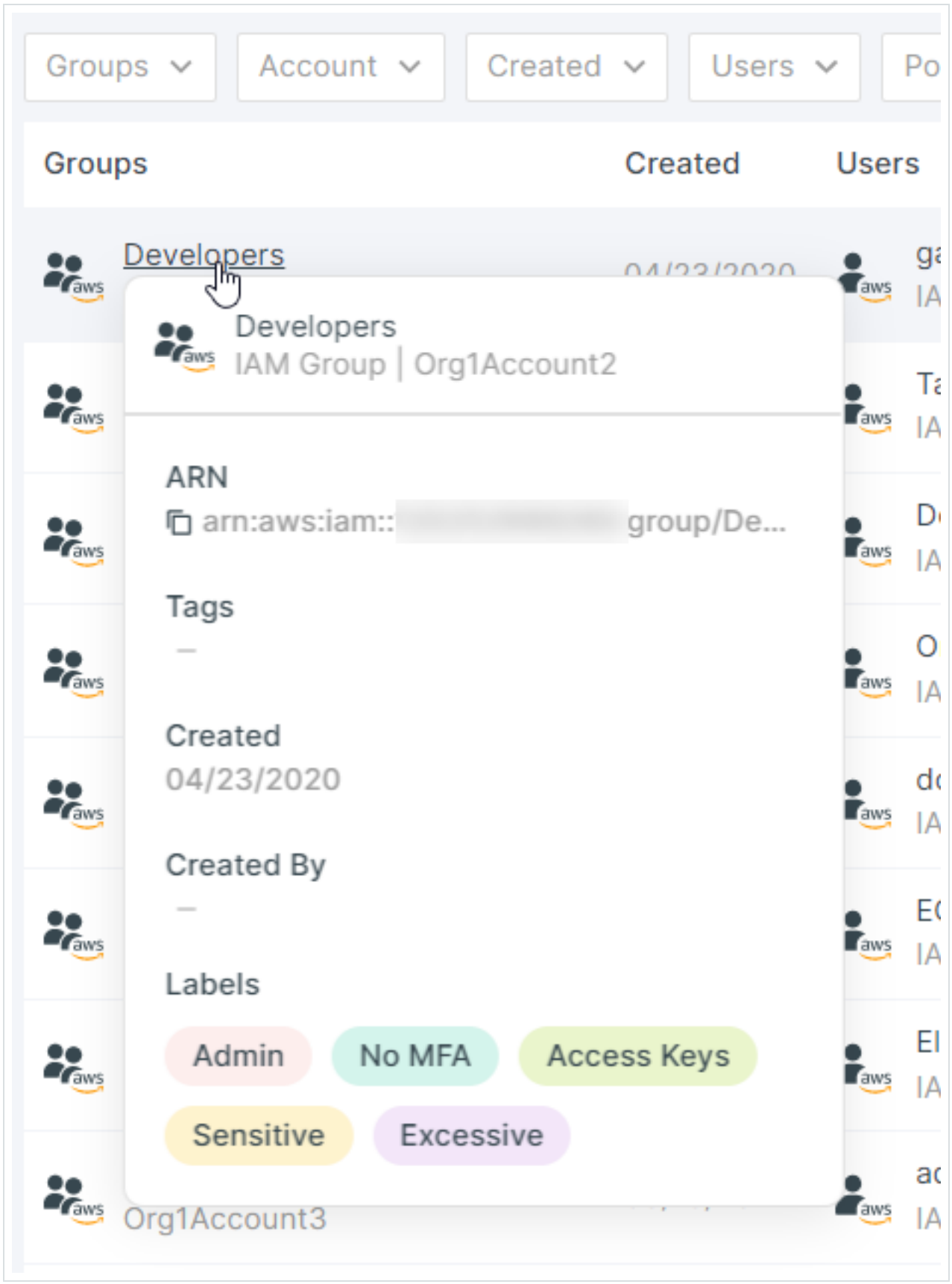
Use the global search to find *resources* (Inventory), *vulnerabilities*, *policies*, *pages*, and *documentation* across your environment, providing a single, streamlined way to navigate and find what you need.

- The search bar appears at the top right of the AI Exposure Console, regardless of which page you're on.
- Click **Ctrl + K** to access via keyboard shortcut.
- (Optional) Select a scope in the account scope dropdown to limit the search to a subset of accounts.
- *Inventory* results are divided by category (for example, AI or IAM) across your organization.



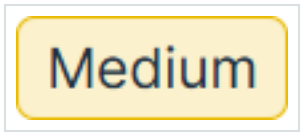
At-a-Glance Resource Profile View

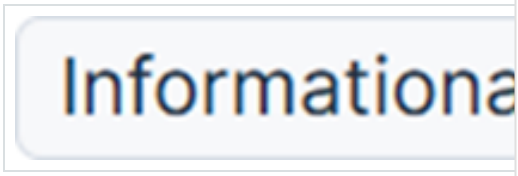
Hover over any resource name in the Inventory, access graph (permission mapping), Activity Log, or Findings page to see a mini profile view that contains a selection of the most important information about the resource. This allows you to learn more about the resource without context-switching to another page to view this information.


Groups
Account
Created
Users
Po
Groups
Created
Users
Developers
Developers
IAM Group | Org1Account2
ARN
arn:aws:iam::
group/De...
Tags
—
Created
04/23/2020
Created By
—
Labels
Admin
No MFA
Access Keys
Sensitive
Excessive
Org1Account3

Color-Coded Risk Severity

Throughout the Console, different colors/icons are used to indicate the various risk severity levels that resources and findings pose to your organization. The following table maps these colors to their respective severity levels, and describes their implications within your cloud environment.

COLOR	ICON	STATUS	DESCRIPTION	EXAMPLE
		**Critical**	Immediate action required	Administrative user with permissions to sensitive data, which aren't in use.
		**High**	Handle as soon as possible	Non-admin user with permissions to sensitive data, which aren't in use.
		**Medium**	Potential risk	User with permissions to sensitive resources such as bucket lists, but without permissions

COLOR	ICON	STATUS	DESCRIPTION	EXAMPLE
				to read the bucket contents.
	Low	**Low**	Monitor for escalation	User with limited use of assigned permissions.
		**Informational**	Useful information	A new GCP project was added to your organization.
	N/A	**In Compliance** (*Compliance only*)	No action necessary	No excessive permissions detected. Policy Rules and best practices met.

Filter Data

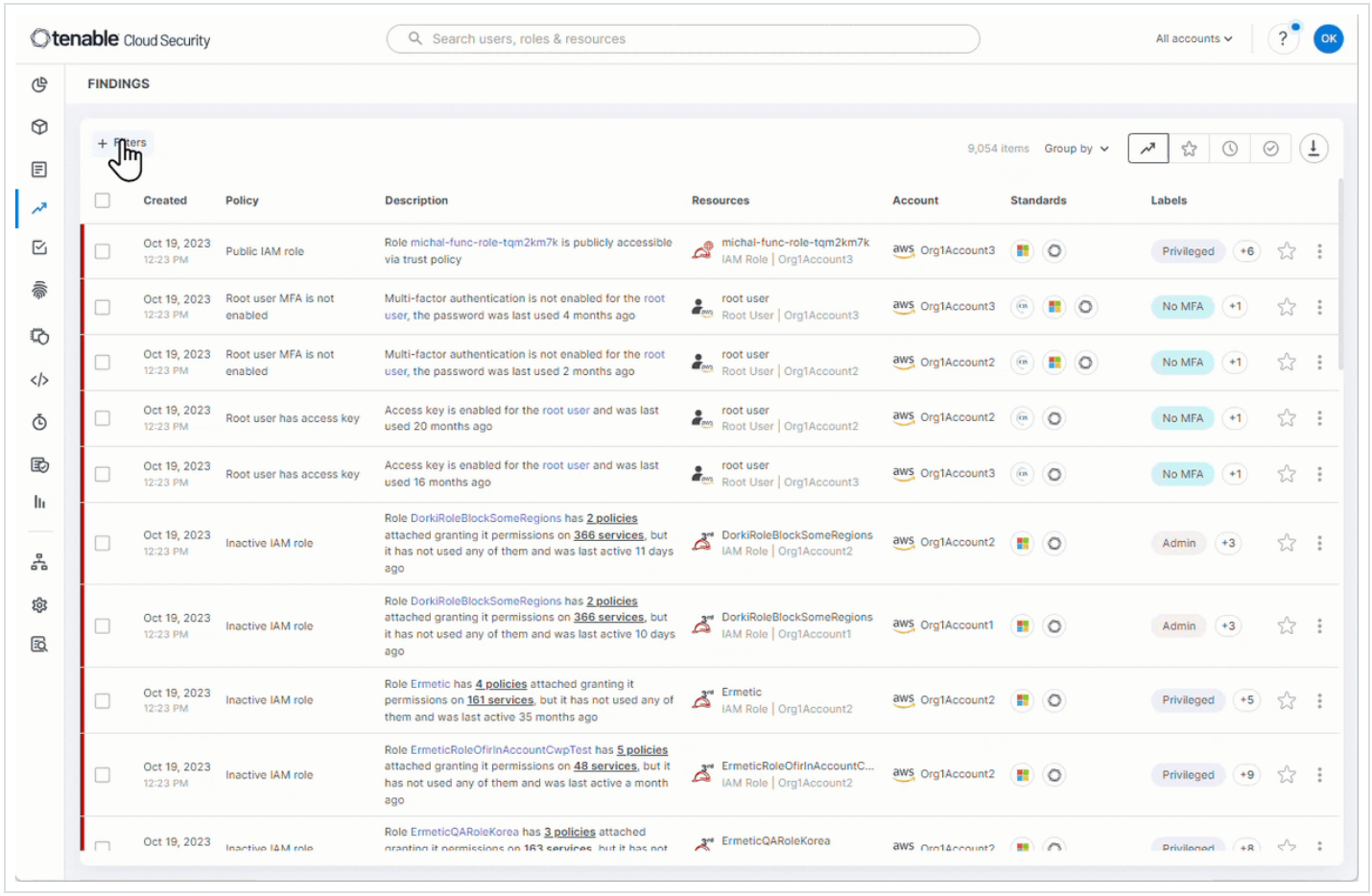
You can filter data throughout the Console in various ways to help you find the specific resource, finding, activity, or other data that you're looking for.

Filter Data in Tables

Use the filters at the top of tables throughout the Console to narrow the scope of the visible data:

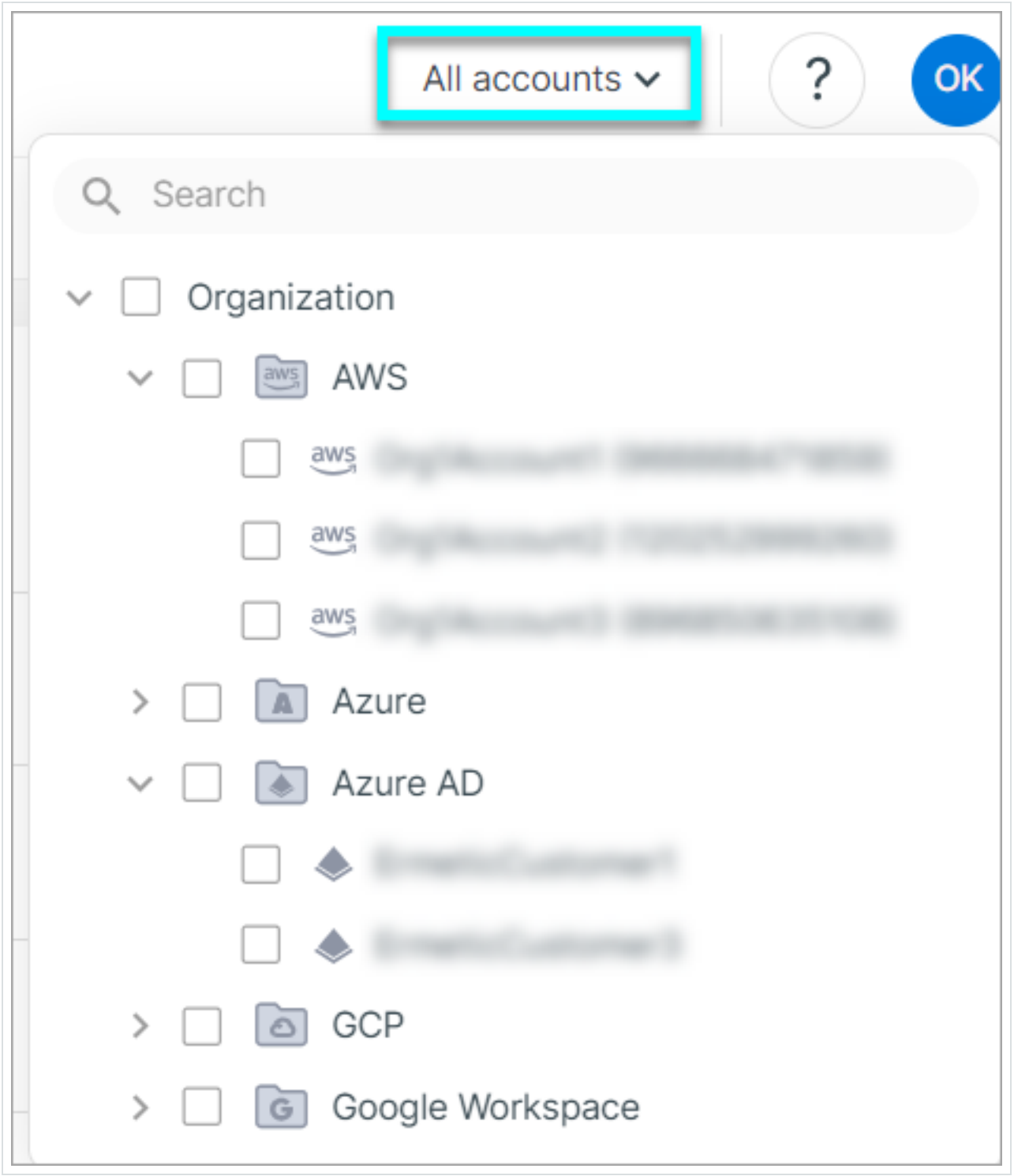
- Each Console page has a set of filters that are displayed by default, based on common usage for each page.
- To add a filter, click on the + Filters button and choose an item/s or type a relevant search term.
- When you add or remove filters, your changes are saved, and those filters will appear by default the next time you navigate to the page. Only the filters themselves will be saved. Any values selected for the filters will not be saved when you leave the page.
- To filter the table by entries that don't have a value for a particular field (empty values), select either:
  - **(Blanks)** – For example: You can filter for all findings that dont have any tickets (e.g. Jira issue).
  - **Not set** (used for date fields, which sometimes contain values which are not dates). For example, you can filter for all *Ignored* findings without an *Ignored Until* date (i.e. that are ignored permanently). Or for entities with an *Expiration* time of *Never/Null*.
- To filter the table by entries that match the search term, click **Select matches**. This option supports up to 65,000 returned entries. If more entries are returned, the option is disabled, and you will need to narrow down the search to use it.
- For some filters that generally contain many values, you can click **Only** to the right of a value to only filter by that value, effectively clearing any other previously selected values.
- Some entities may not have a value for a particular filter/column. To filter the table by all entities that have *any* value for the filter, click **Select all**.
- When you select items from filters, and then navigate back to the filter, any selected items appear on top.
- Click **Clear** to remove any selected filters.

- Compliance standards which have been disabled will not appear in relevant reports. See Compliance Column Data for more information.



Filter Data by Account Scope

You can filter data by account scope (including IdPs) throughout the Console using the **All accounts** dropdown at the top right of the Console. See Account Hierarchy and Folders to learn more.



FAQ: Tenable One AI Exposure

This article contains a list of frequently asked questions related to AI Exposure.

Supported AI Tools and Applications

> Why is activity from Google applications like Google Docs not visible?

AI Exposure supports Gemini chats only and not Google applications, such as Google Docs. This is a Google limitation as Google does not log interactions from its applications.

AI Conversations Viewer Role Requirements

> Why is user activity not visible and the Active Users dashboard widget blocked in the AI Exposure Console?

To view user activity, you must have the **AI Conversations Viewer** role.

To add this role:

1. Go to **Settings** > **User Management**.
2. Click **Add Role Assignment**. The **Add Role Assignment** dialog box appears.
3. From the **Roles** drop-down menu, select **AI Conversations Viewer**.
4. Assign the role to a specific user or group.
5. Click **Save**.

Data Retention

> How long does AI Exposure retain my data?

AI Exposure retains data as follows:

Data Type	Retention Period
AI Conversations	90 days

Data Type	Retention Period
Detections	1 year
Closed findings	1 year
Open findings	Indefinitely

File and Prompt Size Limits

> Is there a size limit for files or prompts that AI Exposure syncs and scans?

Yes. AI Exposure applies the following limits:

- AI Exposure does not sync files larger than **50 MB**. In **Conversations**, an indicator shows that a file was attached, including available metadata such as the file name and size. However, you cannot select or download the file.
- AI Exposure does not currently run detections on files. This applies to files of any size.
- For prompts larger than **200 KB**, AI Exposure syncs the prompt but does not scan its content for sensitive data or policy violations.

Tenable One Data in Tenable One AI Exposure

Tenable One Vulnerability Management sends all software components detected in your environment to the **Software** page in AI Exposure. This creates a unified software inventory that includes components detected on cloud workloads and hosts monitored by Tenable One Vulnerability Management.

AI Exposure imports software data from Tenable One Vulnerability Management into the **Self-Managed** scope. By default, users with a role assignment that includes the **Organization** scope in AI Exposure can view this data.

The unified **Software** page provides:

- **Org-wide visibility** – A unified view of all AI-related software that Tenable detects, including sanctioned and unsanctioned components.
- **Shadow AI detection** – Identification of unsanctioned AI libraries and packages installed on hosts and cloud workloads.
- **Unified inventory** – A single location for your complete AI software inventory eliminating the need to switch between Tenable One Vulnerability Management and AI Exposure.

Important: AI Exposure does not automatically import the Role-Based Access Control (RBAC) configured for this data in Tenable One Vulnerability Management. To prevent unintended access, Tenable removes AI Exposure access from all custom roles in Tenable One that include it. To restrict access for users who require limited data visibility, you must reconfigure RBAC in AI Exposure.

Note: Tenable One Vulnerability Management sends only new findings to AI Exposure. Allow up to 30 days for the findings in both applications to reach full parity.

To configure user access in AI Exposure:

1. In the AI Exposure console, go to **Settings** > **Users and Groups**.
2. For each user who requires access to AI Exposure and has an assigned role with an **Organization** scope, determine the access requirements:
    - If the user requires access to Tenable One Vulnerability Management software data, no action is required.
    - If the user must not have access to Tenable One Vulnerability Management software data, remove the role assignment, and then create a new role assignment that excludes the **Self-Managed** scope.

      To grant a user access to some scopes but not **Self-Managed** data, create a project that includes all scopes except **Self-Managed**, and assign that project instead. For more information, see Projects.
3. After you configure all users and role assignments in AI Exposure, re-enable access from Tenable One:
    1. Enable AI Exposure in a custom role.
    2. Assign the custom role to the relevant users.

For more information, see Manage Custom Roles in the *Tenable One Vulnerability Management User Guide*.

Explore

Inventory

View Your AI Asset Inventory

You can use the Inventory view to analyze the operational characteristics of your AI services. For example, you can perform the following tasks:

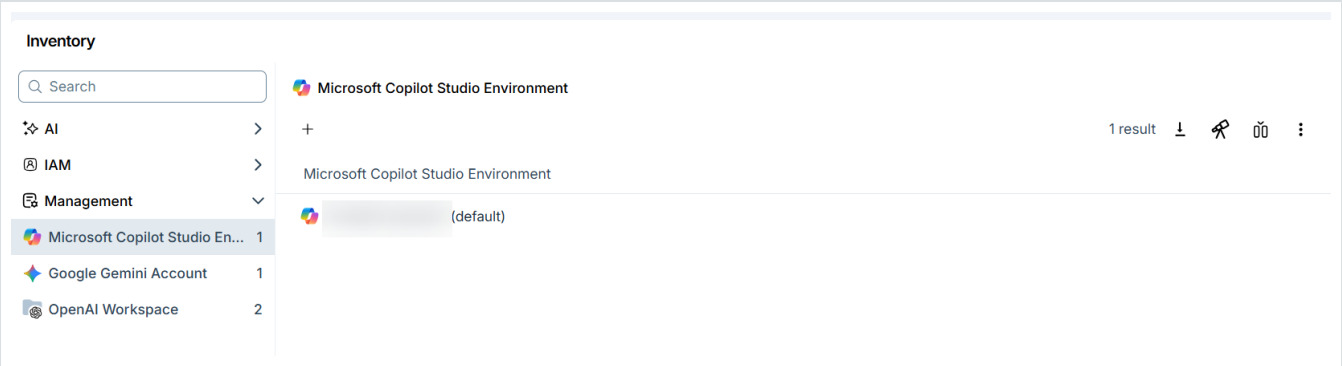
- Identify all AWS Bedrock Agents in your environment running with high-privilege IAM execution roles.
- Review all OpenAI Workspace GPTs configured with public or "Anyone with link" visibility that may expose sensitive instructions or tools.
- Monitor all Azure Microsoft Foundry model deployments across your organization and the accounts they belong to.
- Track all GCP Vertex AI Workbench instances and identify configurations that have not synchronized recently.

The Inventory view lists all AI resource types collectively across cloud and SaaS providers, without separating by provider. To view resources for a specific provider, use the Organization selector at the top of the Console.

The left pane of the **Inventory** page includes three main navigation categories:

- **AI** – A catalog of AI resources and services across cloud providers, including models, agents, and workspaces.
- **IAM** – An inventory of identity and access management entities that interact with AI services, including users, roles, and groups.

- **Management** – The top-level accounts and workspaces that govern AI service configurations, providing organizational context for the resources tracked under AI and IAM.



Each resource type displays columns specific to that type. For example:

- AWS Bedrock Agent shows: Name, Account, Creation Time, Status (Prepared/NotPrepared/Failed), Role, Encryption, Encryption Key.
- OpenAI Workspace GPT shows: Name, Account, Visibility (GPT Store / Workspace / Invite only / Anyone with link), Owner, Creation Time.

To view your asset inventory:

1. In the Tenable One AI Exposure Console, go to **Explore** > **Inventory**.
2. From the Inventory view, search for and select the relevant AI category and resource type that you want to view. For example, **AI** > **AWS Bedrock Agent**.
3. Use the **Column Picker** button on the top right of the table to choose which columns to display.
4. Filter the asset inventory to modify the scope of the visible data. Available default filters include Name, Account, Region, and Labels. Additional filters vary by resource type.
5. Review detailed resource metrics by clicking any row in the table. A detail panel opens displaying the following options:

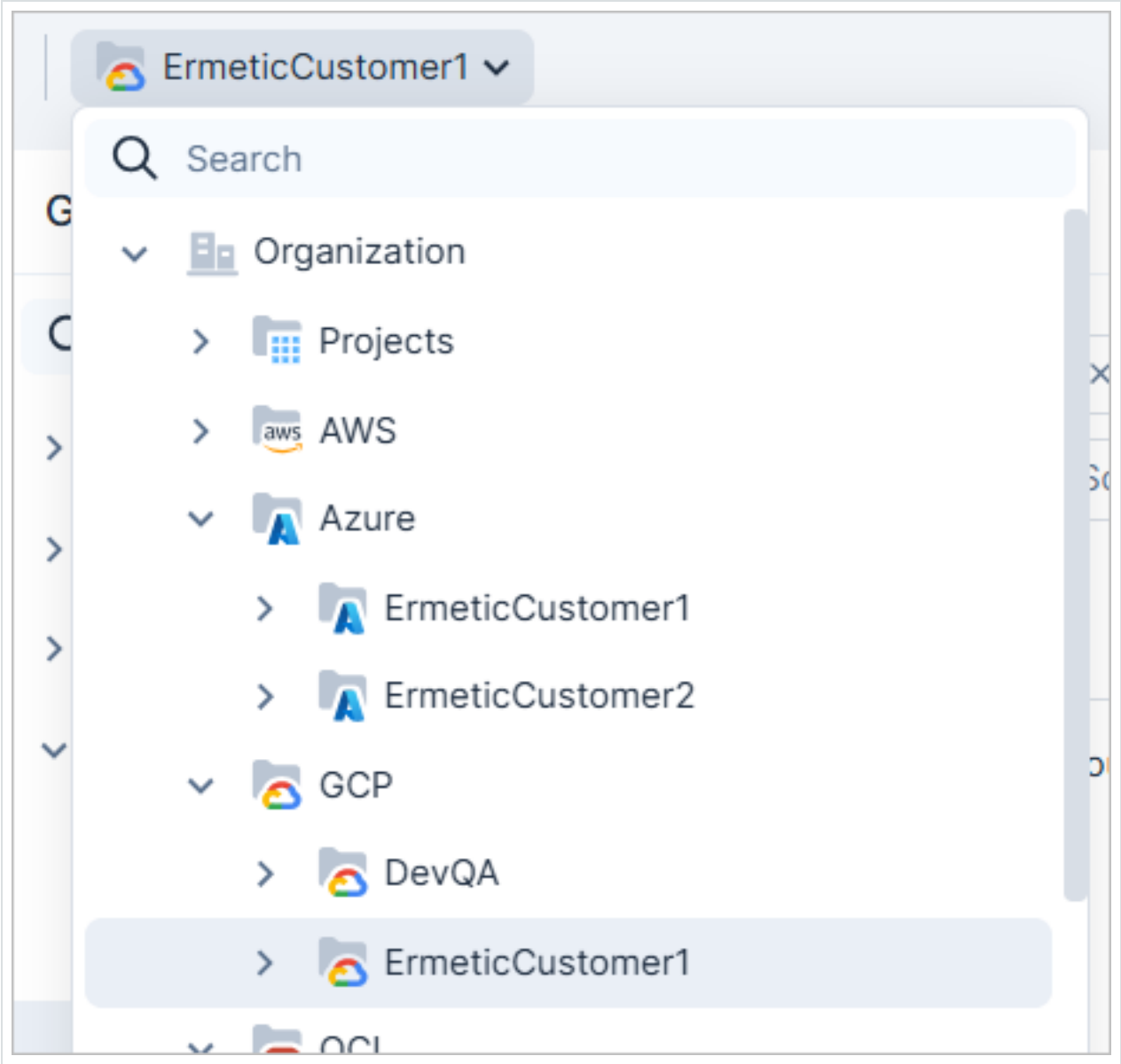
- **Overview** tab – Displays resource properties such as Type, Creation Time, Sync Time, Visibility, Owner, Builder Name, Categories, Description, Instructions, and Tools.
- **AI Findings** – Displays the number of AI-specific findings associated with the resource, with links to investigate further.

Filter the Asset Inventory

Use the filters at the top of the table to narrow the scope of the visible data (for more information, see Filter Data):

- Click the **Add Filter (+)** button to add a filter.
- To filter the table by a specific search term, click **Select matches**.
- Some resources may not have a value for a particular filter/column. To filter the table by all resources that have *any* value for the filter, click **Select all**.

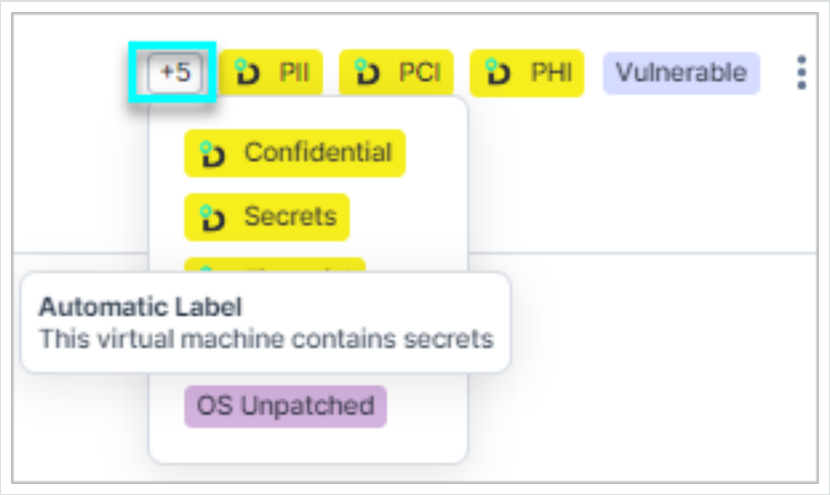
You can also filter by organization or account at the top of the **Inventory** page to see only resources for a specific account or a group of accounts. For more information, see Account Hierarchy and Folders.



The following global filters apply to all resource types:

- **Labels** – Displays all labels applied to the resource, applied by one of the following methods:
  - Manually (via **Settings** > **Inventory** > **Labels**).
  - Automatically based on tag, or tag key and value (via **Settings** > **Inventory** > **Labels**). Labels created in this way have a flag icon next to them.
  - Automatically by the system.

Hover over a label tag for more information. If a resource has multiple labels, click the icon to view them.



See Apply Labels to Resources for more information.

- **Findings** – Displays all findings associated with resources of the specified type.
- **Finding Severity** – Indicates the severity of any findings associated with the resource:

  Critical

  High

  Medium

  Low

  Informational

  If there are multiple findings for the resource, the highest-severity finding is displayed. For example, if the resource has two associated findings, one with Critical severity and one with Medium severity, the Findings column will display Critical.

Export Inventory Data

Export all data for any AI inventory view by resource type. The data exports according to the current filters applied to the table. The output file uses the CSV format and includes all relevant resource data, including the URL of each resource page in the Console.

Alternatively, you can create/schedule an Inventory report for all resource types within a given account scope.

To export inventory data:

1. In the AI Exposure Console, go to **Explore** > **Inventory**.
2. From the Inventory view, select the relevant category and resource type.
3. Apply any relevant filters.
4. From the top-right corner of the table, click **Export**.

Search across Your Inventory

Use the global search to find AI resources across your entire multi-cloud environment. Searches filter data by the organization or account scope you select.

The search supports resource properties including resource name, account, and provider-specific identifiers.

The search bar appears at the top of the AI Exposure Console, regardless of which page you view.

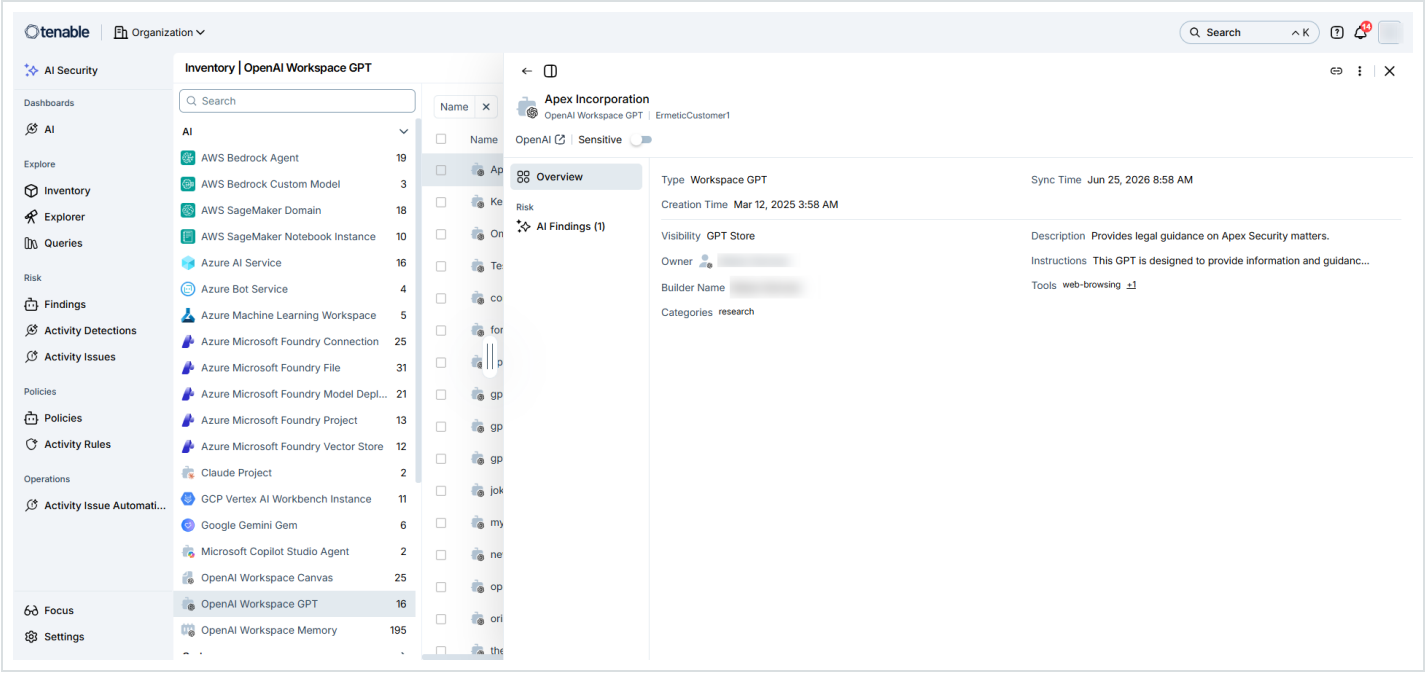
> **Note:** You can also use the search function to find *policies*, *pages*, *documentation*, and *vulnerabilities* across your environment, providing a unified way to navigate the console.

To search across your inventory:

1. (Optional) Select a scope in the organization selector to limit the search to a subset of accounts.
2. Enter a search term in the **Search** box at the top of the Console.

As you type, a list of matching results appears along with the total count. Results break down by resource type, allowing you to review matching results by type. You can scroll across the full list of results.

3. Click the relevant resource to view its details.



Supported Cloud Resources

Provider	Resource Type
AWS	Bedrock Agents
AWS	Bedrock Action Group
AWS	Bedrock Custom Models
AWS	Bedrock AgentCore Gateway
AWS	Bedrock AgentCore Harness
AWS	Bedrock AgentCore Memory

Provider	Resource Type
AWS	Bedrock AgentCore Outbound Auth API Key
AWS	Bedrock AgentCore Outbound Auth OAuth
AWS	Bedrock AgentCore Outbound Auth Payment
AWS	Bedrock AgentCore Policy Engine
AWS	Bedrock AgentCore Runtime
AWS	Bedrock AgentCore Workload Identity
AWS	Bedrock Data Source
AWS	Bedrock Guardrail
AWS	Bedrock Knowledge Base
AWS	SageMaker Domain
AWS	SageMaker Notebook Instance
Azure	AI Search
Azure	Bot Service
Azure	Machine Learning Workspaces
Azure	Microsoft Foundry Agent
Azure	Microsoft Foundry Connection
Azure	Microsoft Foundry Dataset
Azure	Microsoft Foundry File

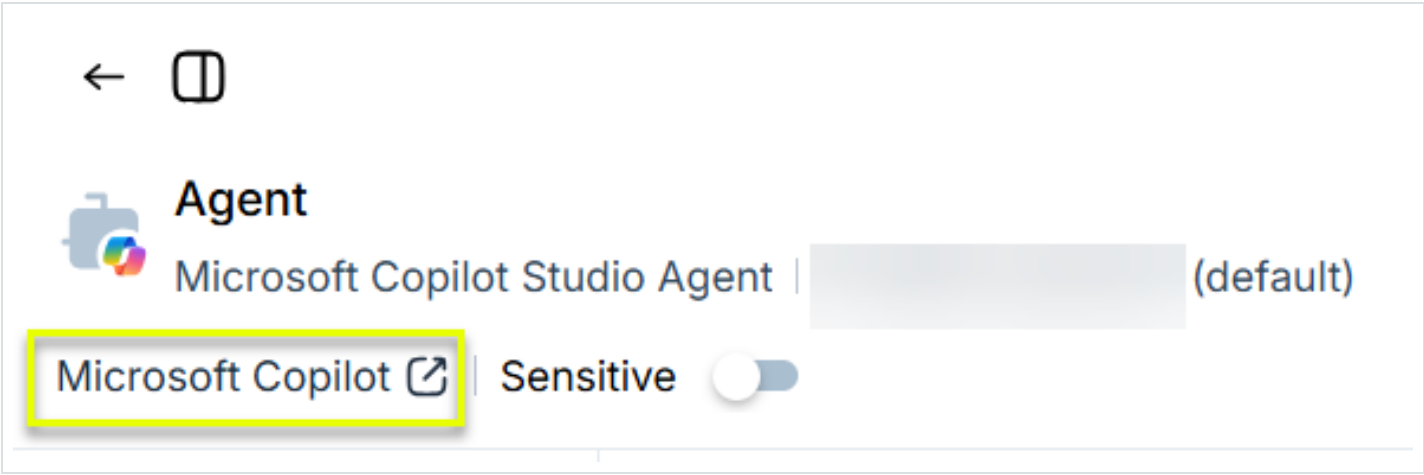
Provider	Resource Type
Azure	Microsoft Foundry Guardrail
Azure	Microsoft Foundry Index
Azure	Microsoft Foundry Knowledge Base
Azure	Microsoft Foundry Knowledge Source
Azure	Microsoft Foundry Model Deployment
Azure	Microsoft Foundry Project
Azure	Microsoft Foundry Vector Store
GCP	Vertex AI Workbench Instance

View Resource Details

You can view the details of a resource from the **Inventory** page. The Resource Details page provides a comprehensive evaluation of a specific AI resource within your Tenable One AI Exposure inventory.

View Resources in AI Provider Console

Click the link below the resource name to view it in the relevant AI console.



Mark Sensitive Resources

Mark resources as sensitive to accomplish the following tasks:

- Elevate the priority of any findings associated with the resource or identities that have access to the resource.
- Label a resource as sensitive within AI Exposure.

Marking resources as sensitive is available for most resource categories, excluding Identity and Access Management (IAM) across all AI service providers.

To mark a resource as sensitive:

1. In the AI Exposure Console, click **Explore** > **Inventory**.
2. From the Inventory view, select the relevant category and resource type. For example, select **IAM** > **Microsoft Entra ID User**.
3. Click the resource to view its details. The resource details panel appears.
4. Click the **Sensitive** toggle below the resource name in the header.

A red circle appears at the top-right corner of the resource throughout the AI Exposure Console to indicate that this resource is marked as sensitive.



Apply Labels to Resources

Manually apply relevant, predefined custom labels to resources to add context for risk assessment. This action enriches your AI Exposure environment by correlating labels with factors like excessive permissions and network exposure.

> **Note:** AI Exposure also automatically applies built-in system labels to resources, as relevant.

To manually apply a label to a resource:

1. In the AI Exposure Console, click **Explore** > **Inventory**.
2. From the Inventory view, select the relevant category and resource type. The Resource Details panel appears.
3. In the upper-right corner, click the three dots button, and then click **Edit labels**.
4. Select the checkboxes for the relevant labels you want to add or clear the checkboxes to remove labels.
5. Click **Save**.

Get More Details about a Resource

Click **Overview** to see extensive characteristics about the resource, including the following examples:

- General resource properties, such as resource type, account, and assigned tags.
- The owner of the resource, the authentication mode (if applicable), and whether authentication triggers automatically.
- The environment, region, location, and the time of the last synchronization.
- Custom properties, which are user-defined parameters such as ownership, team, cost center, or other internal metadata.

View and Manage Associated Risks

In the **Risk** left-hand menu section, click any of the following options to view potential risks associated with the resource:

- **AI Findings**
- **Cloud Findings**
- **Threat Detections**
- **Vulnerabilities**
- **Malicious Files**

Explorer

The Explorer page is the central place for investigating your cloud environment. Use queries across all your resources and findings to precisely identify, prioritize, and remediate risks using a wide range of filters and properties.

When you enter the Explorer page, you have several ways to begin a search:

- **Select a query** from the Popular Queries list. This list shows your recently used Saved Queries first, followed by a set of recommended built-in queries.
- **Select a saved query** from the *Saved queries* section.
- **Build a new query** by selecting an object and applying filters.

Once a query is open, you can modify it and choose to **Save** or **Save as** to create a new custom query.

The query results can be displayed in a table or graph. Learn more.

Saved Queries

Saved queries allow you to reuse a specific query configuration without rebuilding it each time.

To open a saved query from the:

- **Explorer page**:
  1. Go to **Explore** > **Explorer**.
  2. Click the **Saved queries** button.
  3. Filter or search using any of the following:
     - Categories
     - Search bar
     - View filters by query type: *All*, *Built-in*, *Public*, or *Private*
- **Queries page**:
  1. Go to **Explore** > **Queries**.
  2. Click on the query you want to open.

There are two types of saved queries that you can use:

- **Built-in queries** – Out-of-the-box queries provided by Tenable One AI Exposure. You cannot edit or delete these queries. You can modify and click **Save as** to create a custom query.
- **Custom queries** – Created by you or other users. A custom query can be *Public* or *Private*. You can update or duplicate any custom query.

Create a New Query

Create a new query by selecting an object to investigate and refining the results with filters, operators, and relationships. The sections below walk you through each step:

1. Choose an Object
2. Filter Results
3. Combine Filters with Operators
4. Add Relationships
5. Aggregate Results with Group By
6. Save query
7. Edit query

Choose an Object

Every query starts with an object, such as a virtual machine, identity, container, or policy. The object determines which properties and relationships you can filter on.

To choose an object:

1. Go to **Explore** > **Explorer**.
2. Select the **Find Resource** control to open the object selector. You can:
    - **Search** for an object by name.
    - **Pick from recently used objects**.
    - **Browse categories** to view related objects (for example, selecting *Kubernetes* to see all Kubernetes resources).
    - **Scroll** through the full list of available objects.

After you select an object, the query builder opens and you can add filters, operators, and relationships to refine the results.

Native vs Generic Objects

When building custom queries, you can select from different types of objects to explore your environment. These object types are distinguished by their icons, which indicate their scope:

- **Native objects** (Cloud-specific icon e.g., AWS , Azure):
    - These represent objects that are unique to a particular cloud provider or offer more granular details for a specific platform's service (for example, *AWS EC2 Instance*, *Azure Virtual Machine Scale Set*). Selecting a *native* object allows you to query only objects from that specific cloud environment. *Use these when you need to target unique properties or details of a single cloud platform.*
    - While all available resources from your connected cloud environments are supported, not all of them will have every property available for filtering. Every resource you query will, at a minimum, have all the properties from the *Cloud Resource* object, in addition to any properties inherited from its specific unified resource type (for example., a GCP VM Instance inherits from both the *Cloud Resource* and the *Virtual Machine* types).
- **Generic objects** (Icon:).
    - These objects represent common resource types that exist across multiple cloud platforms (for example, *Virtual Machine* or *Identity*) or within a single platform (for example, *Google Identity*). When you query a generic object, you'll see all relevant instances (across platforms, or within a single platform) in a single, consolidated view. *This is ideal for getting a broad, cross-cloud overview.*
    - The **Cloud Resource** object is the highest-level generic object. It defines a base set of properties applicable to every resource, whether it is a generic or platform-specific type.

Filter Results

After you select an object as the core of your query, you can start filtering based on the object's properties.

Filter by Object Property

> **Note:** Custom properties that you define also appear as filters.

To filter by object property:

1. To the right of the selected object, click **+** (**Add filter**).
2. In the **Properties** section, search or scroll to find the relevant property. For example, *Name*.
3. Click the property name to add it as a criterion and then select a property *operator* and *value*. For example, for *Name*, you can select *operator*=**Contains** and *value*=**dev**.

Filter by Multiple Values

When you filter a text property with the **Equals** operator, you can enter several values at once. AI Exposure returns the resources that match any of the values. For example, use this to look up a list of hostnames from an incident ticket in one query.

To filter by multiple values:

1. To the right of the selected object, click **+** (**Add filter**).
2. In the **Properties** section, search or scroll to a property that contains text, such as *Name*, and click it.
3. In the operator drop-down box, select **Equals**.
4. In the value box, type or paste the values, with each value on its own line. For example:

```
web-prod-01
web-prod-02
db-prod-01
```

The filter appears in the query with the values separated by commas, for example: *Name equals web-prod-01, web-prod-02, db-prod-01*.

AI Exposure applies the following rules to the values you enter:

- Each line is one value. Commas do not separate values, so if you paste a comma-separated list, it's treated as a single value.
- Leading and trailing spaces are removed from each value and blank lines are ignored.

To exclude the resources that match any of the values, click **Not** next to the operator drop-down box.

Filter by Entity Traits

Filter cloud resources and entities by functional capabilities (Traits) to quickly find resources that share common characteristics, regardless of their specific service type.

1. To the right of the selected object, click **+** (**Add filter**).
2. In the **Properties** section, search for or select **Traits**.
3. Click the property name to add it as a criterion.
4. Select an operator (for example, **Is** or **Not**).
5. Select the specific traits you want to filter by, such as **Encryptable** or **Taggable**.

Query Property for Blank Values

Use the `is empty` operator to search for resources/findings where a specific property has no defined value. For example, use this operator to find all public-facing virtual machines across all cloud environments that are missing any tags.

Filter by Raw Cloud Provider Source Data

AI Exposure models the most common resource attributes as properties, such as **Name** or **Operating System Type**. When you need an attribute that is not a property, filter on **Source Data** instead. This property contains the JSON that Tenable received from the cloud provider for the resource.

The cloud provider defines the content and structure of this JSON. Tenable does not control it, and the provider can change field names, values, or structure at any time.

Source Data supports the following operators:

Operator	Use It To
Contains	Find resources whose JSON contains a text string anywhere. Click **Aa** for a case-sensitive match.
Matches pattern	Find resources whose JSON matches a pattern. Click **Aa** for a case-sensitive match.

Operator	Use It To
Matches JSON Path	Filter on the value at a specific location in the JSON.
Is empty	Find resources that have no raw JSON.

To exclude matching resources, click **Not** next to any operator.

Before you begin:

- Open a resource of the type you want to query and click the **JSON** tab. Use it to find the exact key names and structure. Key names are case-sensitive and can differ from the cloud provider's API documentation.

To filter on a specific JSON value:

1. To the right of the selected object, click **+** (Add filter).
2. In the **Properties** section, search for and click **Source Data**.
3. In the operator drop-down box, select **Matches JSON Path**.
4. In the **JSON Path** box, type a JSONPath expression that starts with `$`. For example, to find AWS EC2 instances without detailed monitoring, type `$.monitoring.state`, select **String** and **Equals**, and type `disabled`. [TBC: run this once in the Console to confirm it returns results]
5. Under **Conditional Logic**, select how to handle a path that returns more than one value (for example, an array):
    - **Match all** – every value must match. This is the default.
    - **Match any** – at least one value must match.
6. In the **Type** drop-down box, select the data type of the value: **String**, **Number**, or **Boolean**.
7. In the **Operator** drop-down box, select an operator. The available operators depend on the type. See the following table.

Type	Operators
String	Equals, Contains, Starts with, Ends with, Matches pattern
Number	Equals, Greater than, Greater than or equal to, Lower than, Lower than or equal to
Boolean	Equals

8. Set the value:
    - For **String** or **Number**, type the value in the **Value** box.
    - For **Boolean**, select **True** or **False**.

The filter appears in the query, for example: `Source Data matches JSON Path $.monitoring.state equals disabled`.

> **Note:** JSON paths are case-sensitive, and a path with the wrong case returns no results without an error. For example, `$.architecture` matches but `$.Architecture` does not. Always copy key names from the resource's **JSON** tab, not from the cloud provider's API documentation.

> **Note:** Some cloud providers store true and false as text, for example `"ebsOptimized": "false"`. The **Boolean** type does not match these values. If the value is in quotes on the **JSON** tab, select **String** and **Equals** and type `true` or `false`. The **Number** type does match numbers stored in quotes, such as `"coreCount": "1"`.

Filter by Multiple Object Properties

You can filter an object by as many properties as you want.

To filter by multiple properties:

1. To the right of the selected object, click **+** (**Add Filter**).
2. In the **Properties** section, search or scroll to find the relevant property. For example, *Creation Time*.

3. Click the property name to add it as a criterion and then select a property *operator* and *value*.
4. Repeat these steps to add additional properties.

> **Note:** By default, the `And` operator is used to connect multiple filters. To change this, click the three dots to the right of the filters and choose `Or`.

Filter by Relations

In addition to filtering by an object's direct properties, you can filter based on its connections to other resources.

To filter by a relation:

1. To the right of the selected object, click **+** (**Add filter**).
2. In the **Relations** section, search or scroll to find the relevant relationship. For example, *related to Cloud Resource*.
3. Next to the relationship click the inline **Filter** button. Alternatively, you can click **Join** to Create a Join.

Hide/Show a Query Group

You can temporarily disable a set of filters without deleting them from your query. This is a powerful feature for testing and troubleshooting. When you hide a group, its filters are removed from the query's logic and will no longer affect your search results. The group is still saved, allowing you to re-enable the filters instantly by selecting *Show group* at any time.

You can hide a group at any level of your query. For example, you can hide an entire parent group (which will also disable all filters nested within it) or you can hide individual filters within a group.

To hide/show a query group:

Click the three dots next to the relevant group and then click **Hide group**.

Combine Filters with Operators

When you add filters to your query, they interact using logical operators:

Operator	Details	Example
And Logic	By default, when you add multiple property filters (for example, *Name* contains *dev*, and *Labels* is *Privileged*), they are automatically combined with an AND logic. This means an entity must match all of those specified filters to be included in your results.	To find all AWS EC2 Instances that are running AND in production: `AWS EC2 Instance` + `Status` is `Running` + `Labels` is `Production` (This query returns only running EC2 instances that are tagged as in Production.)
Or Logic	To broaden your search, use Or logic. Choosing this allows you to define an alternative set of filters. Your query will then return entities that match either the first set of conditions OR the alternative set you define.	To find AWS S3 Buckets that are either publicly accessible OR not encrypted: `AWS S3 Bucket` + (`Access Level` is `Public` + `OR` + `Encrypted` equals `False`) (This query returns S3 buckets that are publicly accessible, or not encrypted, or both.)
Of Type Logic	The `Of Type` operator refines a query on a generic object by filtering for a more specific resource type. This allows you to select properties that are unique to that specific resource type.	To find all Virtual Machines that are specifically of the AWS EC2 Instance type and have a public network exposure: `Virtual Machine` + `Of Type` + `AWS EC2 Instance` + `Network Exposure is Public` (This query returns only AWS EC2 instances that match the specified criteria, even though you started with the broader "Virtual Machine" resource.)
Not Logic	The Not operator allows you	To find virtual machines that are NOT labeled

Operator	Details	Example
	to exclude entities that meet specific criteria. Choosing this allows you to invert the logic for the filters or groups of filters that immediately follow it. Your query will only return entities that do not satisfy the conditions specified after the Not operator.	as Privileged: `Virtual Machine` + `NOT` + `Labels is Privileged` (This query returns Virtual Machines that do not have the Privileged label.)
Complex Queries	By combining `And` (implicit), `Or`, and `Not` operators, you can create highly specific or broad queries to pinpoint exactly what you need.	To find virtual machines that are NOT a webserver with direct internet exposure OR a Windows machine with an Inactive label: `Virtual Machine` + `NOT` + `OR` (`Name contains webserver` + `Network Exposure is Internet (direct)` + `Operating System Type is Windows` + `Labels is Inactive`). (This query returns virtual machines that are neither publicly exposed web servers NOR inactive Windows machines.)

Add Relationships

The ability to query relationships between objects is at the heart of the Explorer. You can build powerful queries by leveraging these connections in two distinct ways:

- Use Relationship Filters
- Create a Join

Use Relationship Filters

This method allows you to find entities based on a specific property of a related object. When using this method, you are still querying a single object type, but you are filtering it based on its connections. You can add any number of relationship filters to your query to precisely narrow down your search.

Example query - Find all identities that have a critical finding:

> **Note:** Your query will return a list of identities that meet the criteria. The results table will only show information about the identities themselves.

1. Select **Identity** as your primary object.
2. Add a relationship filter and select **has Finding**.
3. Within the *has Finding* filter, add a nested condition for **Severity** and select **Critical**.

Create a Join

This method allows you to combine data from two different object types into a single result set, with each row displaying a unique combination of data from the joined objects. You can add up to ten joins to a single query to create highly complex and detailed result sets. You can add multiple joins in **parallel** (multiple joins branching off the same object) or **linearly** (joins branching off subsequent joined objects).

Example query - Find all findings and their associated identities that have a critical finding:

- By using a `Join`, your query will return a single table with combined information. In this example, each row will display a unique combination of an Identity and a Finding that meets your criteria, showing data from both objects simultaneously.
- You can toggle the `Join` to a `Left Join`, which will return all results from the primary object (on the left side of the query) even if there is no matching data in the joined object. This is useful for seeing a complete list of all items from the primary object.

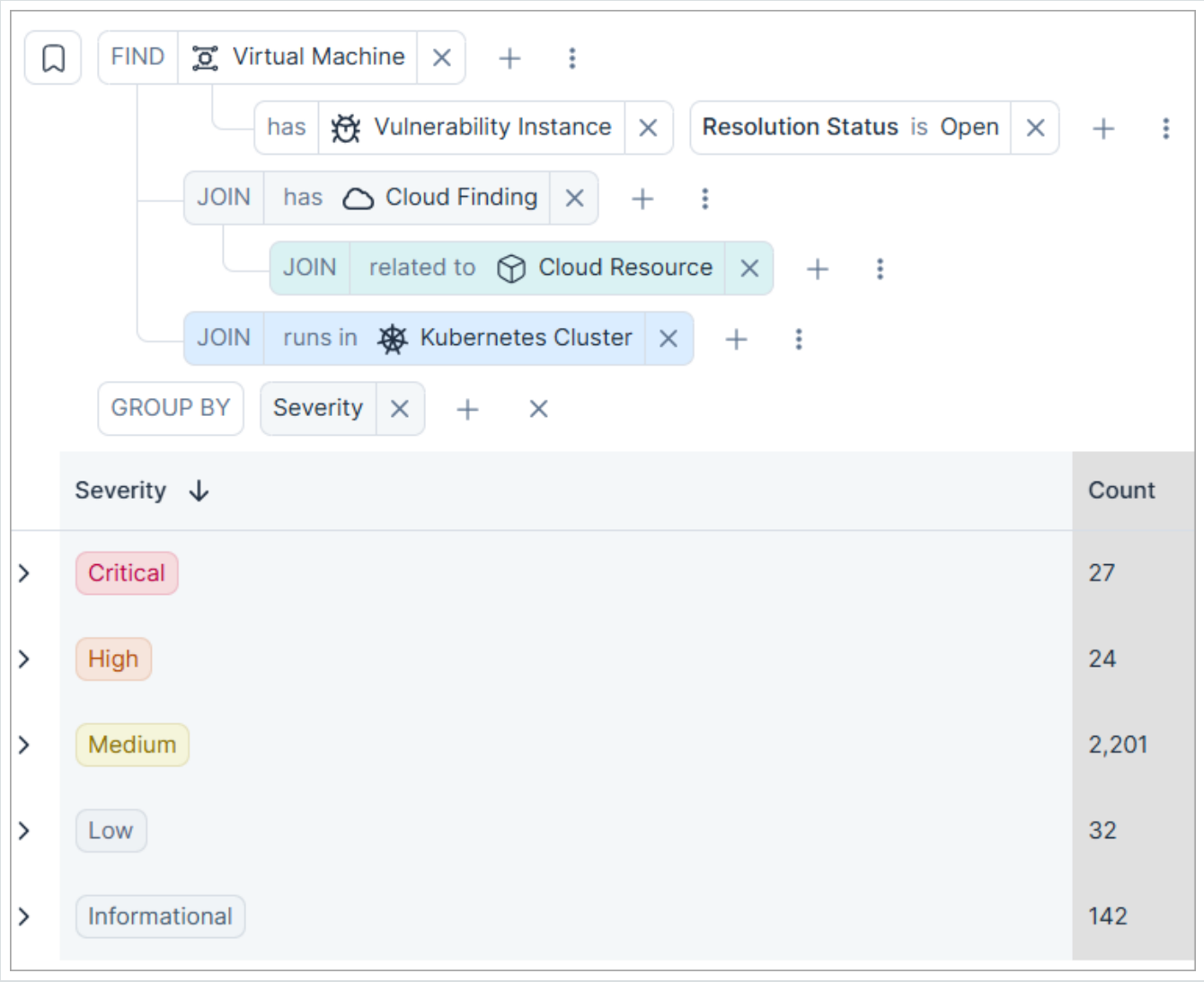
1. Select **Identity** as your primary object.
2. To the right of the selected object, click **+** (**Add filter**).
3. In the **Relations** section, search or scroll to find the relevant relationship. For example, *related to Finding*.
4. Next to the relationship, click the inline **Join** button.
5. Within the joined Finding object, add a nested condition for **Severity** and select **Critical**.

Aggregate Results with Group By

Summarize query data by specific properties, displaying results as counts in a simplified table view. For example, you can group a finding-related query by *Severity* to see a breakdown of results by severity level.

1. Click the three dots icon next to the root entity and select **Group by**. A GROUP BY element is added to the bottom of the query.
2. Next to the GROUP BY element, click the **+** (Add) button and select the grouping target. You

can choose to group data by the root entity or any joined objects.



Save a Query

After building or modifying a query in **Explore** > **Explorer**, you can save it for future reuse.

Changes you make to a saved query remain temporary until you save it.

To save a query:

1. Select **Save** or **Save as**:
    - **Save** updates the current custom query. Save is disabled for built-in queries.
    - **Save as** creates a new custom query.
2. In the Save Query window, enter:
    1. Name
    2. Category
    3. Visibility:
        - **Public** – Visible to everyone in the organization.
        - **Private** – Visible only to you.
    4. Monitor Query:
        - **Monitor** – Tenable captures a daily snapshot of query results starting from when you enable monitoring, enabling trend tracking and widgets on the query profile.

            > **Note:** To monitor a query, it must be Public and have no joins or group properties.

        - **Don't Monitor** (default)
3. Click **Save**. They can later be managed in the Queries page.

Query Widgets

Monitored queries display historical data as widgets on the query profile, viewable in **Explore** > **Queries**. Widgets are also available in the widget bank for use in custom dashboards.

Edit a Query

Update the name, category, or visibility of a custom query directly from the Explorer page.

To edit a query:

1. In **Explore** > **Explorer**, open the custom query you want to modify.
2. Click the three dots icon next to the query name at the top of the page, and then click **Edit**.

3. In the Edit Query window, you can update:
    - **Name**
    - **Category**
    - **Visibility** – Switch between **Private** (visible only to you) and **Public** (visible to the organization).
4. Click Save.

Create a Custom Policy from Query

Convert a query into a custom policy, to transform an ad-hoc search into automated security monitoring. For example, create a policy for tracking publicly exposed *EC2 instances* with *Sensitive* tags.

Query-based policies let you:

- Assign names, descriptions, and custom remediation steps (including external links) to provide clear guidance for security teams.
- Improve remediation workflows by defining your unique environment constraints and avoiding the need for manual report sharing to resolve issues.

> **Note:** Once saved, the policy triggers the next time Tenable syncs data in your environment, generating findings for all matching resources. Currently supports *single-resource* queries for *cloud resources* only. See Supported Objects for more information. You cannot create a custom policy for a joined query. To filter by a related entity, click **Filter** instead of *Join* when adding a relationship.

To create a custom policy from a query:

1. In the Console, navigate to **Explore** > **Explorer**.
2. (Optional) Select a scope in the Organization drop-down.
3. Select an existing query, or create a new one. See Supported Objects for more information.
4. Click **Add** > **Custom Policy**. The Add Custom Policy screen opens.
5. Enter a meaningful **Name** and **Description** (Optional).

6. Assign the policy a **Severity**, which determines the severity level of any findings triggered by the policy.
7. (Optional) Enter custom **Remediation** steps to provide clear guidance for security teams.
8. (Optional) Fine-tune your selected query, if needed, from the query editor.
9. Click **Save**.

Supported Objects

You can create custom policies from queries for:

- *Single-resource* queries
- Cloud resources

Queries using the `Join` operator or targeting non-cloud entities, such as risks and policies, are not supported. The following objects are currently not supported:

Category	Objects
Applications	Software Software Instance
Data	Data Object Data Type Database Table File
IAM	AWS Federated Permission
Network	Network Endpoint
Policies	Policy
Risks	Cloud Finding IaC Finding Vulnerability Instance

Create a Report from Query Data

Beyond manual exports, you can transform your investigation results into automated reports for continuous monitoring.

To create a report from query data:

1. In the Console, navigate to **Explore** > **Explorer**.
2. (Optional) Select a scope in the Organization drop-down.
3. Create your query, as relevant.
4. Use the **Column Picker** to select the data that's included in the export.
5. Click **Add** > **Report**. The Create Report screen opens.
6. Enter a meaningful **Name**.
7. **Delivery time**:
    - **Now** – Generate a one-time report.
    - **Schedule** – Define a cadence to generate a report at a specific time on either a daily, weekly or monthly basis.
8. **Add Delivery Method** to send a copy of the report to specific recipients. See Slack or Teams for more information.
    - Email address

      > **Note:** When sending reports via email, the file size limit is 14.5MB. Larger reports are compressed or provided via a download link.

    - Slack channels
    - Teams channels
9. Click **Create** or **Schedule**.

Create a Finding Automation from a Query

Convert any finding-based query into a permanent rule by creating an automation.

1. In the Console, navigate to **Explore** > **Explorer**.
2. (Optional) Select a scope in the Organization drop-down.
3. Create your query, as relevant.
4. Click **Add** > **Finding Automation**. The Create Finding Automation page opens.
5. *Configure automation settings* (Left pane):
    1. Enter a **Name** and **Description** (optional) that accurately describes the automation rule.
    2. *Status*: Select either **Enabled** or **Disabled**.
    3. *Type*: Define the type of findings this rule targets.
        - **Cloud Findings**
        - **IaC Findings**
    4. *Query*:
        - **Link to existing query** – The automation stays synced with the original query. Once linked, the query cannot be deleted, made private, or edited with unsupported syntax.
        - **Standalone query** – Create an independent copy or write from scratch.
    5. Select the **Target Scopes** for which you want to trigger the automation. Select an entire folder to trigger automations for all existing and future accounts within the folder.
    6. Choose whether to **apply to existing findings**. Enabling this applies the automation to all current findings in the system, in addition to any new findings detected moving forward.

        > **Note:** This option is only available when creating a new finding automation, or if the automation was previously disabled.

    7. **Delivery**: Click **Add Method** to configure where you want to send notifications to. You must first integrate with third-party tools for a specific delivery method to appear in the integrations list (except for Email address, which appears automatically).

        > Email address

Select **Static** to send to a fixed email list, or **Dynamic by Owner** to notify the resource owners. Sending to resource owners may include numerous recipients. For example, if the owner is a group with no associated email address, Tenable sends an email to all group members.

> Slack channels

Select **Static** to send to fixed channels, or **Dynamic by Owner** to notify the resource owners directly. This may include numerous recipients.

> Teams channels

Select **Static** to send to fixed channels, or **Dynamic by Owner** to notify the resource owners directly. This may include numerous recipients.

> Jira

Enable the integration, and then select a **Project**, **Issue Type**, **Assignee** (optional), **Labels**, **Epic** (optional), and **Environment** (URL of Jira instance). For labels, you can either choose from a list of labels already configured in the Jira instance, or manually add new labels, which will be sent to Jira. Label names can't contain spaces.

> ServiceNow

Enable the integration, and then select an **Instance** and **Assignee**.

Datadog organizations

QRadar servers

SQS queues

Splunk event collectors

Webhooks

6. Click **Create**.

Export Query Data

You can export the results of any custom query to a CSV file for offline analysis, reporting, or sharing. This feature allows you to capture a complete snapshot of your query data based on your current view. The export will include all data for the columns that are currently selected and displayed on the page, ensuring that the exported file is tailored to your specific view. There is no limit to the number of rows you can export.

To export query data:

1. In the Console, navigate to **Explore** > **Explorer**.
2. (Optional) Select a scope in the Organization drop-down.
3. Create your query, as relevant.
4. Use the **Column Picker** to select the data that's included in the export.
5. Click **Export** .

Display Query Results

Query results can be viewed in two formats: **Table** or **Graph**. Use the toggle in the top-right corner of the results area to switch between views.

Table View

The table view displays query results in a structured, column-based layout. The columns automatically adjust based on the objects in your query.

You can add or remove columns to control which data appears in the table.

To customize columns:

1. Run a query.
2. Click the Column Picker .

3. Choose the columns you want to display.
    - If you are using a `Join`, multiple objects appear in the column picker. Click to expand each one and then choose the columns.
    - (Optional) Click to **select all** columns for a given object.

If you export query results, the CSV includes only the columns currently selected.

Graph View

The graph view visualizes the objects returned by your query and the relationships between them. This makes it easier to understand how resources connect, depend on each other, or relate through findings, identities, or configurations.

> **Note:** Graphs only support queries that use `Join`. Joins produce a combined result set (for example, Identity + Finding pairs) that can be represented as a relationship graph.

You can interact with the graph to explore the data structure:

- **Drag nodes** to reposition them
- **Expand or collapse** relationship branches (when available).
- **Use the left-side controls** to zoom, reset, or enter fullscreen.

To change how the graph is arranged, use **Change layout** and select one of the available visualization styles:

- **Sequential** – Arranges nodes in a clear top-to-bottom or left-to-right flow. Good for hierarchical paths.
- **Organic** – Spreads nodes evenly to reduce overlap. Good for exploring general relationships.
- **Lens** – Pushes highly connected nodes to the center and less connected ones outward. Highlights hubs in a network.
- **Structural** – Groups nodes with similar connections. Useful for spotting clusters or patterns.

Each layout provides a different way to organize nodes, making it easier to focus on the relationships that matter.

Sample Queries

The following sample queries provide a starting point for leveraging the full power of Unified Explorer. Use these examples to understand how to combine properties and operators to solve common security challenges and build your own custom queries.

Query for Findings That Violate Compliance Standards

Identify findings that violate a specific compliance standard. For example, query for all open cloud findings with critical severity that violate the SOC2 Type II standard.

Build the query:

1. Start by selecting **Cloud Finding** to query across all cloud findings in your environment.
2. Click the three dots to **Add group**.
3. In the new group, add a filter for **Severity** and choose **Critical**.
4. Add a filter for **Status** and choose **Open**.
5. Add a relationship filter to find only those findings that are **related to** a **Cloud Resource**.
6. Click **JOIN** and select **violates Compliance**.
7. In the JOIN, add a filter for **System ID** and choose the relevant standard/s.

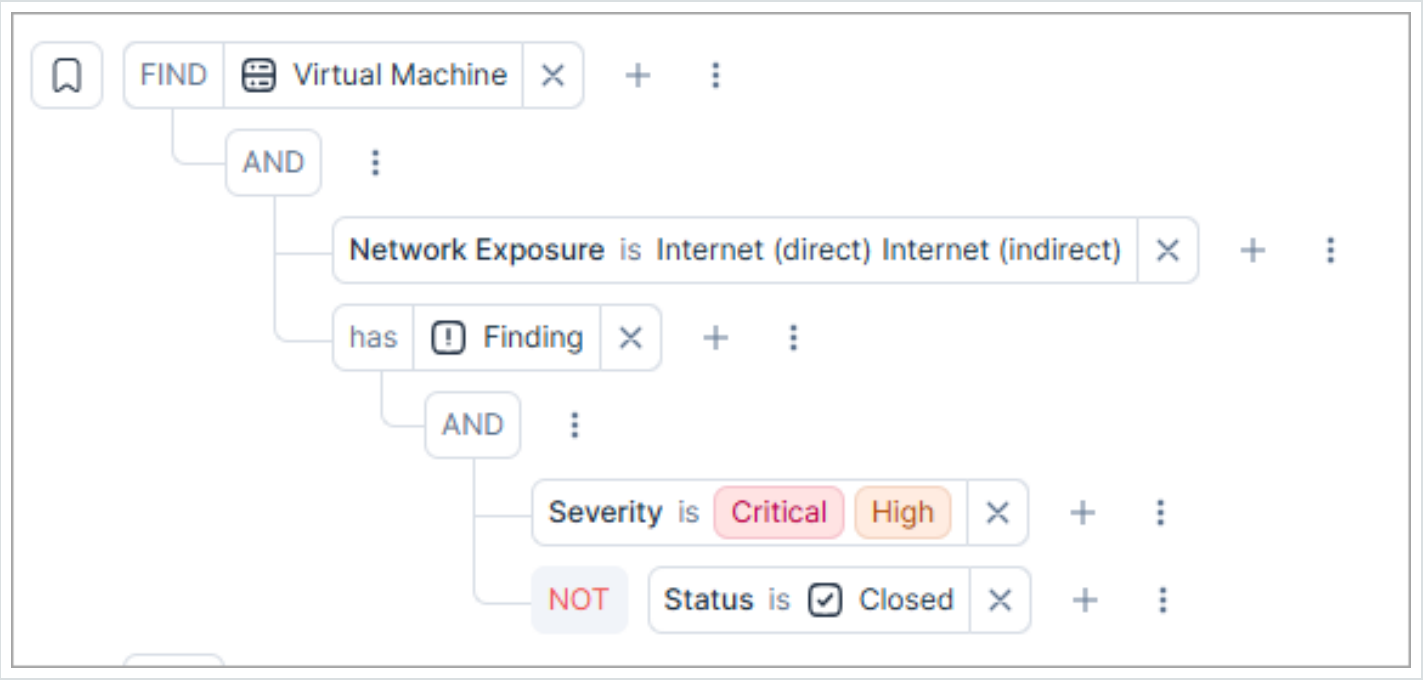
Query for Public-Facing Virtual Machines

You can use this query to find virtual machines with public-facing risks that require immediate attention.

Build the query:

1. Start by selecting **Virtual Machine** to query across all virtual machines in your environment.
2. Add a filter for **Network Exposure** to include **Internet (direct)** and **Internet (indirect)**.
3. Add a relationship filter to find only those VMs that have an associated **Finding**.
4. Click **Add group** and use the And operator to apply a set of conditions specifically to the finding itself. In this nested group, filter by:

- **Severity** to include **Critical** and **High** findings.
- **Status** and select **Closed** findings, and apply the `Not` operator to exclude them.



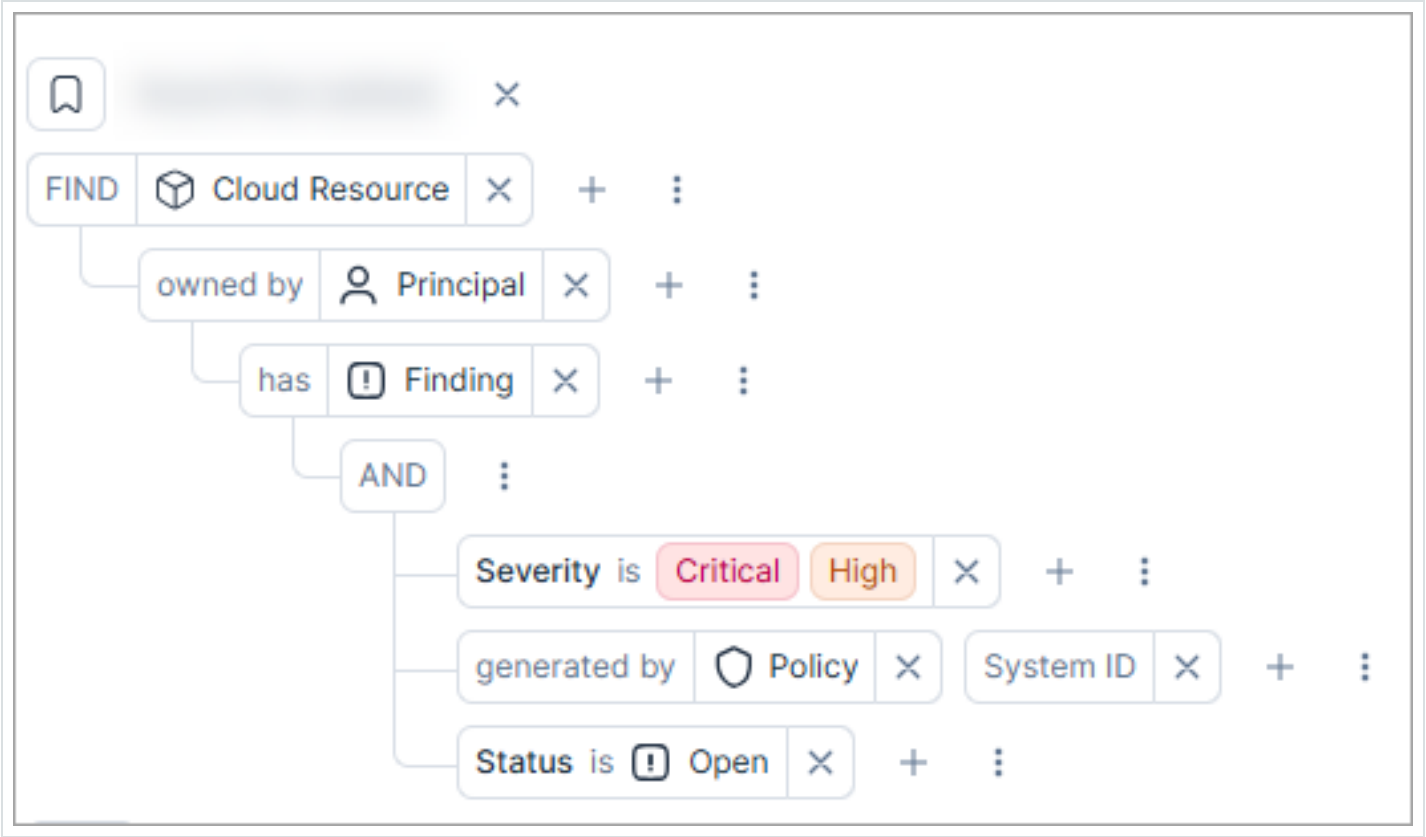
Query for Resources with Inactive Owners

Find cloud resources with open, high/critical severity findings that are owned by a user linked to an inactivity policy.

Build the query:

1. Start by selecting **Cloud Resource** to query across all cloud resource types in your environment. See Generic vs Platform-Specific Objects to learn more.
2. Add a relationship filter to find resources that are owned by a **Principal**. A principal in this context represents the Resource Owner.
3. Add a second relationship filter to find resources that have an associated finding.
4. Click **Add group** and use the `And` operator to apply a set of conditions specifically to the finding itself. In this nested group, filter by:

- **Severity** to include **Critical** and **High** findings.
- Findings that are generated by an inactivity-related **Policy**. To narrow the list of policies, you can use the **System ID** (or **Search Policy**) property to select specific policies.
- **Status** to include only **Open** findings.



Reference: Finding Properties

You can filter findings by the following properties:

Property	Description
Ignore Expiration Date	When a finding is manually ignored, you can set a duration for how long it will be ignored. This duration can be permanent or "Until" a specified date (e.g., 1, 7, 30, or 90 days, or a custom date). If an ignored finding reaches its expiration date, its status transitions back to *Open*

Property	Description
Open Time	This property indicates when a finding was last opened. It provides clear visibility into when findings were, for example, reopened or unignored.
Severity	The risk level assigned to a finding, indicating the immediacy of action required. Possible values: Critical, High, Medium, Low, Informational
Starred	You can star important or significant findings to mark them for later review.
Status	The primary status of a finding, which helps you understand its overall state and progress. Possible values: Open, Ignored, Closed.
Status Update Time	The last time the finding status was updated.
Sub-Status	Provides added granularity to a finding's main status, describing the specific reason for that status. See Finding Status for more information.
System ID	The unique ID of the finding in AI Exposure.

FAQ

> What are "objects" in the Explorer page, and what is the difference between "Generic" and "Platform-Specific" objects?

Every query in the Explorer page starts with an object, which represents a resource type (like a virtual machine) or a policy that you want to explore. To learn more about different object types, see Generic vs Platform-Specific Objects.

> Can I temporarily disable parts of my query without deleting them?

Yes, you can hide a query group.

> What are "relationship filters" and "joins," and how do they differ in the query results?

These are two powerful ways to query relationships between objects. See Add Relationships to learn more.

> Can I track how query results change over time?

Yes. When you Save a Query, you can enable monitoring to capture daily snapshots of results. Monitored queries display historical trend data as widgets on the query profile.

Queries

The Queries page gives you a centralized view of all saved queries available to you. Use it to browse, manage, and monitor queries, and view query-based widgets on individual query profiles. Selecting a query opens the query profile, where you can review its details and widgets.

Queries Table

Each row in the Queries table represents a saved query and includes:

Column	Description
Name	The name of the saved query.
Category	The category selected when the query was saved (for example, *Compute*, *Containers*, or *Data*).
Scope	The main scope of the query, such as a specific cloud provider or environment.
Visibility	Whether the query is **Public** (visible to everyone in the organization) or **Private** (visible only to the creator).
Monitored	Whether Tenable is capturing daily snapshots of query results. Monitored

Column	Description
	queries display widgets on the query profile.
Modified By	The last user who updated the query. Built-in queries always display **Tenable**.
Modification Time	The most recent time the query was updated.
Favorite	A star icon you can toggle to mark frequently used queries.

You can mark a query as a favorite using the star icon and filter by **Favorite** to find it quickly.

Open a Query in Explorer

You can open any saved query in **Explorer** to run it or adjust its configuration.

To open a query:

1. Go to **Explore** > **Queries**.
2. Find the query you want to run.
3. Select the row, or open the three-dot menu and choose **Go to Explorer**.

The Explorer page loads with the selected query applied. From there, you can modify filters, relationships, and other settings, and then use **Save** or **Save As** as needed. To learn more, see Save a Query.

Monitor a Query

Monitoring a query tells Tenable to capture a daily snapshot of results starting from when you enable monitoring. This historical data is displayed as widgets on the query profile and is available in the widget bank for use in custom dashboards.

You can enable monitoring when saving a query in the Explorer.

Query Widgets

Each query profile includes a **Widgets** tab showing the widgets available for that query. Widgets reflect historical data captured through monitoring and vary by query type.

Query Type	Widgets
All queries	Item Count, Table
Cloud/IaC Findings (monitored)	Findings by Severity, Findings Trend, Findings MTTR, Findings Activity, Trend
Cloud resources (monitored)	Trend

Widgets are also available in the widget bank for use in custom dashboards.

Duplicate a Query

Duplicate a query to use a built-in or existing custom query as a template for a new one.

To duplicate a query:

1. Go to **Explore** > **Queries**.
2. Find the query you want to duplicate.
3. Select the row, or open the three-dot menu and choose **Duplicate**.
4. In the Query dialog, adjust the following values, as needed:
    1. **Name**
    2. **Category**
    3. **Visibility**:
        - **Public** – Visible to everyone in the organization.
        - **Private** – Visible only to you.

5. Click **Add**.

Delete Custom Queries

You can delete custom queries from the Queries page to keep your workspace organized. Built-in queries are system-provided and cannot be deleted or modified.

> **Caution:** Deleting a query is permanent.
>
> - If a query is marked Public, deleting it will remove it for everyone in your organization.
> - If the query is monitored, deleting it also permanently deletes all saved historical data.

To delete queries:

1. Go to **Explore** > **Queries**.
2. Select the checkbox next to one or multiple queries you want to remove.
3. Click **Delete**.

AI Conversations

The **Conversations** page provides a centralized view of all AI conversations that Tenable One AI Exposure captures across your organization. Use this page to browse, filter, and investigate interactions with AI tools.

> **Required Tenable One AI Exposure User Role:** To view AI conversations, you must have the **AI Conversations Viewer** role.

1. To add this role, go to **Settings** > **Access Management** > **Users and Groups**.
2. Click **Add Role Assignment**. The **Add Role Assignment** dialog box appears.
3. Select a user or group to assign the role.
4. From the **Roles** drop-down menu, select **AI Conversations Viewer**.
5. Click **Save**.

Conversations Column Data

Column	Description
AI Conversation	The conversation name and an icon indicating the AI tool used. For example, Claude or ChatGPT.
Name	The conversation name.
Identity	The identity associated with the conversation.
Start Time	The date and time when the conversation begins.
Origin	The AI tool where the conversation originates.
System ID	The unique ID of the conversation in AI Exposure.

View Conversation Details

To view conversation details:

1. In the AI Exposure Console, click **Explore** > **Conversations**.
2. Filter the table to narrow the scope of the visible data.
3. Use the column picker on the top right of the table to choose which columns to display. See Conversations Column Data for more information.
4. Click an AI conversation to open a slideout panel that displays the conversation name, AI tool, associated identity, and start time.
5. Click either of the following tabs to view more information:
    - **Overview** – Displays the full conversation transcript, including messages and AI responses. Each message includes a timestamp. Use the **Search** icon in the upper-right corner of the transcript to find specific text within the conversation.
    - **Detections** – Lists any activity rule violations that AI Exposure identifies within the conversation. The detections table includes the following columns:

- **Content Type** – The category of sensitive content detected. For example, Business Email or URL.
- **Conversation** – The conversation in which the detection occurred, linked for quick navigation.
- **Severity** – The risk level of the detection. For example, Informational, Low, Medium, High, or Critical.
- **AI Activity Detection** – The specific detection rule that fired. For example, "AI conversation PII data exposure" or "AI conversation access data exposure".

Software

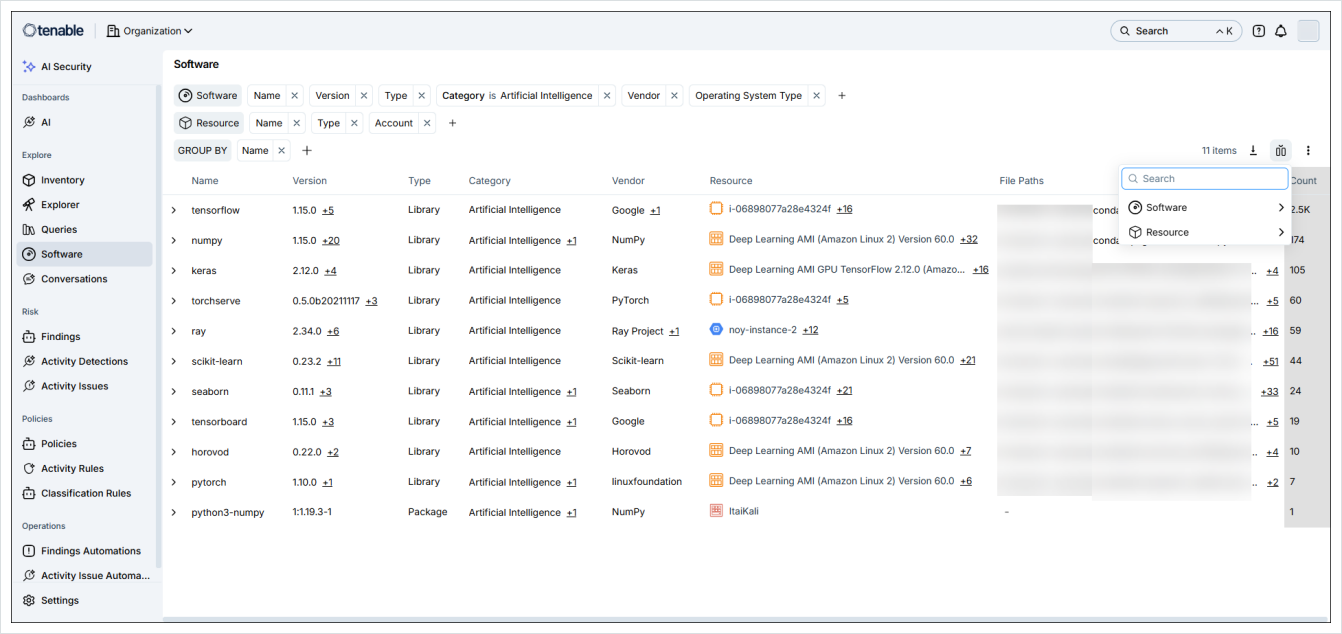
View AI-Related Software Packages

View AI-related software packages installed in cloud workloads across your environment. For each software package, you can view details such as the package name, version, type (library or package), category, vendor, the resource on which it is installed, file paths, and the total number of detected instances.

To view software packages:

1. In the Tenable One AI ExposureConsole, navigate to **Explore** > **Software**.
2. Filter the table to narrow the scope of the visible data. See Software Packages Column Data

for more information.



Software Packages Column Data

Software Columns

Column	Description
Name	The name of the software package or library. (For example, tensorflow, numpy)
Version	The version number of the software. (For example, 1.15.0, 2.12.0)
Type	The package type. (For example, Library, Package)
Category	The software category: Artificial Intelligence.
Vendor	The vendor or publisher of the software. (For example, Google, NumPy, Keras).
File Paths	The file system path(s) where the software is installed on the resource.

Column	Description
Language	The programming language associated with the software.
Operating System Type	The operating system type the software runs on.
Package Manager	The package manager used to install the software. (For example, pip, conda, apt)
Source Package	The source package from which the software was built.
Count	The total number of instances of the software in the environment.

Resources Columns

Column	Description
Resource	The compute resource (EC2 instance, AMI, VM, etc.) where the software is installed.
Account	The cloud account associated with the resource.
Creation Time	The timestamp when the resource was created.
ID	The unique identifier of the resource.
Labels	Labels associated with the resource.
Location	The geographic location or zone of the resource.
Name	The name of the resource.
Region	The cloud region where the resource is located.

Column	Description
Tags	Tags applied to the resource.
Type	The type of resource (For example, EC2 instance, AMI, GCP VM)

Risks

AI Posture Findings

Use the **Findings** page to efficiently triage findings across your AI services. You can discover and remediate critical findings in your production environment. Tenable One AI Exposure detects findings based on your configured policies.
Findings are posture-related, while activity detections and activity issues are activity-related.

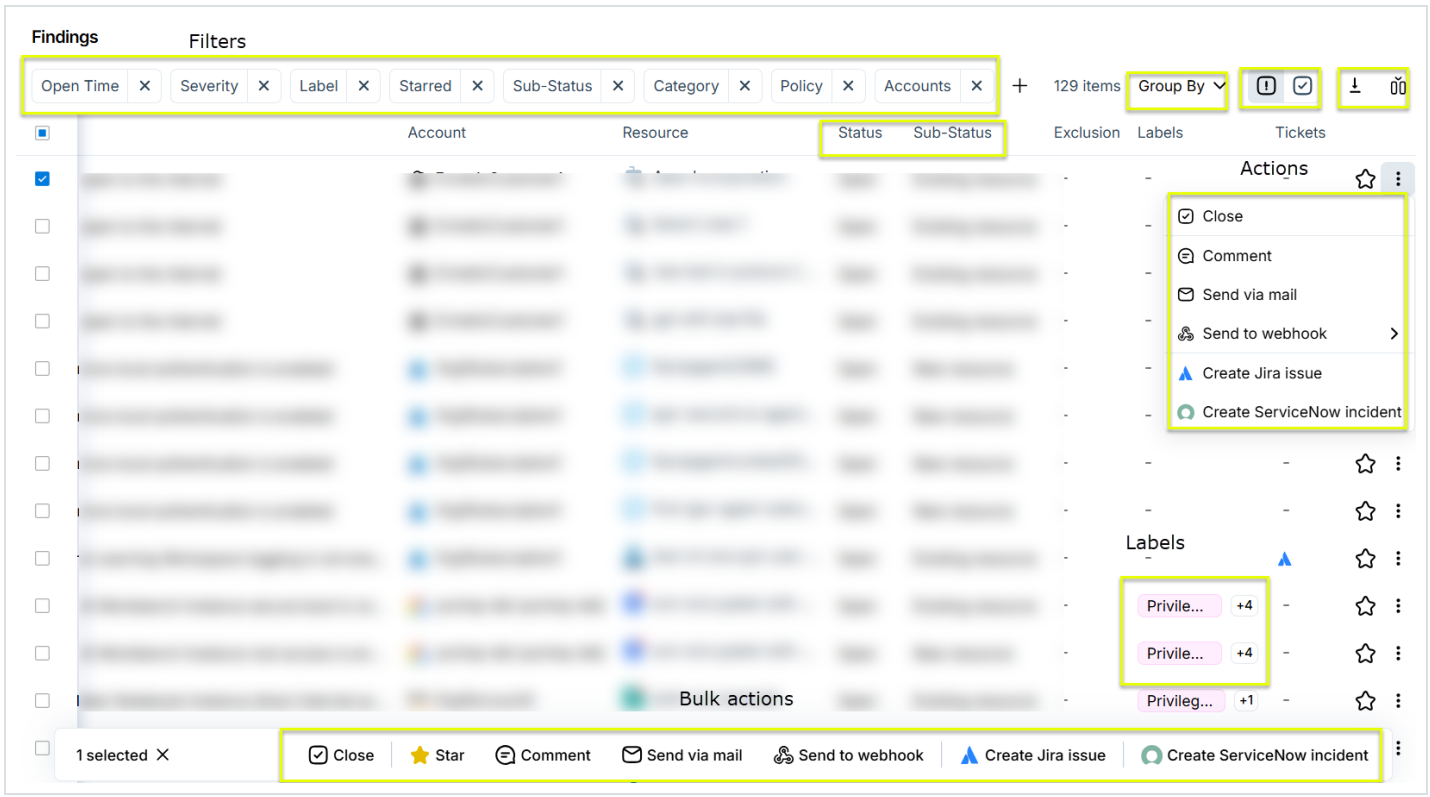
Navigate the Findings Page

View findings from the Findings pages, grouped according to their current status:

- **Open** – Displays all *active* findings in your environment.
- **Closed** – Displays the findings that were closed, either manually or automatically by AI Exposure.

> **Note:** Open/Ignored findings are listed in order of the severity of the potential threat to your cloud environment. Even though multiple findings can have the same severity level (for example, *High*), those listed higher in the table pose a higher risk based on the evaluation by Tenable.

The navigational elements on the **Findings** page allow you to narrow down and organize the results to find specific data.



Item	Description
View by Status	View **Open** or **Closed** findings.
Severity	The color-coded risk severity of the finding, used to filter findings in the default view when you do not apply the **Group by** option.
Status / Sub-Status column/filter	The current lifecycle state of the finding. For more information, see Finding Lifecycle.
Select all	Select all findings based on applied filters to perform bulk actions. For example, if you want to ignore or manually close a certain group of findings. This selection is limited to 10,000 findings.
Filters	Use the filters to narrow the visible data. Available filters include:

Item	Description
	• Creation Time • Open Time • Accounts • Category • Severity • Policy • Resource • Sub-Status • Compliances • Label • Ticket • Starred
Group by	Group findings by one of the following criteria: • **Account** – Groups all findings by the connected cloud account. • **Policy** (default): Groups all findings by the policy that triggered them. • **Ungroup** – Displays all individual findings in a flat list. For both filtering methods, grouped findings are listed in order of the percentage of severe findings they contain. For example, a group of findings where 75% percent have critical severity is listed before a group where 100% have high severity.
Labels	Labels applied to a resource associated with a finding automatically propagate to the finding.
Star	Star important or significant findings to mark them for later review.

Item	Description
Actions	Perform actions on a finding, such as: • **Close** • **Send via email** – Send information about the finding to one or more email addresses. • **Create/update a Jira issue** or **Create/update a ServiceNow incident**. Available if you have Ticketing Integrations installed. /li>
Bulk actions	Apply an action to multiple findings simultaneously.
Export	Export data to a CSV for analysis or processing by an external tool.
Column picker	Choose which columns to display in the Findings table.

Export Finding Data

Export finding data to create a summary report of findings in your environment. The data exports according to the current filters applied to the table.

The output data is in CSV format and includes all relevant findings along with remediation steps.

For example, you can perform the following tasks:

- Create a report of all closed findings containing sub-status information about the reason for closure (for example, *Resource Deleted*) to share with relevant stakeholders in your company.
- Create reports for open/starred findings, or any other subset of findings (using filters).

> **Note:** You can also export data for specific finding types (policies) that contain additional, non-standard information. When the page is grouped by *Policy*, an **Export** button is available for relevant types. For example, you can export all finding data for the *Azure AI Service is exposed to the internet* policy because that type includes additional parameters that are not extracted when exporting the entire **Findings** page.

To export findings data:

1. In the AI Exposure Console, navigate to the relevant **Risk** > **Findings** page and select **Open** or **Closed**.
2. (Optional) Apply filters to narrow down the list of findings.
3. To export data for specific finding types that contain additional, non-standard information:
    1. Click **Group by** > **Policy**.
    2. Click a relevant type to expand the section. For example, *Bot Service is exposed to the internet*.
    3. In the upper-right corner, click the **Export** button.
4. Click **Export** to create and download the CSV.

Manually Close a Finding

When you remediate a finding and solve the underlying security issue, AI Exposure automatically marks the finding as **Closed (Fixed)**. In some cases, however, you may want to **manually close** an open finding.

Consider the following examples:

- Since the automatic identification and marking of a finding as resolved can take time, you can resolve the finding manually to remove it from the **Findings** page sooner.
- Some finding types are never automatically marked as resolved by AI Exposure. This applies to findings that serve primarily as alerts, such as anomaly findings. Due to the unique nature of anomaly findings, you can remediate them traditionally like most other findings. Instead, you can manually mark them as resolved after investigating whether they represent a real threat to your environment.

When you manually close a finding, the finding is marked as **Closed (Manually closed)**. If you close a finding manually, but the issue is not fixed, the finding status reverts to **Open (Reopened)** during the next system synchronization.

To mark and see closed findings:

1. From the Findings table:
    1. *Single finding*: Click the three dots icon next to an individual finding and then click **Close**.
    2. *Multiple findings*: Select multiple findings and then click **Close** at the bottom.
2. In the **Close Finding** dialog, add a comment to indicate the reason for closing, which is added to the finding activity.
3. Click **Close**.
   To see all closed findings, navigate to **Findings > Closed**.

Reopen a Finding

You can reopen a finding that was manually closed. If you do so, the finding status changes to **Open (Reopened)**

To reopen a finding:

1. From the Findings table, use one of the following methods:
    1. *Single finding*: Click on the three dots icon next to an individual finding, and then click **Open**.
    2. *Multiple findings*: Select multiple findings and then click **Open** at the bottom.
2. In the **Open Finding** dialog, add a comment to indicate the reason for reopening, which is added to the finding activity.
3. Click **Open**.
   To see all reopened findings, navigate to **Findings** > **Open**, and then filter the Sub-Status by **Reopened**.

Trigger Actions Based on Findings

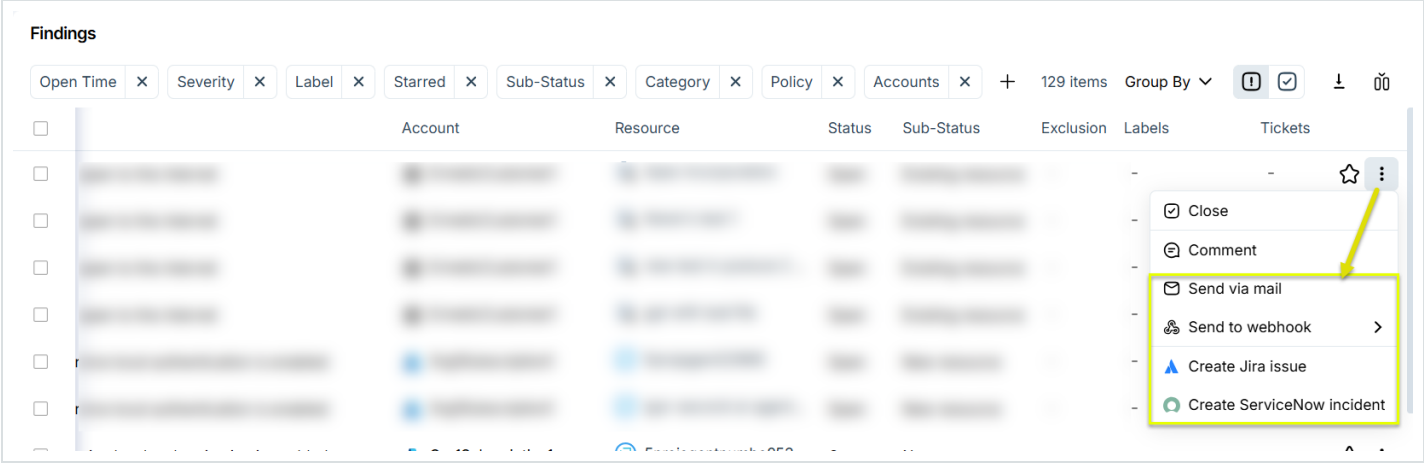
You can manually trigger actions associated with ticketing Integrations and/or send email notifications for individual findings.

> **Required AI Exposure User Role:** You must have either the **Collaborator** or **Administrator** role in AI Exposure to perform this action.

Trigger an Action for a Single Finding

To manually trigger an action for a single finding:

1. In the AI Exposure Console, navigate to the **Risk** > **Findings** page.
2. Click the three dots menu icon next to the finding and select the relevant action:



(Click the ▶ icon below for instructions, per action)

Send via email

1. Enter one or more email addresses. You can also choose to send finding information to any owners of the associated resources. This may include numerous recipients. For example, if the owner is a group with no associated email address, Tenable sends an email to all group members.
2. (Optional) Enter a message to the recipient/s.
3. Click **Send**.

Create a Jira issue

1. Select a **Project**, **Issue Type**, **Assignee** (optional), **Labels**, **Epic** (optional), and **Environment** (URL of Jira instance). The Project you select determines which values are available in the other field dropdowns. For labels, you can either choose from the existing list of labels in the

Jira instance or manually add new labels. Label names cannot contain spaces.

2. (Optional) Edit the predefined content in the **Summary** and/or **Description** fields.
3. (Optional) Click **Add Optional Field** to include non-mandatory data like labels, assignees, or epics.
4. (Optional) Add **attachments** to include a copy of any revised policy suggestions (according to the remediation steps).
5. Click **Create Issue**.

> *Create a ServiceNow Incident*

1. Select an **Instance** and an **Assignee**.
2. Select an **Impact** and **Urgency** for the incident.
3. (Optional) Edit the predefined content in the **Summary** and/or **Description** fields.
4. (Optional) Add **attachments** to include a copy of any revised policy suggestions (according to the remediation steps).
5. Click **Create Incident**.

> *Send to Webhook*

1. If you have more than one webhook configured, select the webhook that you want to send the finding to.
2. Click **Yes** to confirm.

Trigger an Action for Multiple Findings

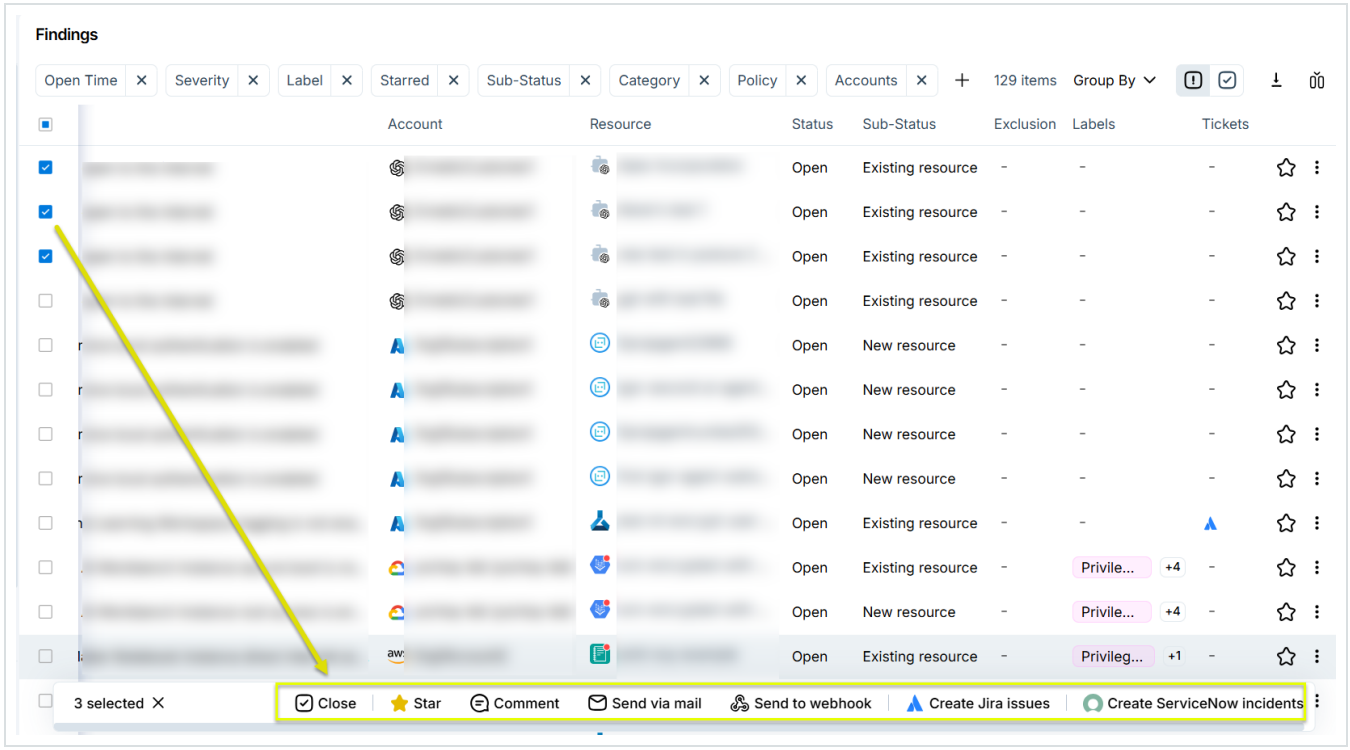
Manually trigger an action for multiple findings. For Jira/ServiceNow, you can choose one of the following options:

- Create a single, unified ticket that includes all selected findings
- Create separate tickets, one per selected finding

Note: When you trigger multiple Jira issues or ServiceNow incidents at once, you cannot edit the summary or description fields. Each issue or incident contains the default summary or description provided by AI Exposure.

To manually trigger an action for multiple findings:

1. In the AI Exposure Console, navigate to the **Risk** > **Findings** page.
2. Select the checkboxes next to the findings for which you want to trigger an action.



3. From the bottom menu panel that appears, select the relevant action:
   - **Send to webhook**
     1. If you have more than one webhook configured, select the target webhook.
     2. Click **Yes** to confirm.
   - **Send via email**
     1. Enter one or more email addresses. You can also choose to send finding information to any owners of the associated resources. This may include numerous recipients. For example, if the owner is a group with no associated email address, Tenable sends an email to all group members.

2. (Optional) Enter a message to the recipient/s.
3. Click **Send**.

- **Create Jira issues**
  1. Choose whether to:
     - **Create a unified Jira issue which includes all findings**
     - **Create separate Jira issues, one per finding**
  2. Select a **Project**, **Issue Type**, **Assignee**, **Epic** (optional), **Environment** (URL of Jira instance), and **Labels**. The Project you select determines which values are available in the other field dropdowns.
  3. (Optional) Click **Add Optional Field** to include non-mandatory data like labels, assignees, or epics.
  4. Click **Create Issue/s**.
- **Create ServiceNow incidents**
  1. Choose whether to:
     - **Create a unified ServiceNow issue which includes all findings**
     - **Create separate ServiceNow issues, one per finding**
  2. Select an **Instance**, **Assignment group**, an **Assignee**, **Category**, **On hold reason**, **Service**, **Severity**, and **Super user**.
  3. Select an **Impact** and **Urgency** for the incident.
  4. Click **Create Incidents**.

Track Jira and ServiceNow Tickets

When you connect your ticketing integrations (Jira, ServiceNow) and create automation rules to streamline remediation workflows, external tickets are created in those systems. You can track these external tickets directly from the **Findings** page.

To track external tickets:

1. In AI Exposure, click on **Risk** > **Findings**.
2. Navigate to the **Open** or **Closed** Findings page.
3. In the **Ticket** filter, select **Jira issue** and/or **ServiceNow incident** to filter the table by findings that have tickets.
4. (Optional) Apply other filters to narrow your search.
5. Hover over the **Jira** or **ServiceNow** icon next to the relevant finding to see ticket details.

View Finding Details

Click a finding to view granular information and to remediate risks associated with it. You can view a detailed historical account of the event, an expanded rationale for the potential risk it imposes, and specific remediation instructions.

Each finding displays distinct information depending on the finding type and the specific circumstances that triggered its creation.

Review finding details to understand the following items:

- What the root cause of the finding is.
- The scope of the finding.
- The potential risk the finding imposes on your environment.
- An explanation of the severity of the finding.

> **Note:** Custom policy violations are limited to the first 10,000 results.

View Finding Activity

View the finding activity to see information about the lifecycle of the finding within AI Exposure, such as when:

- The finding was created.
- The status changed (either by the system or manually).

- Tickets were created for third-party integrations.

  Activity

  To view finding activity:

1. From the Findings table, click a relevant finding.
2. Click **Activity**.
3. (Optional) Write a comment, and then click **Save**.

Remediate Findings

AI Exposure allows you to perform manual remediation.

Manually Remediate Findings

For some findings, you may choose to remediate issues outside of AI Exposure.

To manually remediate a finding:

1. On the **Findings** page, click to open the relevant finding.
2. Navigate to the **Remediation** area.
3. Follow the **Remediation steps** sequentially.
4. Manually close the finding after you remediate it to remove it from the **Open Findings** page.

Remediate with One-Time Credentials

As an alternative to granting AI Exposure management permissions during account connection, you can instead provide temporary, one-time credentials that allow Tenable to automatically remediate findings.

- For AWS IAM configurations: Temporary credentials require an access key for IAM users, or an access key together with a session token for IAM roles. The IAM user or role must have sufficient permissions (often Administrative permissions) to perform remediation actions within that specific account.

- For GCP configurations: Temporary credentials require an access token that you can generate via the Google Cloud CLI.

By default, the credentials you provide apply to the remediation of the specific finding for which you entered them. To extend the credentials for the duration of your current browser session, you can choose to store them locally.

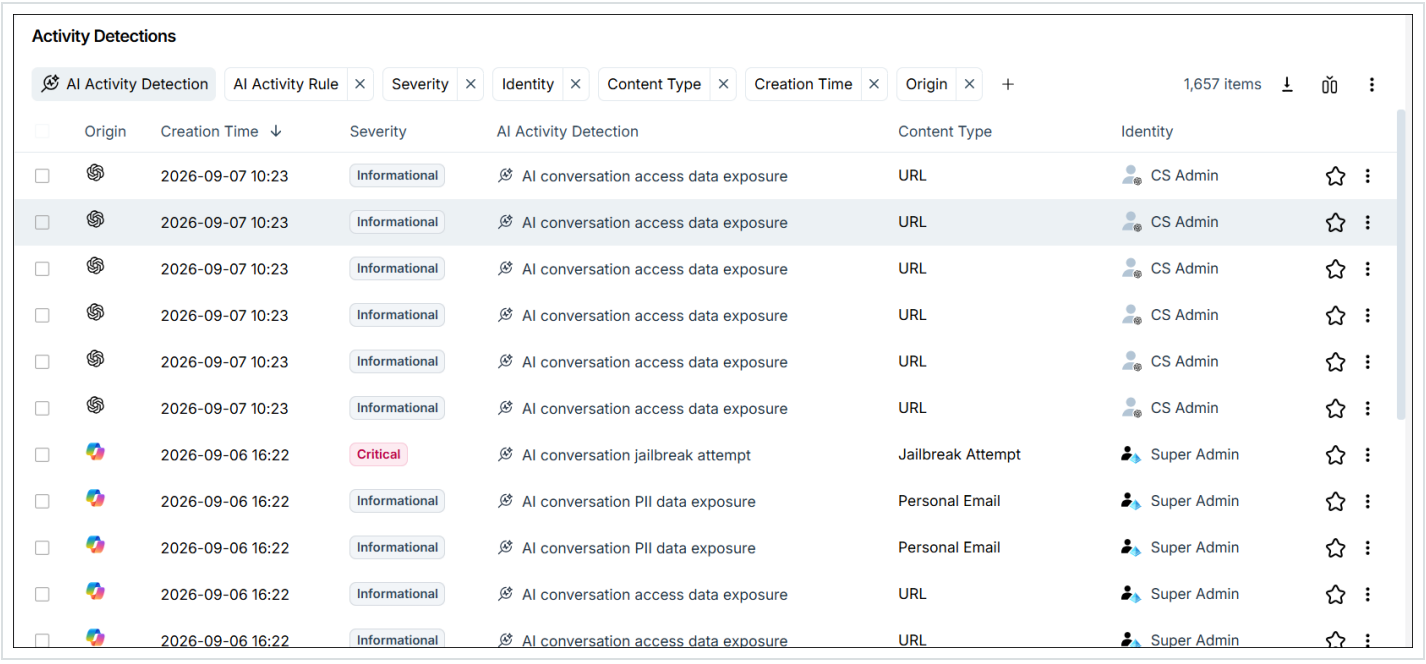
> **Note:** Unless you explicitly select to store them for the session, the credentials are not saved e, and can be safely removed or revoked after the remediation is complete.

AI Activity Detections

Use the **Activity Detections** page to view all the AI activity events detected across your organization's AI services.

Each detection represents a single recorded message or response that triggered an activity rule, the identities involved, and the detection method.

You can use this page to investigate specific AI activity events, filter by content type, and drill into individual detections for more detail.



Required Tenable One AI Exposure User Role: To view AI conversations, you must have the **AI Conversations Viewer** role.

1. To add this role, go to **Settings** > **Access Management** > **Users and Groups**.
2. Click **Add Role Assignment**. The **Add Role Assignment** dialog box appears.
3. Select a user or group to assign the role.
4. From the **Roles** drop-down menu, select **AI Conversations Viewer**.
5. Click **Save**.

Navigate the Activity Detections Page

The **Activity Detections** page includes the following elements:

Item	Description
AI Activity Detection	The specific AI activity rule name. Click the activity rule name to open the details panel.
Severity	The color-coded risk severity of the activity.
Filters	Filter the detections by properties and content type. Select from the following properties: • Identity • AI Conversation • AI Activity Rule • AI Activity Issue • Content Type • Severity • Starred • System ID

Item	Description
	• Conversation
Star	Star important or significant findings to mark them for later review.
Actions	Perform actions on an activity detection, such as: • **Comment** • **Send via email** – Send information about the AI activity detection to one or more email addresses. • **Create Jira issue** or **Create ServiceNow incident**. Available if you have Ticketing Integrations installed. For more information, see Trigger Actions Based on Findings.
Bulk actions	Apply an action to multiple findings simultaneously.
Export	Export data to a CSV for analysis or processing by an external tool.
Column picker	Choose which columns to display in the detections table.

Export Finding Data

Export finding data to create a summary report of AI activities in your environment. The data exports based on the current filters applied to the table.
The output is in CSV format and includes all relevant information, including remediation steps.

For example, you can perform the following tasks:

- Create a report of all closed findings containing sub-status information about the reason for closure (for example, *Resource Deleted*), to share with relevant stakeholders in your company.
- Create reports for open or starred findings, or any other subset of findings using filters.

To export AI activities:

1. In the Tenable One AI Exposure Console, navigate to the relevant **Risk** > **Activity Detections** page.
2. (Optional) Apply filters to narrow down the list of activities.
3. Click **Export** and download the CSV summary report.

Comment on an AI Activity

Add comments to an AI activity to provide additional context or flag important observations.

To add a comment to one or several AI activities:

1. In the AI Exposure Console, navigate to the **Risk** > **Activity Detections** page.
2. From the **Activity Detections** table, use one of the following methods:
   - *Single activity*: Click the three-dot icon next to it and select **Comment**.
   - *Multiple activities*: Select the relevant findings and click **Comment** at the bottom.
3. Enter your comment.
4. Click **Save**.

   The comments appear in the **Activity** tab within the Activity Details panel. You can edit or delete the comment directly from the **Activity** tab.

Trigger Actions Based on Detections

You can manually trigger actions associated with ticketing Integrations and/or send email notifications for individual activities.

> **Required AI Exposure User Role:** You must have either the **Collaborator** or **Administrator** role in AI Exposure to perform this action.

Trigger an Action for a Single Activity

To manually trigger an action for a single activity:

1. In the AI Exposure Console, navigate to the **Risk** > **Activity Detections** page.
2. Click the three dots menu icon next to the activity and select the relevant action.
   (Click the ▶ icon below for instructions, per action)

   Send via email

   1. Enter one or more email addresses. You can also choose to send the information to any owners of the associated resources. This may include numerous recipients. For example, if the owner is a group with no associated email address, Tenable sends an email to all group members.
   2. (Optional) Enter a message to the recipient/s.
   3. Click **Send**.

   Create a Jira issue

   1. Select a **Project**, **Issue Type**, **Assignee** (optional), **Labels**, **Epic** (optional), and **Environment** (URL of Jira instance). The Project you select determines which values are available in the other field dropdowns. For labels, you can either choose from a list of labels already configured in the Jira instance, or manually add new labels, which will be sent to Jira. Label names can't contain spaces.
   2. (Optional) Edit the predefined content in the **Summary** and/or **Description** fields.
   3. (Optional) Click **Add Optional Field** to include non-mandatory data like labels, assignees, or epics.
   4. (Optional) Add **attachments** to include a copy of any revised policy suggestions (according to the remediation steps) in JSON, Terraform, or CloudFormation format.
   5. Click **Create Issue**.

   Create a ServiceNow Incident

   1. Select an **Instance** and an **Assignee**.
   2. Select an **Impact** and **Urgency** for the incident.

3. (Optional) Edit the predefined content in the **Summary** and/or **Description** fields.
4. (Optional) Add **attachments** to include a copy of any revised policy suggestions (according to the remediation steps) in JSON, Terraform, or CloudFormation format.
5. Click **Create Incident**.

Send to Webhook

1. If you have more than one webhook configured, select the webhook that you want to send the finding to.
2. Click **Yes** to confirm.

View Activity Detection Details

Click an activity to view granular information and remediate the risk associated with it. From the details view, you can:

- View the evidence that led to being flagged as a potentially harmful event.
- Click the **View Conversation** link to view the complete conversation history with the AI platform.

Required AI Exposure User Role: You do not need the **AI Conversation Viewer** role to view evidence snippets. However, you must have the **AI Conversation Viewer** role to view the complete conversation history.

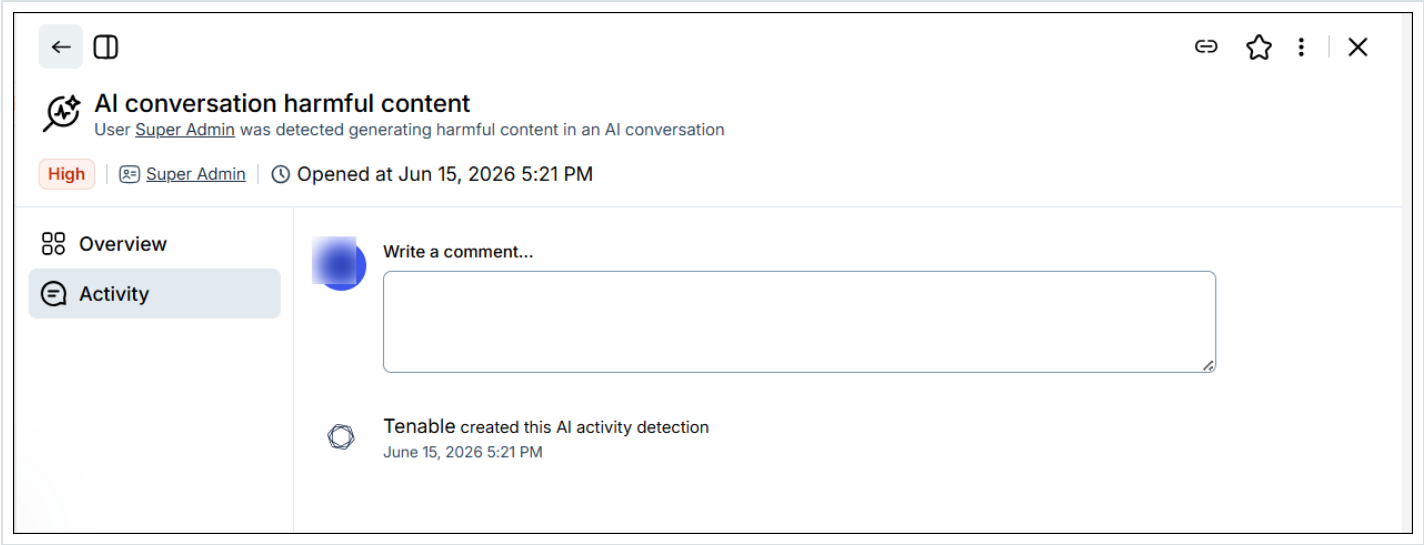
- View an expanded rationale for the potential risk the activity imposes.

View Activity

View the AI activity to see information about the lifecycle of the conversation within AI Exposure.

For example, you can see when:

- The conversation was created
- The status changed (either by the system or manually)
- Tickets were created for third-party integrations



To view activity details:

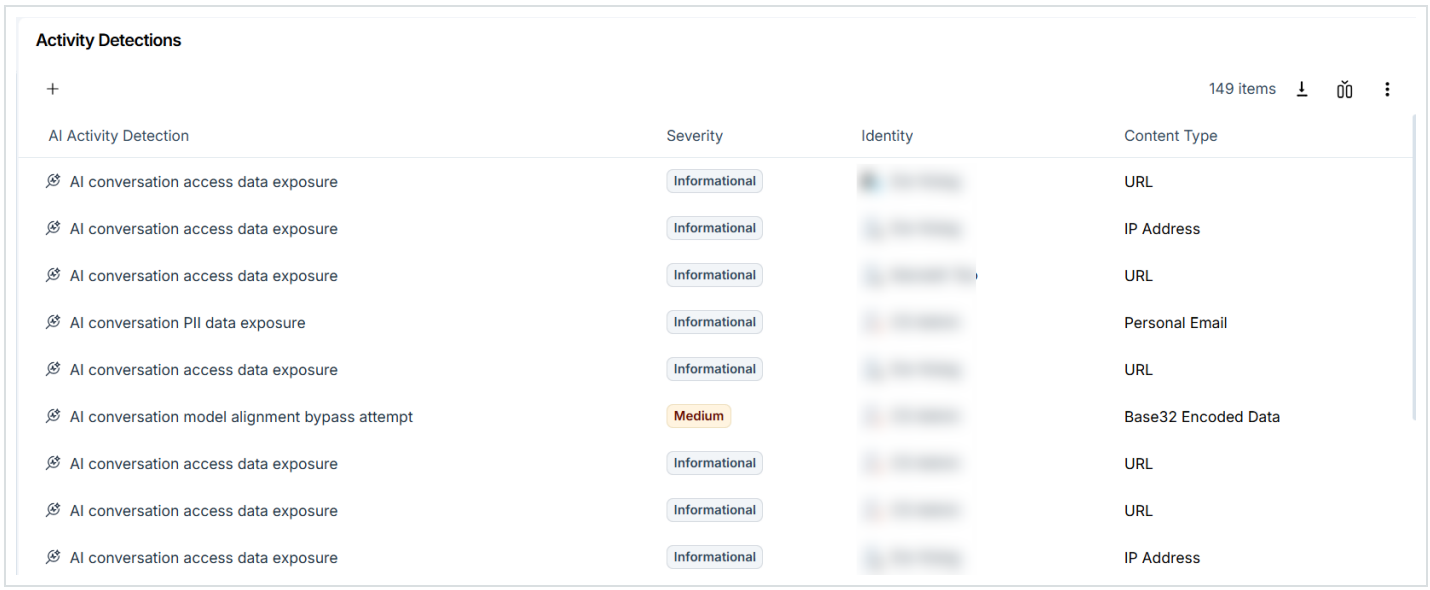
1. From the Activity Detections table, click a relevant AI activity.
2. Click **Activity**.
3. (Optional) Write a comment and then click **Save**.

AI Activity Issues

Use the **Activity Issues** page to view all the issues that Tenable One AI Exposure creates from your AI detections. This page displays all the critical and high-severity issues.

Activity Issues combine multiple related activity detections into one actionable risk.

When you repeatedly trigger the same activity rule, AI Exposure groups the resulting detections together. The system determines whether to create an issue based on the volume and severity of those combined detections.



Navigate the Activity Detections Page

The **Activity Detections** page includes the following elements:

Item	Description
AI Activity Issue	The AI Activity issue with critical or high severity that AI Exposure detected.
Severity	The color-coded risk severity of the activity issue.
Filters	Filter issues by properties and rule type. Select from the following properties: • Account • AI Activity Detection • Severity • Identity • Starred • Status Update Time • System ID

Item	Description
	• Update Time • Verdict
Star	Star important or significant issues to mark them for later review.
Actions	Perform actions on an activity issue, such as: • **Set In Progress** • **Close** • **Comment** • **Send via email** – Send information about the AI activity to one or more email addresses. • **Create Jira issue** or **Create ServiceNow incident**. Available if you have Ticketing Integrations installed.
Bulk actions	Apply an action to multiple issues simultaneously.
Export	Export data to a CSV for analysis or processing by an external tool.
Column picker	Choose which columns to display in the issues table.

Export Activities Data

Export all issues related to AI activities to create a summary report of AI issues in your environment. The data is exported according to the current filters applied to the table. The output data is in CSV format and contains all relevant data, including remediation steps.

For example, you can perform the following tasks:

- Create a report of all closed issues, containing sub-status information about the reason for closure, to share with relevant stakeholders in your company.
- Create reports for open or starred issues, or any other subset of issues using filters.

To export AI activities:

1. In the AI Exposure Console, navigate to the relevant **Risk** > **Activity Issues** page.
2. (Optional) Apply filters to narrow down the list of activities.
3. Click **Export** to create and download the CSV summary report.

Comment on an Activity Issue

Add comments to an AI activity issue to provide additional context or flag important observations.
To add a comment to one or several activity issues:

1. In the AI Exposure Console, navigate to the **Risk** > **Activity Issues** page.
2. From the **Activity Issues** table:
   - *Single activity issue*: Click the three-dot icon next to it and select **Comment**.
   - *Multiple activity issues*: Select the relevant issues and click **Comment** at the bottom.
3. Enter your comment.
4. Click **Save**.
   The comments appear in the **Activity** tab within the Activity Details panel. You hcan edit or delete the comment from the **Activity** tab.

Close an Activity Issue Manually

When you resolve an AI issue and the underlying security issue, you can manually close the open issue.

When you manually close an issue, the issue is marked as **Closed (Manually closed)**. If you do this and the issue is not fixed, its status reverts to **Open (Reopened)** during the next system synchronization.

To mark and see closed issues:

1. From the Activity Issues table:
    1. *Single issue*: In the row of the issue, click the three dots icon and then click **Close**.
    2. *Multiple issues*: Select multiple issues and then click **Close** at the bottom of the table.
2. In the **Close Issue** dialog box, select the reason for closing the issue:
    - **Benign** – The flagged risk exists, but it does not pose a material threat or is already mitigated by other controls.
    - **False positive** – The flagged risk does not actually exist, or the alert is incorrect.
    - **True positive** – The flagged risk exists as reported, and poses a real threat.
3. In the **Comment** box, add a description of the reason for closing the issue, which is added to the activity issue.
4. Click **Close**.

Reopen an Activity Issue

You can reopen an issue that was manually closed. If you do so, the issue is marked as **Open (Reopened)**

To reopen an issue:

1. From the Activities Issues table:
    1. *Single Issue*: Click the three dots icon next to an individual issue, and then click **Open**.
    2. *Multiple Issues*: Select multiple issue and then click **Open** at the bottom.
2. In the **Open Issue** dialog, add a comment to indicate the reason for reopening, which is added to the activity issue.
3. Click **Open**.

Trigger Actions on AI Activity Issues

You can manually trigger actions associated with ticketing Integrations and/or send email notifications for individual activities.

> **Required AI Exposure User Role:** You must have either the **Collaborator** or **Administrator** role in AI Exposure to perform this action.

Trigger an Action for a Single Activity Issue

To manually trigger an action for a single activity issue:

1. In the AI Exposure Console, navigate to the **Risk** > **Activity Issues** page.
2. Click the activity issue for which you want to trigger an action. The issues panel appears.
3. In the upper-right corner, click the three dots menu and select the relevant action. (Click the ▶ icon below for instructions, per action)

> *Send via email*

1. Enter one or more email addresses. You can choose to send the information to the owners of the associated resources. This may include numerous recipients. For example, if the owner is a group with no associated email address, Tenable sends an email to all group members.
2. (Optional) Enter a message to the recipients.
3. Click **Send**.

> *Create a Jira issue*

1. Select a **Project**, **Issue Type**, **Assignee** (optional), **Labels**, **Epic** (optional), and **Environment** (URL of Jira instance). The project you select determines which values are available in the other field drop-down menus. For labels, you can either choose from a list of labels already configured in the Jira instance or manually add new labels. Label names cannot contain spaces.
2. (Optional) Edit the predefined content in the **Summary** and/or **Description** fields.

3. (Optional) Click **Add Optional Field** to include non-mandatory data like labels, assignees, or epics.
4. Click **Create Issue**.

Create a ServiceNow Incident

1. Select an **Instance**, **Assignment group**, an **Assignee**, a **Category** , **On hold reason**, **Service**, **Severity**, and a **Super user.**
2. (Optional) Edit the predefined content in the **Summary** and/or **Description** fields.
3. (Optional) Click **Add Optional Field** to include non-mandatory data.
4. Click **Create Incident**.

Send to Webhook

1. If you have more than one webhook configured, select the webhook that you want to send the issue to.
2. Click **Yes** to confirm.

Trigger an Action for Multiple Issues

Manually trigger an action for multiple activities. For Jira/ServiceNow, you can choose whether to:

- Create a single, unified ticket that includes all selected activities.
- Create separate tickets, one per selected issue.

> **Note:** When you trigger multiple Jira issues or ServiceNow incidents at once, you can't edit the summary or description fields. Each issue/incident will contain the default summary/description provided by AI Exposure.

To manually trigger an action for multiple issues:

1. In the AI Exposure Console, navigate to the **Risk** > **Activity Detections** page.
2. Select the checkboxes next to the issues that you want to trigger an action for.

3. From the bottom menu panel that appears, select the relevant action:
    - **Send to Webhook**
        1. If you have more than one webhook configured, select the webhook that you want to send the issues to.
        2. Click **Yes** to confirm.
    - **Share via email**
        1. Enter one or more email addresses. You can send the information to the owners of the associated resources. This may include numerous recipients. For example, if the owner is a group with no associated email address, Tenable sends an email to all group members.
        2. (Optional) Enter a message to the recipient/s.
        3. Click **Send**.
    - **Create Jira issues**
        1. Choose whether to:
            - **Create a unified Jira issue which includes all issues**
            - **Create separate Jira issues, one per issue**
        2. Select a **Project**, **Issue Type**, **Assignee**, **Epic** (optional), **Environment** (URL of Jira instance), and **Labels**. The Project you select determines which values are available in the other field dropdowns.
        3. (Optional) Click **Add Optional Field** to include non-mandatory data like labels, assignees, or epics.
        4. Click **Create Issue/s**.
    - **Create ServiceNow incidents**
        1. Choose whether to:
            - **Create a unified ServiceNow issue which includes all issues**
            - **Create separate ServiceNow issues, one per issue**
        2. Select an **Instance** and an **Assignee**.

3. Select an **Impact** and **Urgency** for the incident.
4. Click **Create Incident/s**.

View Activity Details

Click an activity issue to view granular information and remediate the associated risk.
From the details pane, you can perform the following actions:

- View the evidence that led to being flagged as a potentially harmful event.
- Click the **View Conversation** link to view the complete conversation with the AI platform.
- View a detailed historical account of the event, an expanded rationale for the potential risk it imposes, and specific remediation instructions.

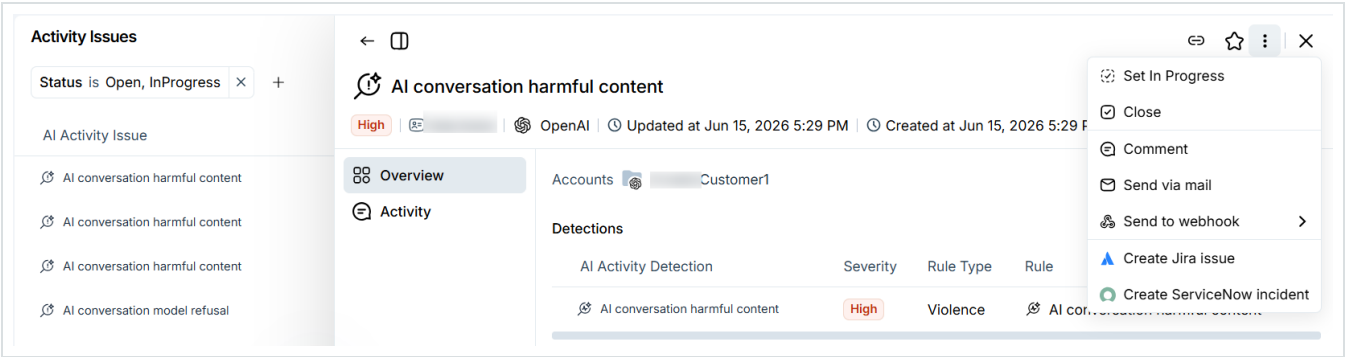
View Activity Issue Details

View the AI activity issue to see information about the lifecycle of the conversation within AI Exposure. For example, you can see when:

- The conversation was created.
- The status changed (either by the system or manually).
- Tickets were created for third-party integrations.

To view details of activity issues:

1. In the Activity Issues table, click the activity issue for which you want to view the details. A panel appears with details about the issue.



2. Click the **Overview** tab to view the related **Accounts** and **AI Activity Detections**.
3. Click the **Activity** tab to view all associated activities.

Add a Comment for an Activity Issue

To add a comment:

1. From the Activity Issues table, click a relevant AI activity issue.
2. Click **Activity**.
3. (Optional) Write a comment and then click **Save**. AI Exposure saves the comment to the activity issue.

Supported Languages for AI-Powered Features

Tenable One AI Exposure processes natural-language input across a broad range of languages, enabling detection of AI threats in languages other than English.

Tenable's AI Exposure detections are trained to identify threats across 10 core languages.

- English
- Mandarin
- Spanish
- German
- Japanese
- French
- Arabic
- Portuguese
- Hindi
- Italian

This capability can also potentially process input in hundreds of additional languages beyond this core set. For these additional languages, success rates vary significantly by language.

Caution: Tenable recommends validating output quality for any language outside the core set of languages before relying on it.

Policies

AI Policies

The **Policies** page is where you view your AI posture policies.

Use this page to see the predefined policies that determine which posture findings Tenable One AI Exposure and AISPM generate. You can also filter, customize the table, and drill into a specific policy's details.

Policies are grouped into the following categories:

- Data
- Excessive access
- Insufficient encryption
- Missing observability
- Risky Tools

Manage Policies

To view and manage policies:

1. In the AI Exposure Console, click **Policies**.
2. Select an account scope in the **Organization** dropdown to enable/disable a policy on a specific subset of cloud accounts. By default, the entire Organization (all accounts) is selected.
3. Filter the table to narrow the scope of the visible data. Use the column picker on the top right of the table to choose which columns to display. See Policy Column Data for more information.
4. In the row of the policy, click the three-dots icon and select **Edit**.

5. Click a policy to open a slideout panel that contains more information and click the three-dots icon and select **Edit**.
6. Edit the policy configuration to enable or disable the policy.

Policy Column Data

The following columns appear in the table on the **Policies** page.

Filter	Description
Provider	The AI service provider. Possible values include: Microsoft Copilot, Google Gemini, OpenAI ChatGPT, or Anthropic Claude.
Category	The logical category to which the policy belongs.
Name	The name of the policy.
Severity	The severity level of the policy, which determines the severity level of any findings triggered by the policy.
Status	Whether the policy is enabled or disabled. You can Enable and Disable Policies so that the policies do not trigger findings for resources in those accounts.
Findings	The total number of findings triggered by the policy.
Modified By	The user identity that modified the policy.
Created By	The user identity that created the policy.
Creation Time	The time of policy creation.
Policy Settings ⋮	• **Edit** – Click **Edit** to enable or disable the required policy.

Enable and Disable Policies

By default, out-of-the-box policies are enabled and apply to all accounts in your organization. You can fine-tune this configuration by either disabling a policy across your entire organization, or just for a specific subset of accounts or folders.

See Account Hierarchy and Folders for more information about grouping accounts together using folders.

Caution: Disabling a policy deletes all associated findings in the relevant accounts and prevents new findings from being created. This action occurs after the next data synchronization and is irreversible.

Note: Enabling and disabling policies is only available to users with the *Administrator* role. Some policies that relate to low-severity issues are disabled by default, but can be enabled if required to achieve compliance or for another security goal.

To enable or disable a policy:

1. In the AI Exposure Console, click **Policies**.
2. Select an account scope in the **Organization** dropdown to enable/disable a policy on a specific subset of cloud accounts. By default, the entire Organization (all accounts) is selected.
3. Navigate to the relevant policy.
4. Click the three dots menu ⋮ and click **Edit**.
5. In the **Status** section, choose a relevant option:
   - **Enabled** (*overrides parent-level configuration*). AI Exposure creates findings when policy rules are violated.
   - **Disabled** (*overrides parent-level configuration*). AI Exposure does not create findings when policy rules are violated.
6. Click **Save**.

Note: If you override the parent-level configuration, the unique configuration remains, regardless of any changes made in the parent-level scope.

AI Activity Rules

The **Activity Rules** page is where you configure AI conversation detection rules.

These rules trigger detections for AI conversations that fall into the following categories within your environment:

- **AI Attacks** – Attacks such as jailbreak attempts and prompt injections.
- **AI Misuse** – Misuse such as hate speech, violence, and overreliance in hiring decisions.
- **Data Exposure** – Exposure of sensitive information such as API credentials, access keys, and payment details.

Activity Rules Column Data

The following columns appear in the table on the **Activity Rules** page.

Filter	Description
Provider	The AI service provider. Possible values include: Microsoft Copilot, Google Gemini, OpenAI ChatGPT, or Anthropic Claude.
Category	The logical category that the policy belongs to.
Name	The name of the policy.
Severity	The severity level of the policy, which determines the severity level of any findings triggered by the policy.
Status	The status of the activity rule (enabled or disabled). You can enable and disable rules so that they do not trigger detections for resources in those accounts.
Modified By	The user who modified the activity rule.
Modified Time	The time the activity rule was modified.
Created By	The user who created the activity rule.
Creation	The time of rule creation.

Filter	Description
Time	
Activity Rule Settings ⋮	• **View Findings** – Click this option to navigate to the **AI Detections** page. • **Edit** – Edit the activity rule to enable or disable the rule.

View Activity Rule Details

When you click a rule in the Activity Rules table, a slideout panel opens on the right side of the page. The panel displays metadata, configuration status, and the content types associated with that rule.

The Activity Rule details panel includes the following:

Section	Field	Description
Details	Policy ID	The unique identifier for the rule.
	Severity	The severity level of the rule. Displays **Dynamic** when severity is calculated based on the content types detected in a conversation.
	Provider	The cloud provider(s) the rule applies to. A **+count** indicates additional providers.
	Activity Detections	A link showing the total number of detections triggered by this rule. Click the link to open the **Activity Detections** page filtered to this rule.
	Modified By	The user or system that last modified the rule. Tenable-managed rules display **Tenable**.
	Created By	The user or system that created the rule. Tenable-managed rules display **Tenable**.

Section	Field	Description
	Modification Time	The date and time the rule was last modified.
	Creation Time	The date and time the rule was created.
Configuration	Status	Indicates whether the rule is active. Displays **Enabled** or **Disabled**.
Content Types		Lists the specific data types in the specific AI conversation. Each entry includes the content type name, source (engine output, user input, or both), its classification category, severity level, detection sensitivity, and enabled status.

Manage Activity Rules

To view and manage activity rules:

1. In the Tenable One AI Exposure Console, click **Policies** > **Activity Rules**.
2. Filter the table to narrow the scope of the visible data. Use the column picker on the top right of the table to choose which columns to display. See Policy Column Data for more information.
3. Click an AI activity rule to open a slideout panel with more information. Review and manage the rule.
4. In the Activity Rules panel, click the three-dot menu and select one of the following:
    - Select **View Findings** to navigate to the **AI Detections** page that the selected Activity Rule triggers.
    - Click **Edit** to enable or disable the rule.

Enable and Disable Activity Rules

By default, predefined rules are enabled and apply to all accounts in your organization. You can choose to fine-tune this by either disabling a policy across your entire organization or just for a specific subset of accounts or folders.

For more information about grouping accounts together using folders, see Account Hierarchy and Folders. For example, you may want to disable a policy if there is a low-severity misconfiguration that your organization decides not to fix.

Caution: Disabling a rule deletes all associated findings in the relevant account/s and prevents new findings from being created. This action occurs after the next data synchronization and is irreversible.

Note: Enabling and disabling activity rules is only available to users with the *Administrator* role. Some rules that relate to low-severity issues are disabled by default but can be enabled if required to achieve compliance or for another security goal.

To enable or disable an activity rule:

1. In the AI Exposure Console, click **Policies** > **Activity Rules**.
2. Navigate to the relevant activity rule.
3. Click the three dots menu ⋮ and click **Edit**.
4. In the **Status** section, choose a relevant option:
    - **Enabled**: AI Exposure creates AI Detections when activity rules are violated.
    - **Disabled**: AI Exposure does not create AI Detections when activity rules are violated.
5. Click **Save**.

Classification Rules

Configure the following settings and scope to fine-tune how Tenable One AI Exposure scans your data to detect different content types across your environment. The different content types are split into two domains:

- Data Types
- AI Abuse

You can configure how each content type is handled to meet your organizational requirements. This includes changes such as updating its status (whether to detect it or not), its severity, or enabling or disabling content type detection.

These adjustments affect labeling and how the data appears across findings and dashboards, but they do not affect core scanning behavior. You must be an admin to edit data types.
You can adjust the following properties:

- **Severity** – Assign a different severity level to the content type.
- **Status**:
  - **Enabled** – The content type is classified and appears in findings.
  - **Disabled** – The content type is not classified and does not appear in findings or risk calculations.

These adjustments affect labeling and how the data appears across findings and dashboards, but they do not affect core scanning behavior. You must be an administrator to edit the content type configuration.

Reports

Reports

Create a one-time or scheduled report of relevant Tenable One AI Exposure data. Each report is generated in a different format, depending on the purpose of the report:

- **CSV** – Use as a working document that you can edit, collaborate on, and share for feedback from others.
- **PDF** – Use to visualize data and share with executive leadership or other relevant stakeholders.

Create a Report

To create a new report:

1. In the AI Exposure Console, click **Reports > Generated Reports**.
2. (Optional) In the **Organization** drop-down list, select a scope to define the group of accounts or IdP tenants for the report data. *The report is accessible to users with permissions in the selected scope*. The **Scope** you select appears in the **New Report** dialog.
3. Click **Create Report**.
4. Enter a name.
5. In the drop-down list, select a report type.
6. Depending on the report type you select, configure the additional fields.
   - **Query** – Click Select query to choose an existing query, or build a query from scratch.

     > **Note:** You cannot delete, make private, or edit linked queries using unsupported syntax.

   - **Dashboard** – Select a dashboard type from the list of built-in options.
7. Choose a **Delivery Time**:
   - **Now** – Generate a one-time report.
   - **Schedule** – Define a cadence to generate reports at specific times. You can set custom intervals (for example, every three weeks, or every six months) and specific days of the week for weekly deliveries.
8. Add **Delivery Methods** to send a copy of the report to specific recipients. See Teams for more information.

   > **Note:** When you send reports by email, the file size limit is 14.5 MB. Tenable compresses larger reports or provides them through a download link.

9. Click **Create** or **Schedule**.

Duplicate a Report

You can duplicate any previously generated report (one-time or scheduled) to use as a baseline for creating a new report. This allows you to quickly create a new report with the same configuration as a previous one, which saves you time and effort.

When you duplicate an item, AI Exposure handles any associated configurations (such as delivery methods and labels) based on their original scope:

- If an associated configuration was set up on a narrower scope than your current one, the configuration does not duplicate with the item. For example, if you duplicate an item from a specific scope into your broader Organization scope, any configurations tied only to that narrower scope do not carry over.

This helps prevent irrelevant or misconfigured data from being created in your new scope. To use these specific configurations, you must reconfigure them manually within your current scope.

To duplicate an existing report:

1. In the AI Exposure Console, click **Reports > Generated Reports**.
2. (Optional) In the **Organization** drop-down list, select a scope to define the group of accounts for the report data. *The report is accessible to users with permissions in the selected scope*.
3. In the table, click the three dots menu next to the relevant report and then click **Duplicate**.
4. Modify the report as needed and then click **Create**. See Create a Report for more information.

Report Types

You can create the following report types from the **Reports** page:

Report	Description
Query (CSV)	A portable snapshot of investigation results. It captures all active rows and columns (for example, Principal, Labels, and Tags) providing point-in-time data for offline analysis and auditing.

Report	Description
Dashboard (PDF)	Generates reports from public dashboards to simplify sharing insights. Automatically provides stakeholders with actionable data, such as executive overviews or findings trends. Reports remain dynamically connected to the dashboard, ensuring updates to widgets or names are reflected in future deliveries.

View and Edit Scheduled Reports

After you schedule a report, you can view and edit the report schedule and any delivery methods.

To view and edit scheduled reports:

1. In the AI Exposure Console, click **Reports > Scheduled Reports**.
2. Navigate to the **Scheduled Reports** tab.
3. Select an account scope in the **Organization** dropdown to define the group of accounts/IdP tenants that you want to access reports for.
4. Find the relevant report, using the **Type** filter to narrow the list, if necessary.
5. Click the **Edit** button to make any changes to the scheduled report.
6. Click the **Delete** button to delete the scheduled report.

Access Historical Reports

Every time you create a report AI Exposure saves a copy of the report for future reference.

To access historical reports:

1. In the AI Exposure Console, click **Reports > Generated Reports**.
2. Select an account scope in the **Organization** dropdown to define the group of accounts or IdP tenants that you want to access reports for.

3. Use the filters to narrow the list of reports according to the **Creation Time** and the **Type** of report.
4. Click **View report** to see a copy of the historical report in a browser.
5. Click the **Download** button to download a copy of the report.
6. Click the **Delete** button to delete the copy of the report.

Other Ways to Export Data

While the **Reports** page serves as the central hub for report creation, you can also export data from other areas in the AI Exposure console:

- Export Inventory Data – Export all data for a specific inventory view, by resource type in CSV format. For example, export all AI agents inventory data.
- Create a Report from Query Data – Export your investigation results as CSV reports.

Settings

Audit

View audit log information about user actions performed within the Tenable One AI Exposure Console. For example, you can monitor:

- Administrative activities such as managing users, onboarding cloud accounts, or integrating AI Exposure with 3rd party tools.
- Open and resolved findings
- Remediation of findings

Note: You can also:

- Create automations that send audit log data to third-party tools. See Send Finding Data to Third-Party Tools for more information.
- Access audit log data programmatically via the GraphQL API.

To view audit log information:

1. In the AI Exposure Console, navigate to **Settings** > **Audit**.
2. Filter the table to narrow the scope of the visible data. Each action entry lists information about:
    - Time - When the action was performed (based on the local time of the user viewing the audit log).
    - User - Who performed the action. By default all users are selected in the filter. Although not selected by default, you can also filter for system actions (for example, when a finding was created or updated).
    - Action - The action performed. For example:
        - Add account
        - Add user
        - Automation rule created/updated
        - Finding updated
        - User sign-in/sign-out
    - Result - Whether the action succeeded or failed.
    - Scope - Which accounts the action was performed on. By default, all accounts are included in the filter.
    - Details
3. Export the currently filtered results of the audit log to a CSV file.

Access Management

Users and Groups

Add new users/groups and assign them specific permissions within the Tenable One AI Exposure Console.

> **Note:** You can also add users via the API.

Tenable One customers:

- Tenable One users with the Administrator role are automatically assigned Administrator role permissions within AI Exposure with access to the entire Organization, even if such permissions were not explicitly granted in the AI Exposure Console.
- To allow non-Administrator users/groups to access the AI Exposure Console, they must first be defined and granted access in Tenable One, and then added in the AI Exposure Console.
- Tenable One users with any role can be granted access to AI Exposure at a specific account scope by assigning them the desired scope when you add a user/group.

New users/groups are added within a specific scope that defines which accounts the user has access to in AI Exposure. For example, you can add a user to the entire organization (all accounts) or a subset of accounts. See Account Hierarchy and Folders for more information.

If you add an individual user, and that user is also a member of a group that you added, the user will have the highest-level access granted by the role/scope assigned to the user/group, if they are different. For example, in the following situation:

- *User X*: Role = Administrator; Scope = All AWS accounts
- *Group Y* (User X is a member): Role = Collaborator; Scope = Entire Organization

User X will have Administrator permissions for the entire Organization.

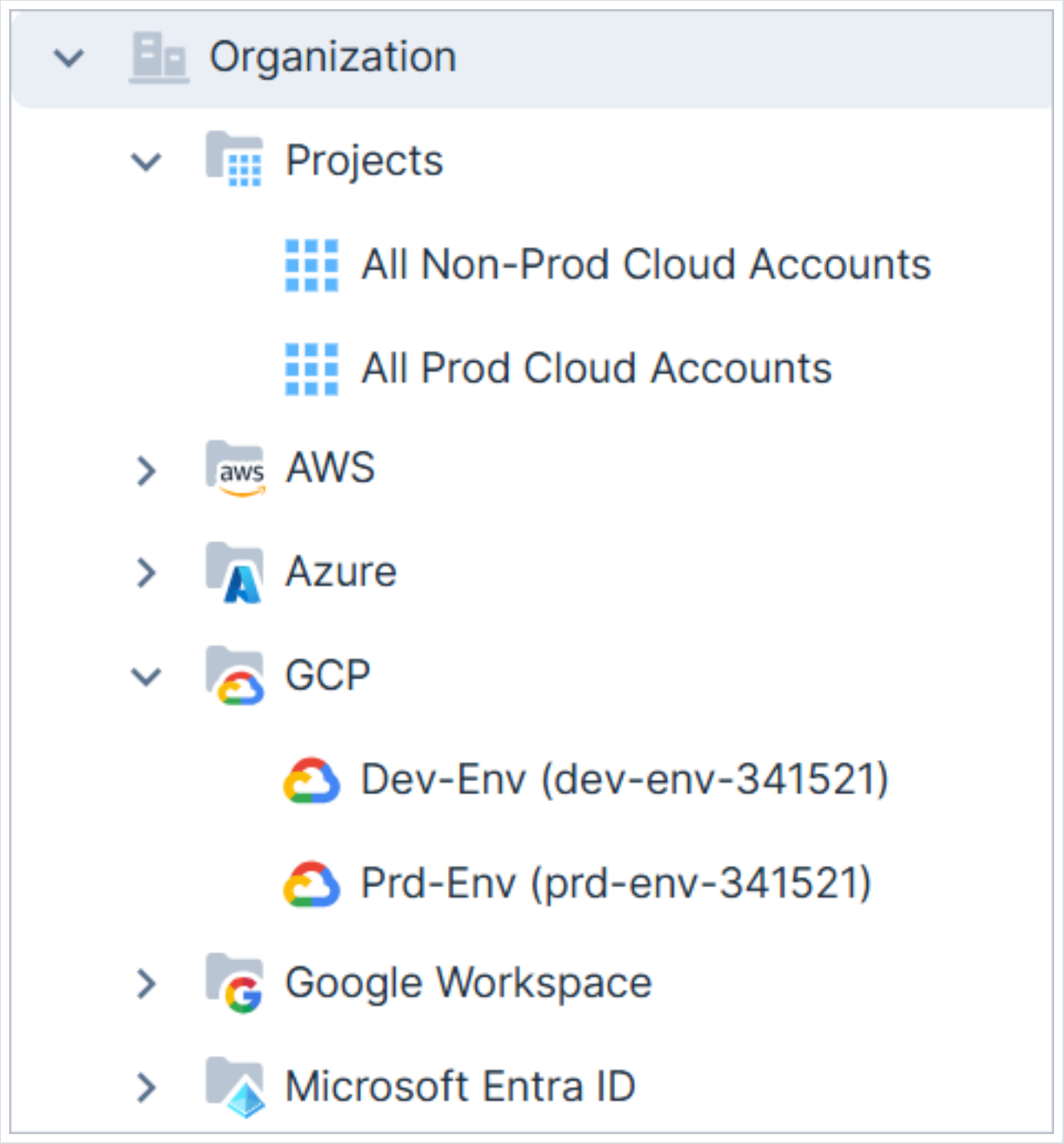
> **Note:** If you have SSO configured for logging in to AI Exposure, the user email addresses that you add must be existing users within your organization.

Add a New User

> **Note: Tenable One customers**: To allow users to access the AI Exposure Console, they must first be defined and granted access in Tenable One, and then added in the AI Exposure Console.

To add a new user:

1. Navigate to **Settings > User Management**.
2. Select a scope for the user in the **Organization** tree on the top of the page:



A scope can be any of the following:

1. The entire Organization (all accounts onboarded to AI Exposure).
2. A group of accounts. For example, all accounts belonging to a specific cloud provider (all AWS accounts) or identity provider (all Microsoft Entra tenants), or a group of accounts within a specific cloud provider (grouped by folder).
3. A specific account/identity provider tenant.
4. A project, or project folder.
5. All **IaC** organizations, or a subset of individual repositories. This grants access to view code scan results for a specific scope.

> **Note:** Adding a user within an IaC scope will **only** grant the user access to IaC-related features. Such a user will not have access to cloud resources, or to other features such as the Dashboard. The IaC hierarchy is only available within the context of Tenable RBAC (adding users/groups), and will not be visible in other contexts (for example, Policies or Reports).

See Inherited Users for more information about how users created on a parent level are inherited to children accounts.

3. Click **Add Role Assignment**, and for **Principals**, select **User**.
4. In the box, search for and select the user's email address.

   If you have SSO configured for logging in to AI Exposure, the user email address that you add must be an existing user within your organization.
5. Assign a **Role** to the user and then click **Save**:
   1. **Viewer** - View access to AI Exposure (except for Administrative tabs)
   2. **Collaborator** - All *Viewer* permissions, plus the ability to categorize resources and respond to findings.
   3. **Administrator**- All *Collaborator* permissions, plus the ability to administer AI Exposure (add accounts, configure settings, view audit trail).
   4. **JIT Administrator** - Manage JIT eligibilities and view JIT audit trail via the JIT Portal.

   Custom roles also appear in the **Role** drop-down box. For information about creating and managing custom roles, see Roles.

   For a detailed list of permissions granted by each built-in role, see Roles and Permissions.

6. If you need to change the permission level of a user, select the Edit icon next to the user, choose a new role, and then **Save**.

> **Note:** If you change your own role from an Administrator to either Collaborator or Viewer, you will no longer be able to access User Management to edit your role.

Add a New Group

> **Note: Tenable One customers**: To allow group members to access the AI Exposure Console, relevant groups must first be defined in Tenable One, and then added in the AI Exposure Console.

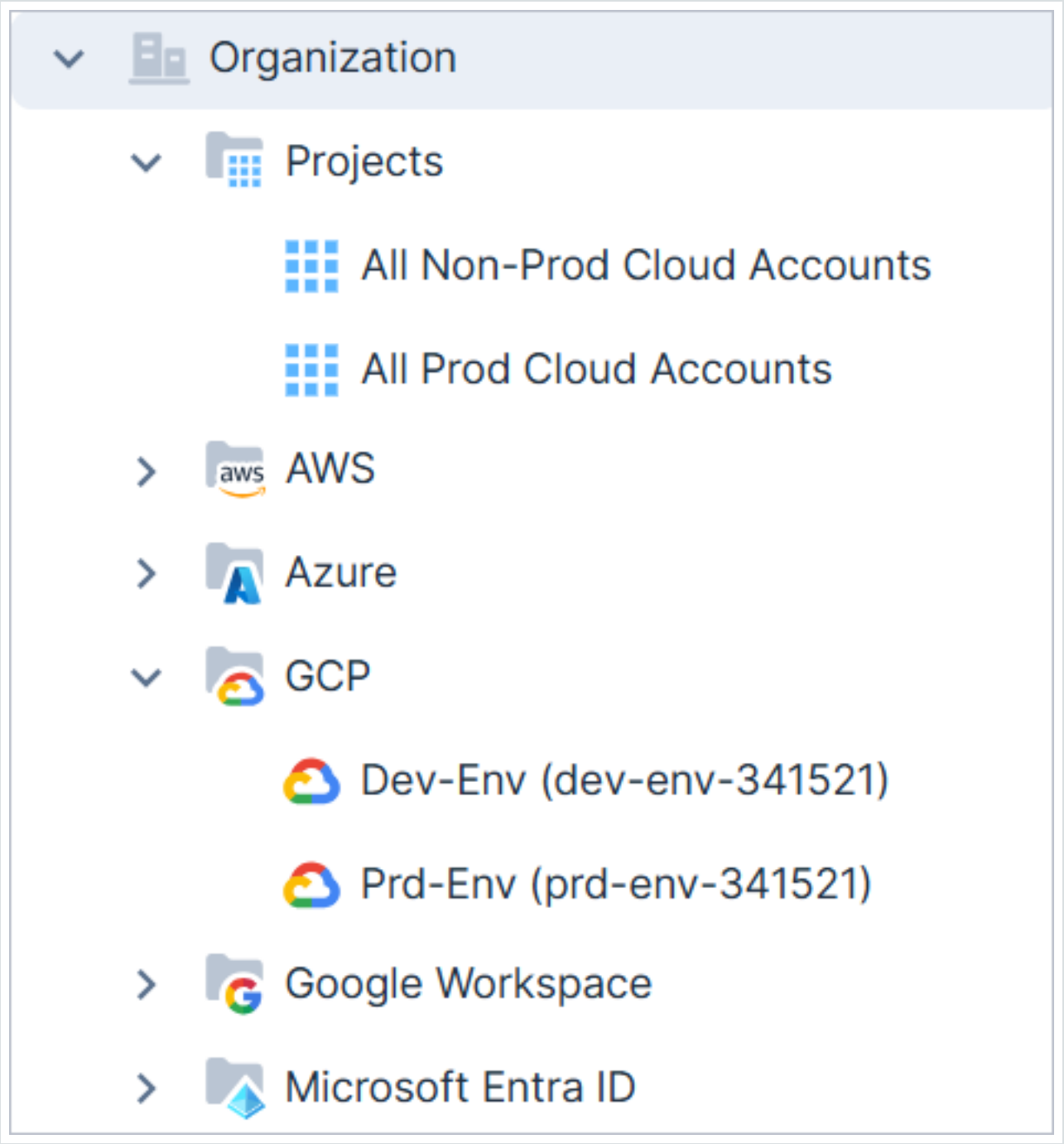
Prerequisites:

Before you can add a new group in the AI Exposure Console, follow the steps to Single Sign-On by:

- establishing trust between your IdP and Tenable.
- configuring group mapping for your IdP to send group claims to AI Exposure.

To add a new group:

1. Navigate to **Settings > User Management**.
2. Select a scope for the group in the Organization tree on the left:



A scope can be any of the following:

1. The entire Organization (all accounts onboarded to AI Exposure).

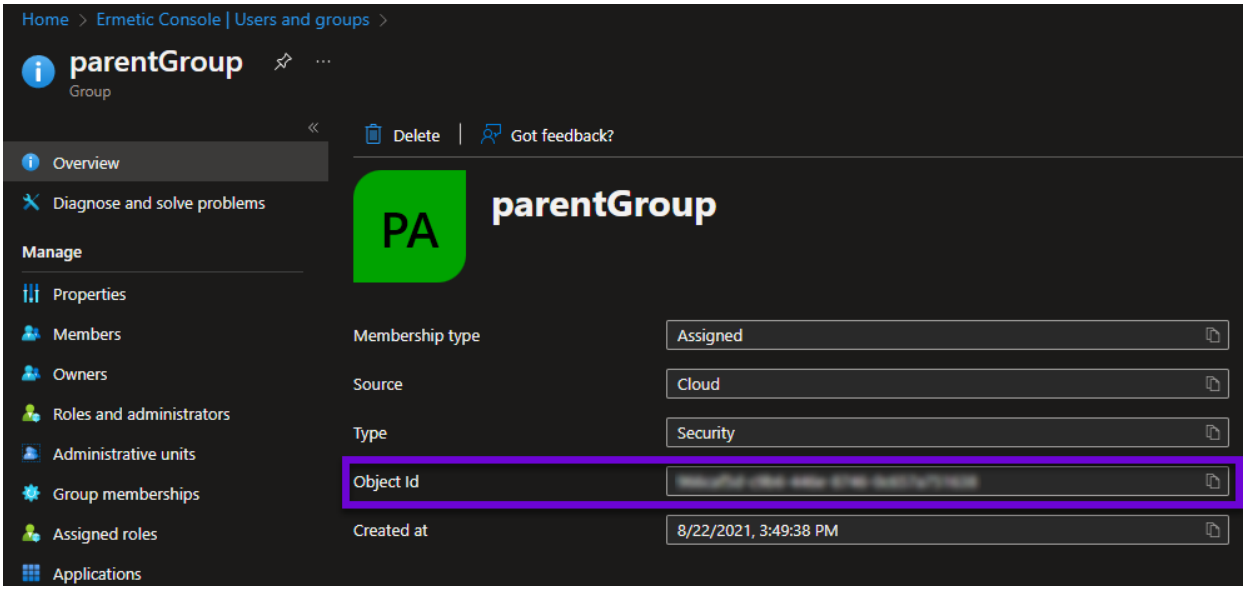
2. A group of accounts. For example, all accounts belonging to a specific cloud provider (all AWS accounts) or identity provider (all Microsoft Entra tenants), or a group of accounts within a specific cloud provider (grouped by folder).
3. A specific account/identity provider tenant.
4. A project, or project folder.
5. All **IaC** organizations, or a subset of individual repositories. This grants access to view code scan results for a specific scope.

   > **Note:** Adding a user within an IaC scope will **only** grant the user access to IaC-related features. Such a user will not have access to cloud resources, or to other features such as the Dashboard. The IaC hierarchy is only available within the context of Tenable RBAC (adding users/groups), and will not be visible in other contexts (for example, Policies or Reports).

   See Inherited Users for more information about how users created on a parent level are inherited to children accounts.

3. Click **Add Role Assignment**, and for **Principals**, select:
   - **Group** – Use this option for groups defined in your identity provider.
   - **Microsoft Entra ID Group** – (only available if the Microsoft Entra ID integration is configured). Select this option only if you are adding a Microsoft Entra ID group, since these require a group ID in addition to a group name.
4. Enter the group information. The fields depend on the option you selected in step 3.
   - **Group Name** – For groups added using the **Group** option, this is the group name as defined in your identity provider. For groups added using the **Microsoft Entra ID Group** option, this is the name that will appear in the AI Exposure Console.
   - **Group ID** (**Microsoft Entra ID Group** only). The Microsoft Entra ID Group **Object ID**

(GUID) of the group you want to add.



5. Assign a **Role** to the group and then click **Save**:
    1. **Viewer** - View access to AI Exposure (except for Administrative tabs)
    2. **Collaborator** - All *Viewer* permissions, plus the ability to categorize resources and respond to findings.
    3. **Administrator**- All *Collaborator* permissions, plus the ability to administer AI Exposure (add accounts, configure settings, view audit trail).
    4. **JIT Administrator** - Manage JIT eligibilities, and view JIT audit trail.

    Custom roles also appear in the **Role** drop-down box. For information about creating and managing custom roles, see Roles.

    For a detailed list of permissions granted by each role, see Roles and Permissions.
6. If you need to change the permission level of a group, select the Edit icon next to the group, choose a new role, and then **Save**.

> **Note:** If you change your own role from an Administrator to either Collaborator or Viewer, you will no longer be able to access User Management to edit your role.

Inherited Users

Users created on the organization level or within a group of accounts are inherited to all children accounts, including to any children accounts created at a later time. For example, if you create “User X” on the organization level and assign it the *Collaborator* role, “User X”, with the same role, will exist and have permissions to all children accounts. If, at a later time, you add a new account/s to the organization, “User X” will have permissions to the new account as well.

In the User Management table, under a child account, “User X” will appear, and the Role column will indicate that the user is inherited.

Within a child account, you can only edit an inherited user’s role to increase the user’s permission level. For example, a user with the *Collaborator* role can be changed to “Administrator”, but not cannot be reduced to “Viewer”. Likewise, a user granted the “Administrator” role within a parent account/group cannot have their role changed at all. See Roles and Permissions for more information.

Built-in Roles and Permissions

There are three built-in roles that can be assigned to users/groups.

- **Viewer**
- **Collaborator**
- **Administrator**

In addition, an **Owner** role exists to provide greater clarity and definition to the single person responsible for owning and managing the AI Exposure environment at any given time:

- The Owner role has the same permissions as an Administrator.
- Only one user can have the Owner role at any given time.
- A user with this role can transfer ownership to another user.

Administrators can also create custom roles with granular, module-level permissions. See Roles for more information.

Each role provides a different level of access within the AI Exposure Console. The following table provides a detailed list of permissions granted by each role.

Permission	Sub-Permission	Viewer	Collaborator	Administrator	JIT Administrator
Dashboards					
	View	✓	✓	✓	–
	Manage – Private Dashboards	✓	✓	✓	–
	Manage – Public Dashboards	–	✓	✓	–
Inventory					
	View	✓	✓	✓	–
	Manage	–	✓	✓	–
Workload Resources					
	Scan Now	–	✓	✓	–
Data Resources					
	Scan	–	✓	✓	–
Events					

Permission	Sub-Permission	Viewer	Collaborator	Administrator	JIT Administrator
	View	✓	✓	✓	–
CI/CD Scans					
	View	✓	✓	✓	–
Queries					
	View	✓	✓	✓	–
	Manage – Private Queries	✓	✓	✓	–
	Manage – Public Queries	–	✓	✓	–
Risks					
	View	✓	✓	✓	–
	Manage – Comment	–	✓	✓	–
	Manage – Status	–	✓	✓	–
	Manage – Star	–	✓	✓	–
	Manage – Remediation	–	✓	✓	–

Permission	Sub-Permission	Viewer	Collaborator	Administrator	JIT Administrator
	Manage – Share	–	✓	✓	–
Threats					
	View	✓	✓	✓	–
	Manage – Comment	–	✓	✓	–
	Manage – Change Status	–	✓	✓	–
	Manage – Share	–	✓	✓	–
	Manage – Star	–	✓	✓	–
Vulnerabilities					
	View	✓	✓	✓	–
Malicious Files					
	View	✓	✓	✓	–
Policies					
	View	–	✓	✓	–

Permission	Sub-Permission	Viewer	Collaborator	Administrator	JIT Administrator
	Manage	–	✓	✓	–
Exclusions					
	View	✓	✓	✓	–
	Manage	–	✓	✓	–
AI Activity					
	View	✓	✓	✓	–
	Manage	–	✓	✓	–
Automation					
	View	✓	✓	✓	–
	Manage	–	✓	✓	–
Reports					
	View	✓	✓	✓	–
	Manage	–	✓	✓	–
Compliance					
	View	✓	✓	✓	–
	Manage	–	✓	✓	–
Integrations					
	View	✓	✓	✓	–

Permission	Sub-Permission	Viewer	Collaborator	Administrator	JIT Administrator
	Manage	–	–	✓	–
Settings					
	View	–	–	✓	–
	Manage	–	–	✓	–
Settings - Organization					
	View	✓	✓	✓	–
	Manage	–	–	✓	–
Settings - Audit					
	View	✓	✓	✓	–
JIT - Eligibility					
	View	–	–	✓	✓
	Manage	–	–	✓	✓
JIT - Audit					
	View	–	–	✓	✓

* Administrators who were assigned a limited account scope (anything less than the entire Organization) may have partial access to certain Settings pages. See Settings Access for Administrators: Full vs. Limited Scope for more information.

Integrations + Organization dependency: The **Create Integration** button requires both the **Integrations** and **Organization** permissions. Users who hold only one of the two cannot create integrations.

Single Sign-On

Important: New Tenable One customers should set up SSO via Tenable One. However, if you want to use Identity Provider (IdP) groups, you'll also need to follow the guidelines in this article to add support for groups. **JIT Access**: To enable JIT Portal login via SSO, follow these guidelines.

Allow individual users or group members to log in to the Tenable One AI Exposure Console via SSO by establishing trust between your external identity provider (IdP) and Tenable. This process eases user provisioning by leveraging the existing corporate identities of your users. It does not, however, provide for automatic user provisioning: after trust is established, you still need to add new users or groups via the console, or via API.

Leverage existing IdP groups to grant all users associated with the group identical permissions in AI Exposure. To add support for IdP groups in Tenable, first configure group mapping for your IdP to send group claims to Tenable using the relevant procedure below, and then add any relevant groups in Tenable.

You can enable Console login using any of the following IdPs:

- AWS Identity Center
- Google
- Microsoft Entra ID
- Okta
- OneLogin
- Ping Identity
- JumpCloud

If you work with a provider other than one of those listed above, you can enable login to the AI Exposure Console via that provider by leveraging the SAML 2.0 identity specification. See Enable Login via Custom SAML 2.0 Provider for more information.

For more information about enabling SSO login, contact Technical Support.

Enable Login via Tenable One

New Tenable One customers should follow these guidelines for setting up SSO via Tenable One.

Enable Login via AWS Identity Center (SAML 2.0)

Use AWS Identity Center as your identity provider (IdP) to enable login to the AI Exposure Console via SAML 2.0.

Before you begin:

- **Prerequisite: Authentication Domain** The email domain used by your AWS Identity Center users must be added as an authentication domain in AI Exposure. If the domain is not configured, uploading the SAML metadata will fail during SSO setup.

To enable login using AWS Identity Center (SAML 2.0):

1. In AWS, open **AWS Identity Center**.
2. Navigate to **Applications** and click **Add application**.
3. Select **I have an application I want to set up**, choose **SAML 2.0**, and then click **Next**.
4. Under *Configure application*, enter a **Display name** and **Description** (for example, *Enabling Console access via SSO for AI Exposure*).
5. Under *Application properties*, enter the value of the **Application start URL**:
    - **Global (All regions)**: `app.tenable.com`
    - **United States Gov Cloud**: `app.tenable.us`
6. Under *Application metadata*:
    1. Enter the value of the **Application ACS URL** :
       https://{URL}/api/console/authentication/saml2/customer/acs

Where {URL} is:

- **Global (All regions)**: `app.tenable.com`
- **United States Gov Cloud**: `app.tenable.us`

2. For **Application SAML audience**, enter:

   urn:app.ermetic.com

   > **Note:** The Application SAML Audience (also known as the Entity ID) uniquely identifies AI Exposure as the service provider. This value is not region-specific.

7. Click **Submit** to create the application.
8. Click **Assign users and groups** to assign any users or groups that should access the AI Exposure Console:
   1. From the search bar, add the relevant users or groups.
   2. Click **Assign**.

9. After the application is created, open it and select **Actions > Edit attribute mappings**:
    1. Review or add the following attribute mappings*:

User Attribute in the Application	Maps to This String Value or User attribute in IAM Identity Center	Format
Subject (NameID)	`${user:email}`	emailAddress
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	`${user:email}`	unspecified
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	`${user:givenName}`	unspecified
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	`${user:familyName}`	unspecified
groups (optional)	`${user:groups}`	unspecified

    *The **groups** attribute is case sensitive. Enter it exactly as shown if you plan to use AWS groups.

    2. Click **Save changes**.
10. Still on the application page, select **Actions > Edit configuration**, and download the **IAM Identity Center SAML metadata file**.
11. In the AI Exposure Console, navigate to **Settings > Access Management > Single Sign-On**.
12. Click **Add Identity Provider** and then select **SAML**.
13. In the **Choose Application** drop-down, select **AI Exposure**.

14. Select **File**, upload the metadata file downloaded from AWS Identity Center, and click **Add**.

Enable Login via Google

Enable login to the AI Exposure Console via Google using one of the following identity specifications:

- OpenID Connect (OIDC)
- SAML

> **Note:** To work with groups in AI Exposure using Google as your IdP, you will need to use SAML and not OIDC.

Enable Login via Google Using OIDC

To enable login using OIDC:

1. In the AI Exposure Console, navigate to **Settings** > **Access Management** > **Single Sign-On**.
2. Click **Add Identity Provider** and then click **Google**.
3. In the **Add Identity Provider** dialog, click **Add**.

> **Note:** Adding Google as an IdP in this way enables login to both the AI Exposure Console and the JIT Portal.

Enable Login via Google Using SAML

To enable login using SAML:

1. In the Google Admin console, navigate to **Apps > Web and mobile apps**.
2. Click **Add app > Add custom SAML app**.
3. Enter an **App name** and then click **CONTINUE**.
4. On the Google Identity Provider details page, click to **DOWNLOAD METADATA**.
5. In the AI Exposure Console, navigate to **Settings** > **Access Management** > **Single Sign-On**.
6. Click **Add Identity Provider** and then click **SAML**.

7. In the **Add Identity Provider** dialog, select **AI Exposure** from the dropdown.
8. Select **File**, upload the metadata that you downloaded from Google, and then click **Add**.
9. In the Google Admin console, on the Service provider details page, enter the following values for the respective fields:
    - *ACS URL*: **https://{URL}/api/console/authentication/saml2/customer/acs**

      Where `{URL}` is:
        - **Global (All regions)**: `app.tenable.com`
        - **United States Gov Cloud**: `app.tenable.us`
    - *Entity ID*: **urn:app.ermetic.com**
    - *Name ID format*: **EMAIL**
    - *Name ID*: **Basic Information > Primary email**
10. Click **CONTINUE**.
11. On the Attribute mapping page, click **ADD MAPPING**, and then add the following attributes:

    Google Directory Attributes to Mappings (App Attributes):
    - **First name** – http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
    - **Last name** – http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
    - **Primary email** – http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
12. (Optional) Add Support for Google Groups.
13. Click **FINISH**.

Add Support for Google Groups

To work with groups using Google as your IdP, you will need to use SAML and not OIDC.

To add support for Google groups:

1. In the Google Admin console, navigate to **Apps > Web and mobile apps** and open the SAML application that you configured (See Enable Login via Google Using SAML).
2. Expand the **SAML attribute mapping** section.

3. Under Group membership (optional), enter the following:
    - The **Google groups** that you want to use as groups in AI Exposure.
    - For *App attribute*, type **groups**.
4. Click **SAVE**.
5. After you finish, add the group/s in the AI Exposure Console.

Enable Login via Microsoft Entra ID

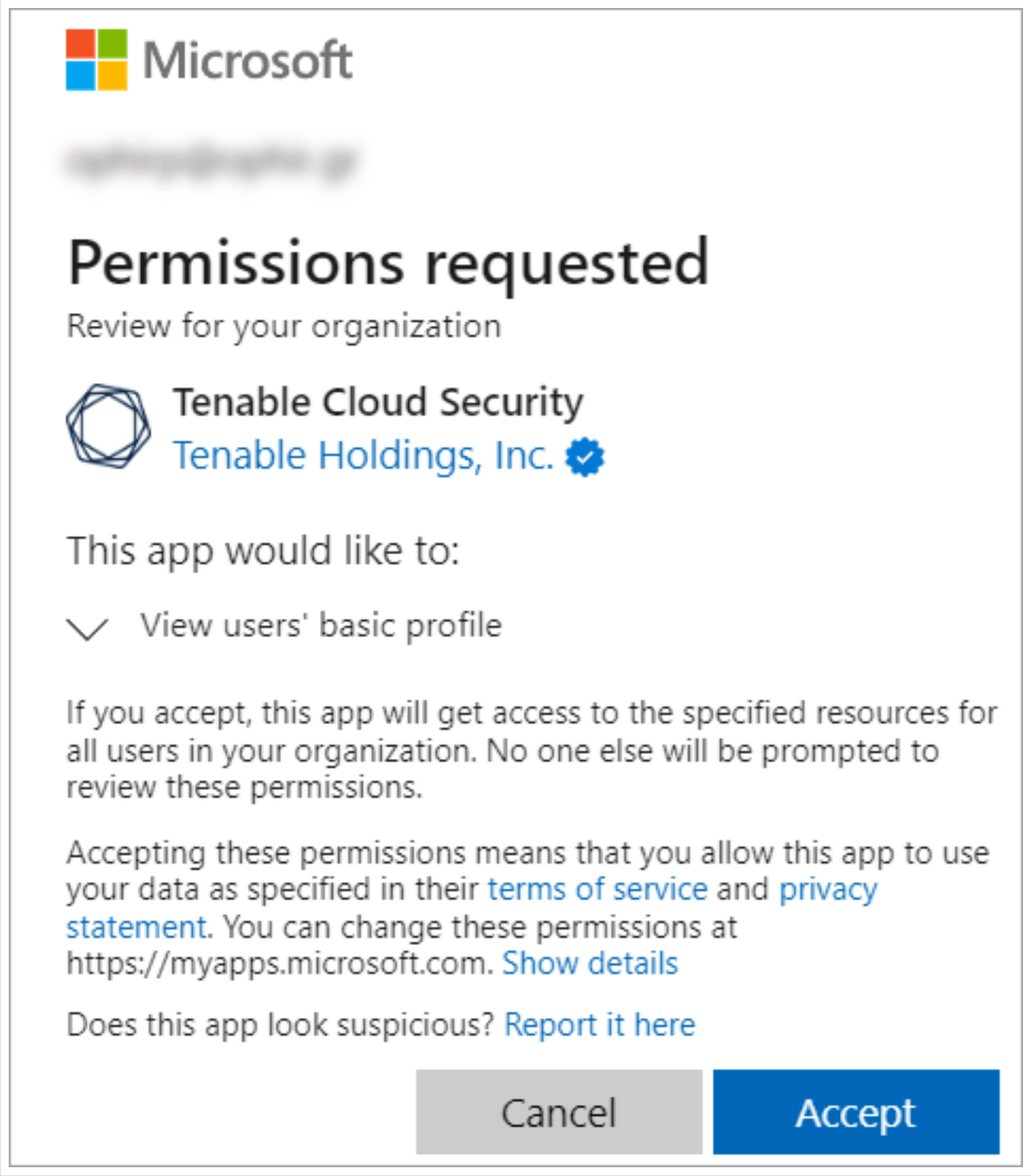
Enable login to the AI Exposure Console via Microsoft Entra ID using one of the following identity specifications:

- OpenID Connect (OIDC)
- SAML

Enable Login via Microsoft Entra ID Using OIDC

To enable login using OIDC:

1. In the AI Exposure Console, navigate to **Settings** > **Access Management** > **Single Sign-On**.
2. Click **Add Identity Provider** and then click **Microsoft**.
3. In the **Add Identity Provider** dialog, grant access by clicking the link for **AI Exposure**.
4. Pick an account associated with the AI Exposure administrator in your organization.
5. **Accept** the requested permissions.



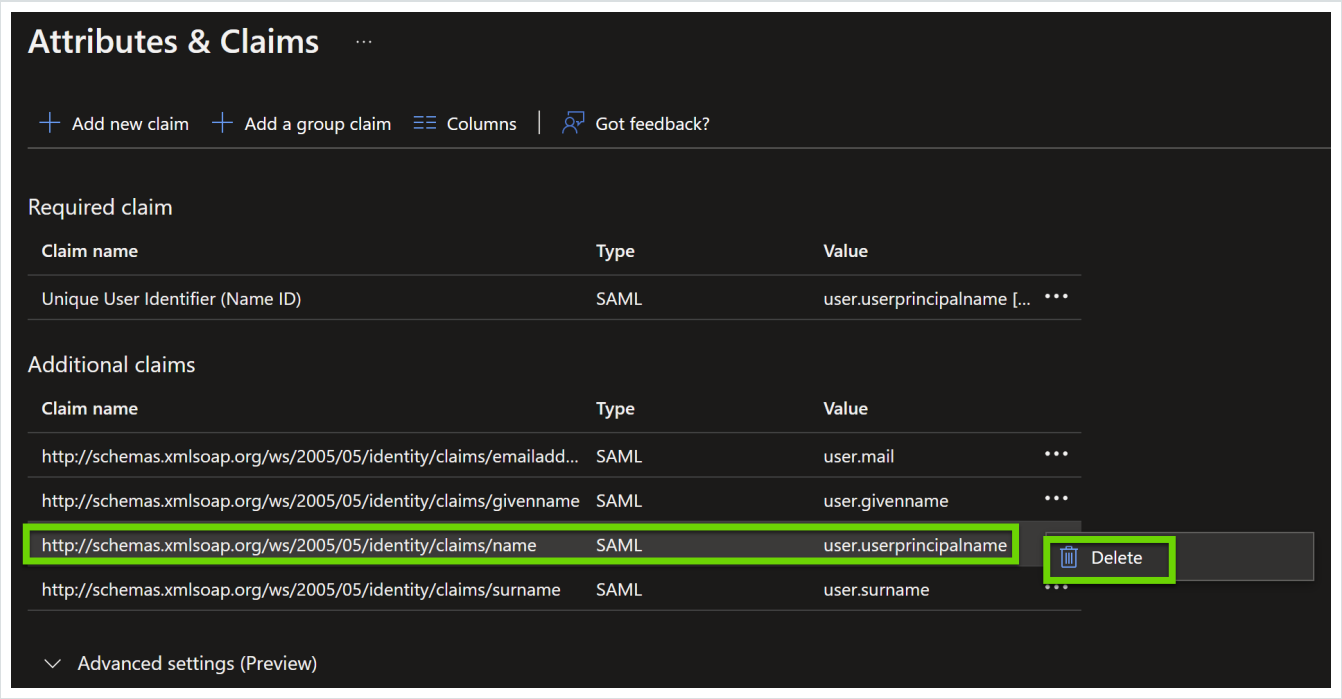
6. Verify that **I confirm that I granted access** is selected, and click **Add**.

Enable Login via Microsoft Entra ID Using SAML

To enable login using SAML:

1. In the Azure portal, navigate to **Enterprise applications**, and then add a **New application**.
2. Click **Create your own application**, and then enter a name for the app.
3. Select the default value of Integrate any other application you don't find in the gallery (Non-Gallery) and then click **Create**.
4. On the app Overview page that displays, in the *Set up single sign on* step, click **Get started**.
5. Choose **SAML** as the SSO method.
6. Under Basic SAML Configuration, click **Edit**, and enter the following values for the respective fields:
    - *Identifier (Entity ID)*: **urn:app.ermetic.com**
    - *Reply URL (Assertion Consumer Service URL)*: **https://{URL}/api/console/authentication/saml2/customer/acs**

      Where `{URL}` is:
        - **Global (All regions)**: `app.tenable.com`
        - **United States Gov Cloud**: `app.tenable.us`
7. Click **Save**.
8. Under Attributes & Claims, click **Edit**, and then, under Additional claims, delete the **user.userprincipalname** claim.



9. Under SAML Certificates, click to download the **Federation Metadata XML**.
10. In the AI Exposure Console, navigate to **Settings** > **Access Management** > **Single Sign-On**.
11. Click **Add Identity Provider** and then click **SAML**.
12. In the **Add Identity Provider** dialog, select **AI Exposure** from the dropdown.
13. Select **File**, upload the metadata that you downloaded from Azure, and then click **Add**.

Add Support for Microsoft Entra ID Groups

To add support for Microsoft Entra ID groups, perform the relevant procedure below, depending on the identity protocol that you use with Microsoft Entra ID:

- OIDC
- SAML

Doing so will send relevant group claims to AI Exposure, and allow you to then add those groups in Tenable, granting all users associated with the group identical permissions in Tenable.

Add Support for Microsoft Entra ID Groups Using OIDC

Note: This procedure only works for users who are directly assigned to a group, and not, for example, for a group nested within another group.

To add support for Microsoft Entra ID groups:

1. Verify that you have enabled Console login via Microsoft Entra ID.
2. In the Azure Portal, navigate to the **Enterprise applications** page, and then select the **AI Exposure** application.
3. Under Manage, click **Users and Groups**.
4. Click **Add User/Group**.
5. In the Add Assignment page, under Users and groups, click **None Selected**.
6. Select any relevant groups from the list of users and groups, and then click **Select**.
7. After you finish, add the group/s in the AI Exposure Console.

Add Support for Microsoft Entra ID Groups Using SAML

Use the following procedure to add support for groups (SAML) in AI Exposure, either by sending:

- *groups assigned to the AI Exposure SAML application*
- *all groups* (not assigned to the app)

Be aware of relevant limitations when choosing which option to use. For example, if you choose *all groups*, there is a limitation in the number of groups that can be sent this way. Alternatively, if you choose *groups assigned to the application*, you will need to manually assign groups to the application, and there is no support for nested groups. Refer to the relevant Microsoft documentation for more information.

To add support for Microsoft Entra ID groups:

1. Verify that you have enabled login via a custom SAML 2.0 provider.
2. In the Azure Portal, navigate to the **Enterprise applications** page, and then select the relevant SAML application that you created for AI Exposure when you enabled login.

3. (Optional) Choose specific groups that you want to use with AI Exposure:
    1. Under Manage, click **Users and Groups**.
    2. Click **Add User/Group**.
    3. In the Add Assignment page, under Users and groups, click **None Selected**.
    4. Select any relevant groups from the list of users and groups, and then click **Select**.
4. Navigate to the **Single sign-on** page for the SAML application.
5. In Attributes & Claims, click **Edit**.
6. Click **Add a group claim**.
7. Select which groups associated with the user should be returned in the claim. Select one of the following options:
    - **All groups** – Selecting this option will send all groups to Tenable.
    - **Groups assigned to the application** – Selecting this option will send any groups that you assigned to the Tenable SAML application earlier in this procedure to Tenable.
      Refer to the relevant Microsoft documentation for more information.
8. For the Source attribute, keep the default value of **Group ID**.
9. Open the **Advanced options**.
10. Select **Customize the name of the group claim**, and for the Name, enter **groups**.

    > **Important:** The Name field is case sensitive. The `groups` value must be entered exactly as is.

11. Click **Save**.
12. After you finish, add the group/s in the AI Exposure Console.

Enable Login via Okta

Enable login to the AI Exposure Console via Okta by leveraging the SAML 2.0 identity specification.

To enable login to the AI Exposure Console via Okta:

1. In the Okta Admin Console, navigate to **Applications > Applications**.
2. Click **Browse App Catalog**.

3. Enter **AI Exposure** in the Search field, click the application tile, and then click **Add Integration**.
4. In the **General Settings** tab, enter a **Console Domain**, where the value you enter depends on the value in the URL you use to log in to the AI Exposure Console:
    - `app.tenable.com`
    - `app.tenable.us`

    Note: If you don't enter a value, it will default to *app.tenable.com*.
5. In the SAML Setup section, click **View SAML setup instructions**.
6. Under Configuration Steps, copy the URL value listed in step 2.
7. In the AI Exposure Console, navigate to **Settings** > **Access Management** > **Single Sign-On**.
8. Click **Add Identity Provider** and then click **SAML**.
9. In the **Add Identity Provider** dialog, select **AI Exposure** from the dropdown.
10. Select **URL**, paste the URL value from Okta, and then click **Add**.

Add Support for Okta Groups

To add support for Okta groups:

1. In the Okta Admin Console, navigate to the **AI Exposure** application that you added in Enable Login via Okta
2. Navigate to the **Sign On** tab, click **Edit** next to Settings, and then under SAML 2.0, expand the **Attributes** section.
3. Under Group Attribute Statements, in the Name field, type **groups**, and then enter a relevant filter to define which groups will be sent to AI Exposure. For example, if you want to send all groups, you can select **Matches regex** with a value of `.*`.

    Important: The Name field is case sensitive. The `groups` value must be entered exactly as is.
4. Click **Save**.
5. After you finish, add the group/s in the AI Exposure Console.

Enable Login via OneLogin

Enable login to the AI Exposure Console via OneLogin by leveraging the SAML 2.0 identity specification.

To enable login to the AI Exposure Console via OneLogin:

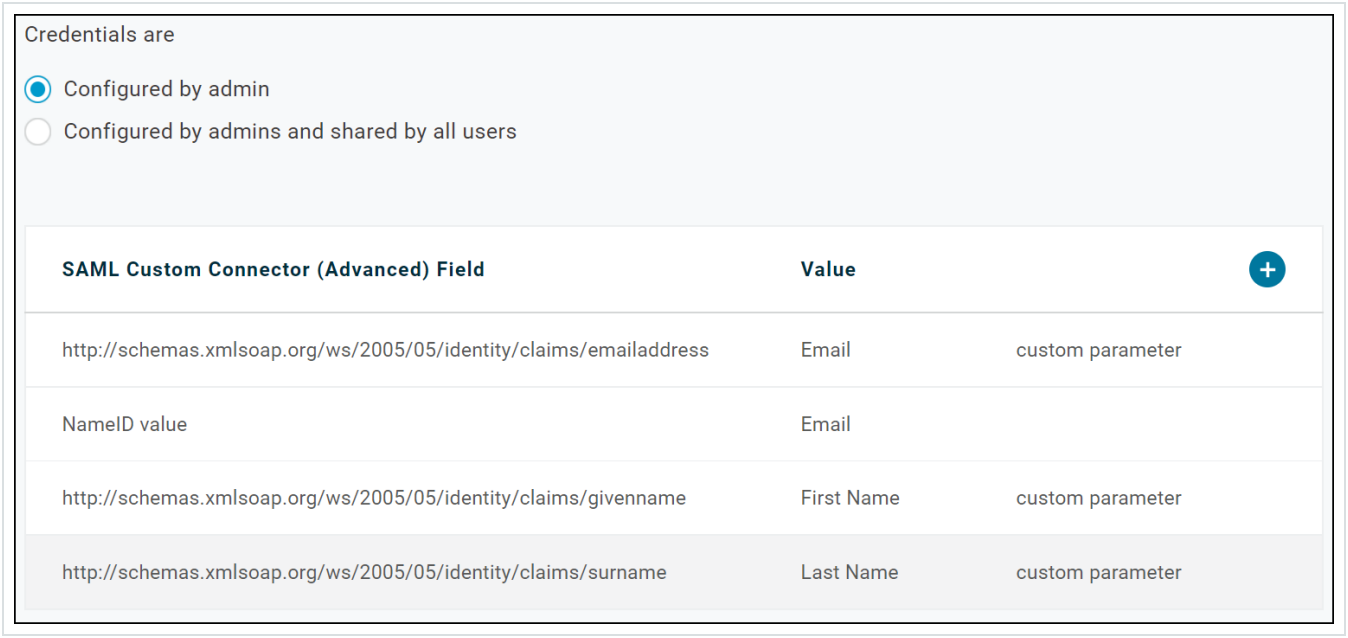
1. In the OneLogin Admin Console, navigate to **Applications > Applications**.
2. Click **Add App**.
3. Search for and select **SAML Custom Connector (Advanced)**.
4. In the Configuration page, enter a **Display Name** (For example, 'AI Exposure'). and then click **Save**.
5. Navigate to the **Configuration** tab, and enter the following values for these application details:
   - Audience (EntityID): **urn:app.ermetic.com**
   - ACS (Consumer) URL Validator / ACS (Consumer) URL: **https://{URL}/api/console/authentication/saml2/customer/acs**

     Where `{URL}` is:
     - **Global (All regions)**: `app.tenable.com`
     - **United States Gov Cloud**: `app.tenable.us`
6. Navigate to the **Parameters** tab, and click ⊕ to add the following new fields/values:

   Field name to Value:
   - **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress** – Email
   - **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname** – First Name
   - **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname** – Last Name

   Important: Make sure to enable the **Include in SAML assertion** flag for each field/value.

   Note: The *NameID value* field appears out-of-the-box in OneLogin. You can leave this field as is.



7. Navigate to the SSO tab and set the **SAML Signature Algorithm** to **SHA-256**.
8. Click on the More Actions dropdown and select **SAML Metadata**. Copy the metadata.
9. In the AI Exposure Console, navigate to **Settings** > **Access Management** > **Single Sign-On**.
10. Click **Add Identity Provider** and then click **SAML**.
11. In the **Add Identity Provider** dialog, select **AI Exposure** from the dropdown.
12. Select **File**, upload the metadata you copied from OneLogin, and then click **Add**.

Add Support for OneLogin Roles

In OneLogin, **roles** are used to assign users to one or more applications, and **groups** are used to assign a user security policy to users. OneLogin users can only belong to one OneLogin group at a time.

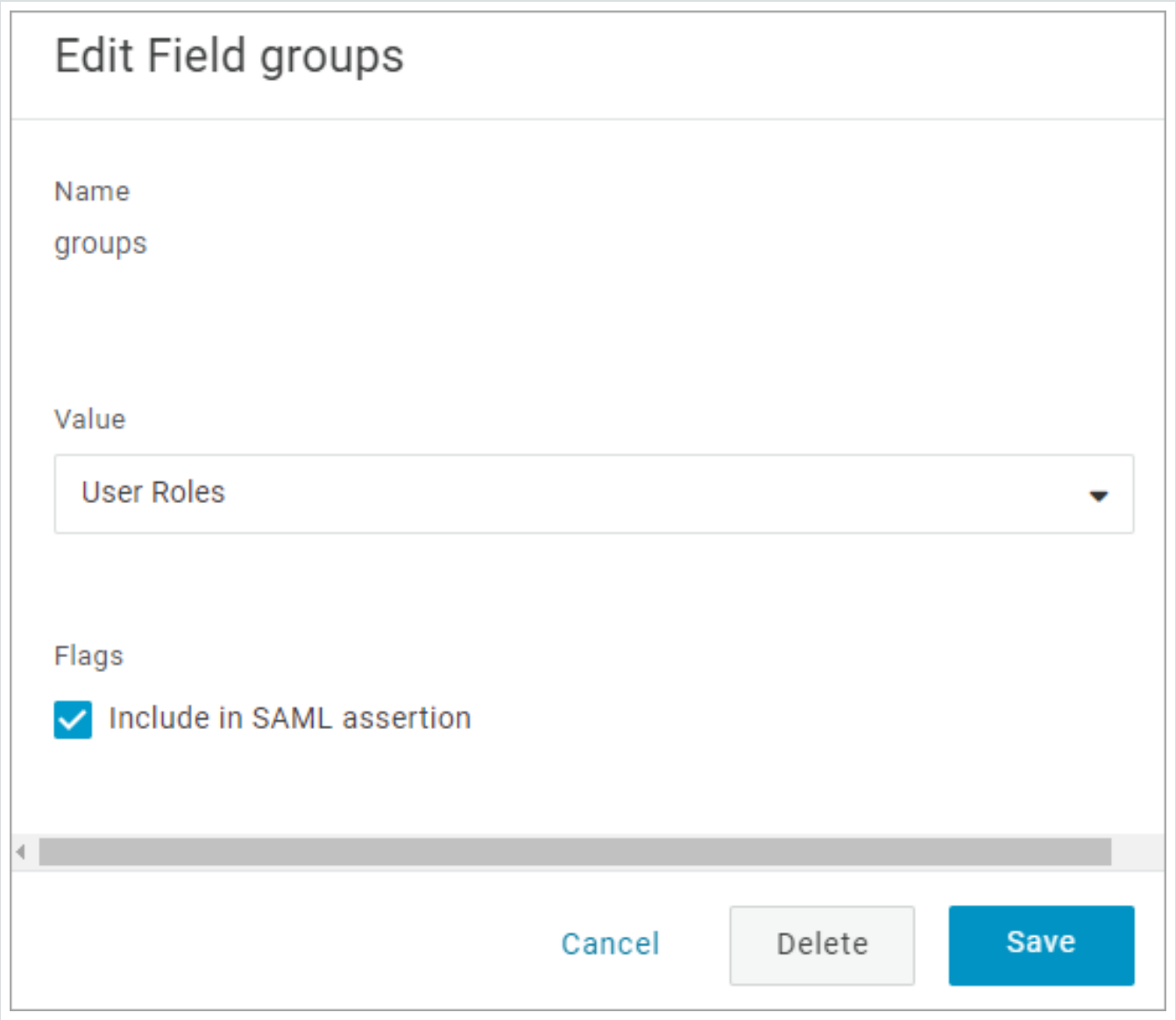
As a result of the fact that OneLogin groups function differently than in most other applications, to work with groups in AI Exposure, it is more likely that you would want to map OneLogin roles to AI Exposure groups, as opposed to OneLogin groups.

To add support for OneLogin roles:

1. In the OneLogin Admin Console, navigate to **Applications > Applications** and then open the AI Exposure SAML application that you added in Enable Login via OneLogin.
2. Navigate to the **Parameters** tab, and click ⊕ to add the following new field/value:
    - Field name: **groups**

      > **Important:** The Name field is case sensitive. The `groups` value must be entered exactly as is.

    - Value: **User Roles**
    - Flag: **Include in SAML assertion** enabled
3. Click **Save**.



4. After you finish, add the group/s in the AI Exposure Console.

Enable Login via Ping Identity

Enable login to the AI Exposure Console via Ping Identity by leveraging the SAML 2.0 identity specification.

To enable login to the AI Exposure Console via Ping Identity:

1. In the Ping Identity Admin Console, navigate to **Connections > Applications**.
2. Click ⊕ to add an application.

3. Enter an **Application Name**. For example, 'AI Exposure'.
4. Choose **SAML Application** as the Application Type and then click **Configure**.
5. Under SAML Configuration, choose **Manually Enter** and then enter the following details:
    - **ACS URL** – https://{URL}/api/console/authentication/saml2/customer/acs

      Where {URL} is:
        - **Global (All regions)**: app.tenable.com
        - **United States Gov Cloud**: app.tenable.us
    - **Entity ID** – urn:app.ermetic.com
6. Click **Save**.
7. Navigate to the Attribute Mappings tab, click Edit and then add the following attributes:

    Attributes to PingOne Mappings:

    - **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress** – Email Address
    - **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname** – Given Name
    - **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname** – Family Name
8. Click the radio button to enable the App.



9. Navigate to the Configuration tab and click **Download Metadata**.
10. In the AI Exposure Console, navigate to **Settings** > **Access Management** > **Single Sign-On**.
11. Click **Add Identity Provider** and then click **SAML**.
12. In the **Add Identity Provider** dialog, select **AI Exposure** from the dropdown.
13. Select **File**, upload the metadata you copied from OneLogin, and then click **Add**.

Add Support for Ping Identity Groups

To add support for Ping Identity groups:

1. In the Ping Identity Admin Console, navigate to **Connections > Applications** and then open the AI Exposure SAML application that you added in Enable Login via Ping Identity.
2. Navigate to the Attribute Mappings tab, click Edit and then add the following attribute:
    - Attribute: **groups**
    - PingOne Mapping: **Group Names**

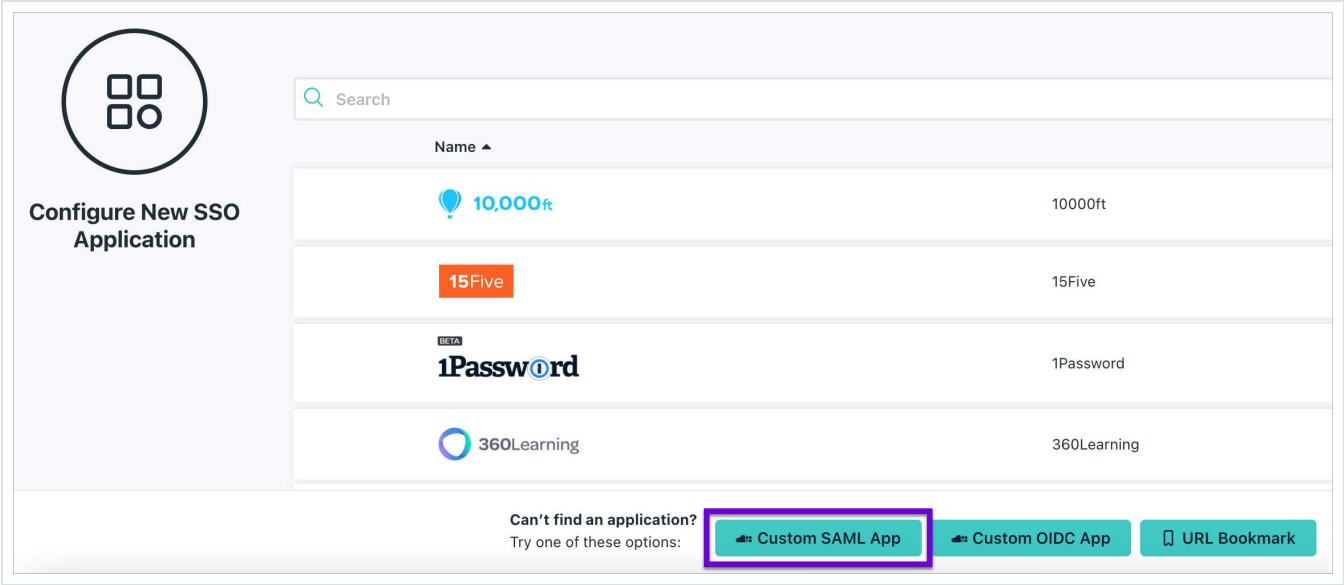
    > **Important:** The Attribute field is case sensitive. The `groups` value must be entered exactly as is.
3. Click **Save**.
4. After you finish, add the group/s in the AI Exposure Console.

Enable Login via JumpCloud

Enable login to the AI Exposure Console via JumpCloud by leveraging the SAML 2.0 identity specification.

To enable login to the AI Exposure Console via JumpCloud:

1. In the JumpCloud Admin Portal, navigate to **User Groups** (under USER MANAGEMENT), create a new group for the AI Exposure SSO Application, and then add any relevant users.
2. Navigate to **SSO** and click **Add New Application**.
3. Search for, and select **Custom SAML App**.



4. In the General Info tab, enter a **Display Label** (For example, *Tenable_SSO*).
5. Navigate to the **SSO** tab, and enter the following values for each field:

Field	Value
IdP Entity ID*	urn:{your-domain.com} Where `your-domain.com` is the primary domain name of your company. For example, urn:ermetic.com.
SP Entity ID*	urn:app.ermetic.com
ACS URL*	**https://{URL}/api/console/authentication/saml2/customer/acs** Where `{URL}` is: • **Global (All regions)**: `app.tenable.com` • **United States Gov Cloud**: `app.tenable.us`
SAMLSubject NameID*	email
SAMLSubject	urn:oasis:names:tc:SAML:1.0:nameid-format:unspecified (Default)

Field	Value
NameID Format*	
Signature Algorithm	RSA-SHA256
Sign Assertion	Enabled/Selected

6. Under **Attributes > USER ATTRIBUTES MAPPING**, click **add attribute** and add each of the following mappings:

Service Provider Attribute Name	JumpCloud Attribute Name
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	email
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	firstname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	lastname

7. Navigate to the **User Groups** tab, add the group you created earlier, and then click **Activate**.
8. Click on the new app you created, navigate to **SSO**, and then click **Export Metadata**.
9. In the AI Exposure Console, navigate to **Settings** > **Access Management** > **Single Sign-On**.
10. Click **Add Identity Provider** and then click **SAML**.
11. In the **Add Identity Provider** dialog, select **AI Exposure** from the dropdown.
12. Select **File**, upload the metadata you copied from JumpCloud, and then click **Add**.

Add Support for JumpCloud Groups

To add support for JumpCloud groups:

1. In the JumpCloud Admin Console, navigate to **SSO** and open the AI Exposure SAML application that you added in Enable Login via JumpCloud.
2. Navigate to the **SSO** tab, and under GROUP ATTRIBUTES, select **include group attribute**, and then type **groups**.

   > **Important:** The Attribute field is case sensitive. The `groups` value must be entered exactly as is.

3. Click **Save**.

Enable Login via Custom SAML 2.0 Provider

If you work with a provider other than one of those documented in the sections above, you can enable login to the AI Exposure Console via that provider by leveraging the SAML 2.0 identity specification.

> **Note:** Each provider may use slightly different names/terminology to refer to the details/parameters/attributes listed below. Verify that you configure the values below for the correct parameter.

To enable login to the AI Exposure Console via a custom SAML provider:

1. Follow the steps outlined by the relevant provider to add a dedicated application for AI Exposure. Consult with any relevant documentation, if needed.
2. In the application, configure the following SAML details:

SAML Parameters	Value
Entity ID	**urn:app.ermetic.com**
ACS (Redirect URL)	**https://{URL}/api/console/authentication/saml2/customer/acs** Where `{URL}` is: • **Global (All regions)**: `app.tenable.com`

SAML Parameters	Value
	• **United States Gov Cloud**: `app.tenable.us`
Encryption	**SHA-256**
SAML NameID Format	**Email**

3. Add the following SAML attributes, mapping them, as relevant, to the given provider:

Attributes	Mappings	Name Format
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	Email Address	Unspecified
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	Given Name	Unspecified
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Family Name	Unspecified

4. Download the metadata.
5. In the AI Exposure Console, navigate to **Settings** > **Access Management** > **Single Sign-On**.
6. Click **Add Identity Provider** and then click **SAML**.
7. In the **Add Identity Provider** dialog, select **AI Exposure** from the dropdown.
8. Select **File**, upload the metadata that you downloaded earlier, and then click **Add**.

Add Support for Groups

To add support for groups using a custom SAML 2.0 provider:

Map the native IdP group attribute to the AI Exposure **groups** attribute.

Important: The **groups** attribute is case sensitive. The value must be entered exactly as is.

Console Timeout Settings

To enhance account security and reduce the risk of unauthorized access, administrators can configure two types of timeouts for the web Console:

- Inactivity Timeout – Ends a session after a period of user inactivity.
- Session Timeout – Ends a session after a fixed duration, regardless of user activity.

These settings can be adjusted based on your organization's security and compliance needs.

Inactivity Timeout

The inactivity timeout automatically signs out users after a period of no interaction with the console. The default value is **12 hours**.

Note: Any configuration changes to the timeout period take effect the next time each user logs in.

To configure the inactivity timeout:

1. In the Tenable One AI Exposure Console, navigate to **Settings** > **Access Management** > **Single Sign-On**.
2. In the **Inactivity Timeout** section, enter a number, in minutes and click **Save**.

Session Timeout

The session timeout defines the maximum duration a user session remains valid from the moment of login, regardless of activity. Once the session duration expires, the user is logged out and must sign in again. *This setting is disabled by default.*

Note: Any configuration changes to the timeout period take effect the next time each user logs in.

To configure the session timeout:

1. In the AI Exposure Console, navigate to **Settings** > **Access Management** > **Single Sign-On**.
2. In the **Session Timeout** section, click the radio button to enable the session timeout.
3. Enter a number, in minutes and click **Save**.

Roles

Custom roles let you define precisely which areas of the Tenable One AI Exposure Console a user or group can access. You create a role by selecting individual permissions from a list of Console modules, then assign it to users or groups in User Management.

Use custom roles when the built-in roles (Viewer, Collaborator, Administrator) grant more or less access than a user needs. For example, you can create a read-only compliance role without granting the broader access that *Collaborator* includes. For information about built-in roles and the permissions they include, see Built-in Roles and Permissions.

Common Use Cases

The following table shows typical custom roles and the minimum permissions required to support them.

Use Case	Who It Is For	Minimum Permissions
Audit Viewer	Compliance officers or external auditors who need to review Console activity without access to other product areas.	**Audit** – **View**
AI Conversations Viewer	Users who need visibility into the complete conversation history. Without this role, users can only view evidence snippets in **AI Activity Detections**.	**AI Conversations** – **View**
Reports Viewer	Executive stakeholders or compliance reviewers who need to generate and download reports without broader Console	**Reports** – **View**

Use Case	Who It Is For	Minimum Permissions
	access.	
Compliance Viewer	Users who monitor compliance benchmark status and scores without the ability to create or modify compliance rules.	**Compliance – View**
Read-Only Findings Reviewer	Stakeholders who need visibility into risk findings, threats, and vulnerabilities without the ability to respond to or modify them.	• **Risks – View** • **Threats – View** • **Vulnerabilities – View**
JIT Visibility	Users who need to view JIT eligibility configurations and audit events via the Console without managing eligibilities or holding the JIT Administrator role.	• **JIT - Eligibility – View** • **JIT - Audit – View**
Automation Manager	DevSecOps team members or integration owners who need to create and manage automation rules without full Administrator access.	• **Automation – View** • **Automation – Manage**

Create a Custom Role

To create a custom role:

1. In the AI Exposure, navigate to **Settings** > **Access Management** > **Roles**.
2. Click **+ Create Role**.
3. In the **Name** box, type a name for the role.
4. In the **Permissions** section, select the checkboxes for the modules you want to include.

To view sub-permissions for a module, click the expand arrow. For example, **Inventory** includes separate **View** and **Manage** sub-permissions.

Some permissions are automatically selected and marked **Required** because they support other selected permissions. Hover over the **Required** badge to see which selected permissions depend on it.

5. Click **Create**.

Edit a Custom Role

Edit a custom role to change the name or permission mapping of the role.

To edit a custom role:

1. In the AI Exposure Console, navigate to **Settings** > **Access Management** > **Roles**.
2. In the roles list, click the options menu next to the role you want to edit.
3. Click **Edit**.
4. Update the role name or permissions as needed.
5. Click **Save**.

Duplicate a Role

Duplicate a built-in or custom role to create a new role based on existing permission mappings.

1. In the AI Exposure Console, navigate to **Settings** > **Access Management** > **Roles**.
2. In the roles list, click the options menu next to the role you want to edit.
3. Click **Duplicate**.
4. Update the role name or permissions as needed.
5. Click **Create**.

Delete a Custom Role

Deleting a custom role will immediately revoke permissions from any users who have been granted it.

To delete a custom role:

1. In the AI Exposure Console, navigate to **Settings** > **Access Management** > **Roles**.
2. In the roles list, click the options menu next to the role you want to delete.
3. Click **Delete**.
4. In the confirmation window, click **Delete**.

Available Permissions

The following table lists the permissions available when creating or editing a custom role. Each top-level permission maps to a module in the Console. Where a permission includes sub-permissions, selecting the parent does not automatically select its children. You must select each sub-permission individually.

Permission	What It Controls
Dashboards	• **View** – See dashboards and widget data. • **Manage** – Create, edit, and delete dashboards. Includes separate sub-permissions for **Private Dashboards** and **Public Dashboards**.
Inventory	• **View** – See cloud resources, IAM principals, access graph, network graph, and entity details. • **Manage** – Add labels to resources, mark resources as sensitive, and set custom property values.
Workload Resources	• **Scan Now** – Request an on-demand scan for a workload resource.
Data Resources	• **Scan** – Request an on-demand scan for a data resource.
Events	• **View** – See cloud events and Kubernetes admission controller events.

Permission	What It Controls
AI Conversations	• **View** – See the content of AI conversations.
CI/CD Scans	• **View** – See security scan results for container images, code pipelines, and pull requests.
Queries	• **View** – See and run saved queries. • **Manage** – Create, edit, and delete queries. Includes separate sub-permissions for **Private Queries** and **Public Queries**.

Findings	• **View** – See AI posture findings.
	• **Manage** – Includes the following sub-permissions:
	  • **Comment** (add and delete comments on findings)
	  • **Status** – Update the finding state to Open or Closed (To ignore findings, use the Exclusions > Manage permission)
	  • **Star** (star findings)
	  • **Remediation** – Trigger automated cloud remediation.
	  • **Share** (create Jira issues and ServiceNow incidents from findings).

AI Activity Risks	• **View** – See activity detections and activity issues.
	• **Manage** – Includes the following sub-permissions:
	  • **Comment** (add and delete comments)
	  • **Share** (create Jira issues and ServiceNow incidents from threats)
	  • **Star** (star threats)
	  • **Status** (change threat status)

Threat Detections	• **View** – See threat detection findings.

Permission	What It Controls
	• **Manage** – Includes the following sub-permissions: **Comment** (add and delete comments); **Status** (change threat status); **Share** (create Jira issues and ServiceNow incidents from threats); **Star** (star threats).
Vulnerabilities	• **View** – See vulnerability findings, packages, and CVE details.
Malicious Files	• **View** – See malicious file detections.
Policies	• **View** – See built-in and custom risk policies. • **Manage** – Create and delete custom risk policies. Enable and disable built-in policies.
Exclusions	Applies to risk/finding exclusions only. Data/workload exclusions are managed through the **Settings** permission. • **View** – See risk exclusions. • **Manage** – Create, update, and delete risk exclusions, and manually ignore individual findings.
Automation	• **View** – See automation rules. • **Manage** – Create, update, and delete automation rules.
Reports	• **View** – See, generate, and download reports. • **Manage** – Schedule and delete reports.
Compliance	• **View** – See compliance benchmarks and scores. • **Manage** – Create and delete custom compliance rules; enable and disable built-in compliance benchmarks.
Settings	*Covers the Access Management, Inventory, Security, and Licensing pages in Settings, including all child pages.*

Permission	What It Controls
	• **View** – See user and role assignments and licensing data. • **Manage** – Add, edit, and delete user and group role assignments, and create or update custom roles.
Settings - Organization	• **View** – See projects and the account and folder hierarchy. • **Manage** – Create, update, and delete projects, and organize the account and folder hierarchy.
Settings - Integrations	• **View** – See configured integrations. • **Manage** – Create, update, and delete integrations. Includes connecting Kubernetes clusters, which is accessible via **Explore** > **Inventory** > **Kubernetes Clusters** but is controlled by this permission, not the Inventory permission.
Settings - Audit	• **View** – See the Console audit event log.
JIT - Eligibility	• **View** – See JIT eligibility configurations. • **Manage** – Create, update, and delete JIT eligibilities.
JIT - Audit	• **View** – See JIT access request audit events.

Permission Dependencies

Some permissions are automatically required when you select others. Selecting **Dashboards**, for example, automatically requires **Inventory** (View), **Queries**, **Risks**, and **Vulnerabilities**. Hover over the **Required** badge on any auto-selected permission to see which permissions depend on it.

Organization

Projects

Projects simplify the management of accounts and resources by logically grouping them, allowing you to align Console data with your organizational structure.

This is a how-to guide for configuring projects. For a conceptual overview, see How Projects Work.

Who Can Create a Project?

To create or edit a project, a user must have the *Administrator* role on both:

- The **project or folder scope** where the project is being created or modified.
- The **account scope** for each account included in the project.

This means:

- Admin users assigned the *Organization* scope can create or edit projects in any scope.
- Admin users assigned to the root *Project* folder scope can manage any project or folder within that root.
- Admin users assigned to a specific project folder scope can manage any project or subfolder within that folder.
- Admin users assigned to a specific project *cannot create new projects*. They can only edit the project they've been assigned to.

Example: Delegating Project Ownership

Suppose you're the Organization-level admin for your environment and want to delegate project ownership to another team member. You can:

1. Add a Project Folder. For example, `Development`.
2. Add a user role assignment granting the user the *Administrator* role on the new `Development` folder.

   > **Note:** Verify that this user also has the *Administrator* for any accounts that should be included in the project.

3. That user can now create and manage projects or subfolders within `Development`.

Supported Features

Many Tenable One AI Exposure features support projects, allowing you to perform actions within a specific project scope. Only users assigned a matching project scope can view/manage these features.

For example, you can perform the following for a project scope:

- Grant AI Exposure users access
- Create integrations and automations
- Create reports
- Create a custom compliance
- Create API tokens and query the AI Exposure API
- View licensing data
- Create custom policies

So, for example, only a user assigned to *Project A* can create an API token for that scope.

Add a Project Folder

> **Required AI Exposure User Role:** Administrator. For more information, see Who Can Create a Project? and Roles and Permissions.

Add a project folder to organize one or more projects logically. Console users granted access to a project folder will have access to all of its child projects. For example, you may want to create projects for each product group in your organization, and group them together in folders by region. You can then grant relevant users access to either a specific project, or to the entire project folder.

1. In the AI Exposure Console, navigate to **Settings** > **Accounts** > **Projects**.

   Any existing folders/projects appear in the tree on the left-hand side of the page.
2. Navigate to the location where you want to add the folder.
3. Click **Add** > **Add folder**.
4. Enter a **Folder name** and then click **Add**.

Add a Project

Before you add a project, ensure that you onboard any accounts containing the cloud resources that you want in the project. After adding a project, you can only use it after the next data synchronization in your environment.

> **Required AI Exposure User Role:** Administrator. For more information, see Who Can Create a Project? and Roles and Permissions.

1. In the AI Exposure Console, navigate to **Settings** > **Accounts** > **Projects**.

   Any existing projects appear in the tree on the left-hand side of the page.
2. Navigate to the location where you want to add the project.
3. Click **Add** > **Add project**.
4. In the **Add Project** dialog, enter project details:
   1. Enter a unique and meaningful **Name** to display in AI Exposure.
   2. (Optional) Enter a **Description**.
5. **Scopes**. *Define one or more scope groups. Users assigned to the project will be able to access resources in these scopes.*
   1. Select **Accounts** that you want to include in the project. An account scope can be, for example, an onboarded *cloud account*, *IdP tenant*, or *code repository*.

      > **Note:** When you select a folder (or the entire organization), the project will contain all existing and future accounts in that folder.

   2. Define one or more **Condition** to narrow the scope of the project:
      - **Account name pattern** – Enter a name pattern, based on text patterns found in cloud account names. Accounts with patterns in their names that match the pattern you define are included in the project. For example, entering `dev*` will cause an account named `development` to match.
      - **Account tag pattern** – Enter a tag key-value pair, based on text patterns found in account tag keys or patterns. Accounts tagged with key-value pairs that match the

pattern you define are included in the project. For example, entering a key of `type` and a value of `prod` will cause accounts with that key-value pair to match.

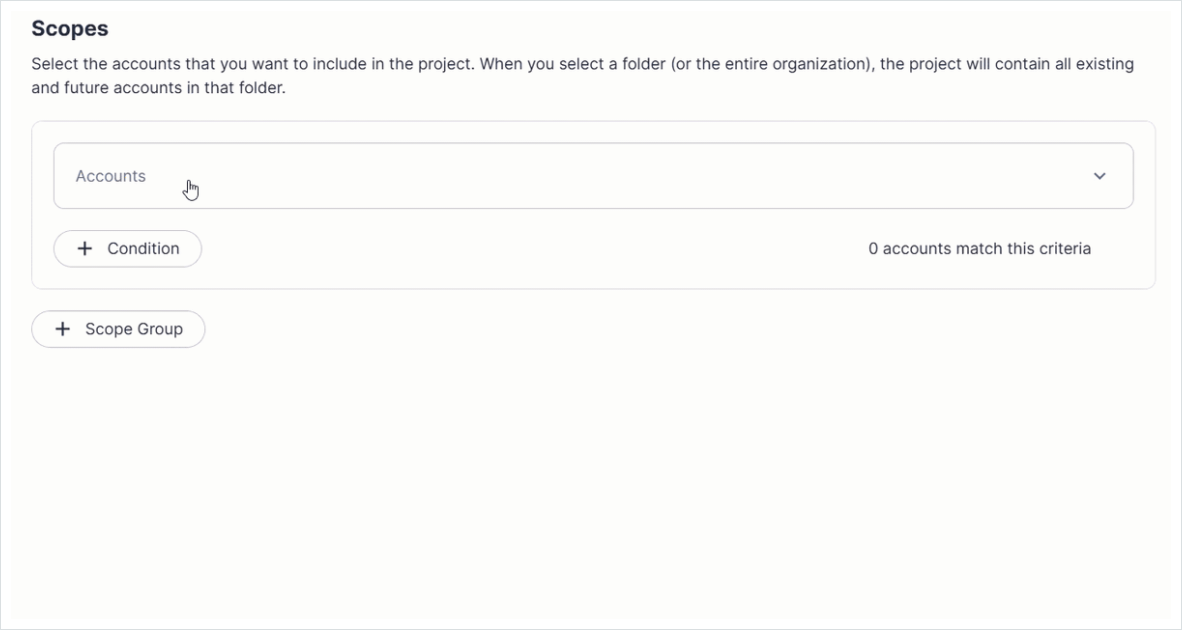
- **Resource tag pattern** – Enter a tag key-value pair, based on text patterns found in resource tag keys or patterns. Resources tagged with key-value pairs that match the pattern you define are included in the project. For example, entering a key of `business_unit` and a value of `finance` will cause resources with that key-value pair to match.
- **Azure resource group name pattern** – Enter a name pattern, based on text patterns found in resource group names. Resource groups with patterns in their names that match the pattern you define are included in the project. For example, entering `cust-facing-apps-*` will cause a resource group named `cust-facing-apps-europe-prod` to match.
- **Azure resource group tag pattern** – Enter a tag key-value pair, based on text patterns found in Azure resource group tag keys or patterns. Resource groups tagged with key-value pairs that match the pattern you define are included in the project. For example, entering a key of `environment` and a value of `production` will cause resource groups with that key-value pair to match.

  > **Important:** When you define a resource-based condition for a project, the system not only includes resources that directly match the condition but also related resources. These are additional resources that have a meaningful relationship to the matched resources, ensuring broader visibility into relevant dependencies. For example, if a key vault matches the defined condition, its associated secrets may also be included as related resources. This allows you to see a more complete picture when filtering the Console by a project.

- See Common Project Use Cases to see examples of common ways to use conditions when creating projects.
- Use `*` to indicate zero or more characters, or `?` to indicate a single character.
- Use either the `is` or `is not` operator, as required. For key/value pairs, you can use different operators for each. For example, where a resource tag **key** pattern `is`:

`environment`, and **value** pattern `is not: test`. This would include only production resources that are not for testing.

- If you select multiple conditions, you can use either **AND** (default) or **OR** operator logic.
- As you enter a condition/s, you can see how many accounts match the criteria that you are entering.



3. Click **Scope Group** to add another logical group of accounts to the project.

> **Note:** If you add multiple scope groups, the operator logic used is **OR**.

6. Decide whether to **extend user access to scopes in project**. This determines whether users assigned to this project are also automatically assigned to accounts within the project.

> **Note:** This applies only to accounts not filtered by resource-based conditions defined in this project.

- **Do not enable automatic assignment**
- **Automatically assign to eligible scopes**

7. When finished, click **Add**.

After adding a project, it will be available for use after the next data synchronization in your environment.

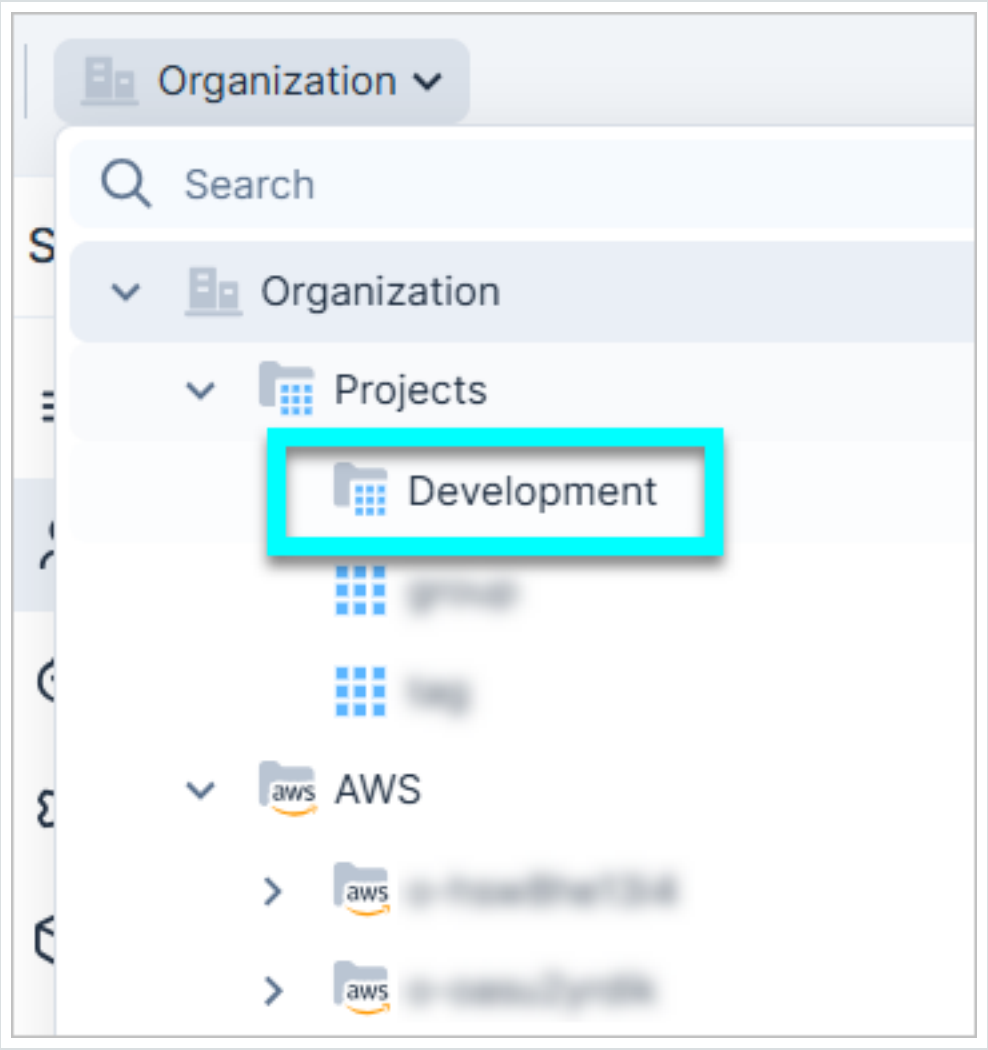
Grant Access to a Project Scope

To allow a system user to manage or view a specific project or project folder, you must assign them a role (such as Administrator or Viewer) at the relevant project scope.

> **Note:** In addition to directly assigning a user to a project scope, you can also decide to automatically extend (propagate) user assignments from a project to its contained accounts, reducing manual configuration and ensuring consistent access. See Add a Project for more information.

For example, to delegate access to a `Development` project:

1. Navigate to **Settings** > **Access Management** > **User Management** and add a role assignment.
2. Select the `Development` project as the scope.



3. Select the appropriate role.

For more details, see Users and Groups.

Move a Project

> **Required Tenable One AI Exposure User Role:** Administrator. For more information, see Users and Groups.

You can move:

- A *project* or *project folder* to an existing *folder*
- A *project* or *project folder* to the root *Projects folder*

1. In the AI Exposure Console, navigate to **Settings** > **Accounts** > **Projects**.

   Any existing projects appear in the tree on the left-hand side of the page.
2. Select the project/s or project folder/s that you want to move.
3. At the bottom of the page, click **Move**.
4. Select the destination folder location, or select **Projects** to move to the root folder.

Delete a Project

> **Required Tenable One AI Exposure User Role:** Administrator. For more information, see Users and Groups.

To delete folders that contain child projects/folders, first delete or move the child projects/folders.

To delete a project:

1. In the AI Exposure Console, navigate to **Settings** > **Accounts** > **Projects**.
2. Select the project/s or project folder/s that you want to delete.
3. At the bottom of the page, click **Delete**.

Filter Console Data by Projects

Data throughout the Console is filtered by scope, via a dropdown visible on every Console page. A user who was assigned a role for a specific, single project scope, will automatically see the AI Exposure Console filtered by that scope. Users assigned more than one project scope can view and configure specific features in the AI Exposure Console within a specific project scope.

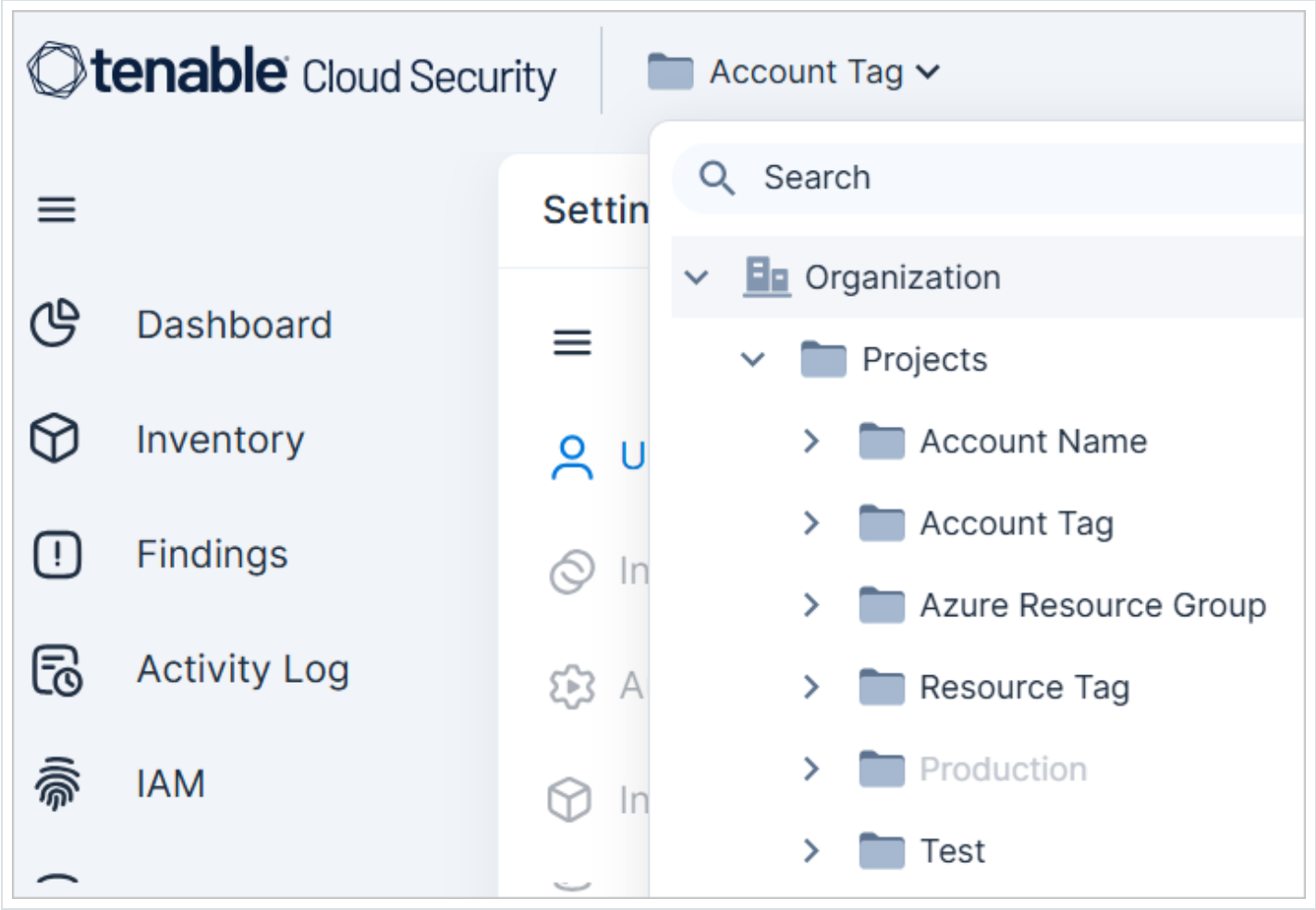
You can use projects/project folders to:

- Filter data throughout the AI Exposure Console.
- View and configure specific features in the AI Exposure Console.

> **Note:** The project scope you select will persist as you navigate across Console pages. It will remain set to your chosen scope, and won't revert to a default unless you manually change it.

To filter data by projects:

- On the relevant Console page, click on the scope dropdown and select a project or project folder as a scope.



View Projects

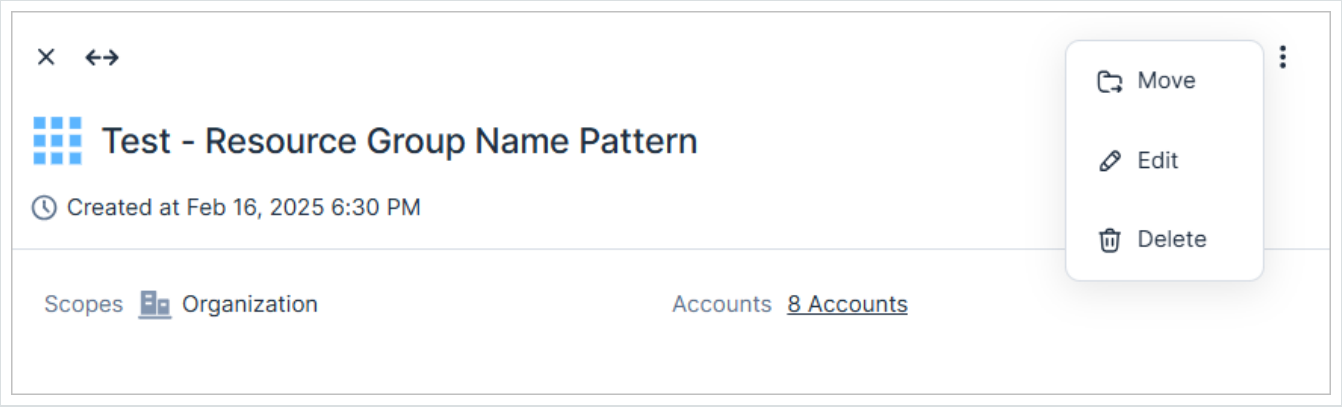
By default, the Projects page displays projects and project folders in the root folder.

To view projects:

1. In the AI Exposure Console, navigate to **Settings** > **Accounts** > **Projects**.
2. Do one of the following:

- Click **Flat View** to see projects created in all children folders. Use the **Path** column to identify the location of each project.
- Click a specific project folder to see projects (and subfolders) created in that folder.

3. Click on a specific project to see project details. For example, you can:
   - See when the project was created.
   - See which scopes and accounts are in the project.
   - Move the project.
   - Edit the project.
   - Delete the project.



Export Project Data

Export project data in CSV format. The data is exported according to the current filters applied to the table.

1. In the AI Exposure Console, navigate to **Settings** > **Accounts** > **Projects**.
2. Apply any relevant filters. Click **Flat View** to see projects created in all children folders.
3. Click **Export**.

Accounts

This is a how-to guide for managing accounts after you connect them to Tenable.

- For how-to guides on how to connect accounts, see Integrations for a list of supported providers.
- For a conceptual overview of account hierarchy, see Account Hierarchy and Folders.

The **Accounts** page is the central hub for managing all third-party accounts that Tenable One AI Exposure monitors. Centralizing these accounts allows you to monitor the health and connectivity of your entire scannable infrastructure in a single unified view.

- Cloud providers
- Identity providers
- Data platforms
- On-premises
- Container registries
- Code repositories

Manage Your Accounts

After you successfully connect an account to AI Exposure via onboarding, the account appears in the **Accounts** table (Settings > Organization > Accounts).

From the Accounts table, you can:

- View account details
- Monitor connectivity
- Troubleshoot issues
- Create projects and folder structures

The unified table displays all integrated accounts regardless of provider type. Use the navigation tree on the left to filter the table by specific categories.

Accounts Column Data

The unified **Accounts** table displays all integrated accounts regardless of provider type. Use the navigation tree on the left to filter the table by specific categories.

Column	Description
Name	The account or repository name with its associated provider icon.
ID	The unique identifier for the account.
Scope	The parent folder or organizational level where the account resides.
Status	The standardized connection health status. See Troubleshoot Onboarding Issues.
Issues	Displays specific errors, such as missing permissions or connectivity failures.

Manage Code Accounts

After you connect your repository, it appears in the table on the **Accounts** page (**Settings** > **Organization** > **Accounts**).

- If you used a code repository integration to connect your repository, the repository is added as a folder on this page.
- If you used a CI/CD integration to connect your pipeline, Tenable attempts to identify information about the associated provider and organization:
    - If successful, the repository is added as a folder on this page. If it was already added via code repository integration, the existing folder will remain, and wont be added again.
    - If no information is available, the repository is added to the *Other* folder.

If your organization has a large number of repositories, it's important to maintain a structured hierarchy within AI Exposure, using folders. You can create this structure in the following ways:

- (Recommended) Automatically Update Folder Structure in AI Exposure based on the repository structure of the onboarded organization.

- Manually create folders in Tenable to group your onboarded repositories together logically. For example, you may want to group your repositories by location.

  > **Important: Repositories**: To add or move repository folders, you need to disable the *Automatically update folder structure* option for the relevant source and destination organization. See Connect Your Repository for more information about this option. **CI/CD pipelines**: You can freely add or move pipeline folders.

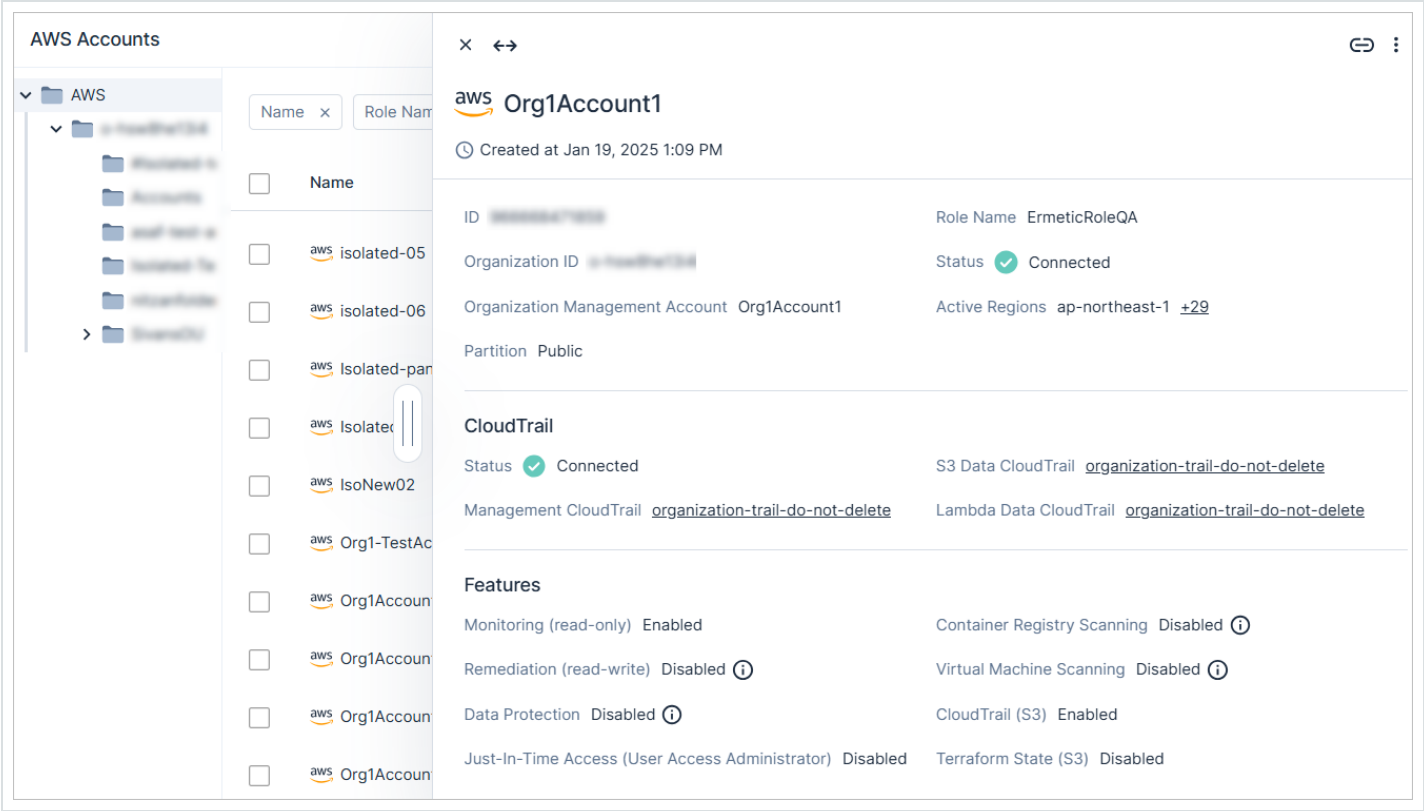
View Account Details

From the **Accounts** page, click on an account to see a detailed slideout panel. This panel lets you easily access all relevant account insights in one place for improved visibility and management.

The panel includes details such as:

- Account information.
- Information about the associated parent organization.
- For Cloud providers only:
  - **CloudTrail** (AWS). The connectivity status of the trail, and a list of Management/S3 Data/Lambda Data trails. See AWS Required Permissions for more information.
  - **Features** – The status of relevant platform features. For each feature, you can see:
    - Whether it was enabled/disabled.
    - Tooltips indicating whether the required permissions were actually granted.

    For example:
    - You may have *enabled* the feature, but the required permissions *weren't actually granted*, meaning that the feature isn't active.
    - Conversely, you may have *disabled* the feature, but the required permissions *are still granted*, meaning that you may want to consider removing permissions if the feature is not needed.



Account Management Options

The following global actions are available in the **Accounts** table toolbar:

Option	Description
Create Folder	Add a new folder to organize accounts logically. See Account Hierarchy and Folders for more information.
Add Account	Add a new integration to AI Exposure.
Create Project	Select one or more accounts and click this to initiate a new project scope.
Flat View	By default, the table displays items defined in the selected scope and parent scopes. Click **Flat View** to also see any items defined in children scopes.

Option	Description
Move	Move an account to a different location within the AI Exposure folder hierarchy. If the target folder does not have the same configured integrations as the source folder, you wont be able to move the account.
Delete	Delete either a folder or account from AI Exposure. It may take up to an hour to delete an account. For cloud providers, you may need to delete an account as part of offboarding.

Troubleshoot Onboarding Issues

AI Exposure provides monitoring and status indicators within the Console to help you troubleshoot issues that may arise during the account onboarding process. The status displayed for your accounts can offer immediate insights into potential problems.

After attempting to onboard an account, you can typically view its status on the **Accounts** page within the Console. This status indicates whether Tenable has successfully connected to the account and can help identify areas needing attention.

Account Status

Status	Description
Connected	The integration is in a healthy state and communicating as expected.
Connected with Issues	The account is currently operational, but non-critical issues have been detected that may require attention.
Failed	The connection is currently disconnected or has encountered a critical error preventing communication.
Deleted	The account or integration has been marked for removal and is currently pending deletion from the system.

Status	Description
Excluded	The account has been excluded from scanning or monitoring by a user. See Exclusions.
Not supported by current license	The account cannot be monitored due to limitations within your existing subscription tier.

Common issues encountered during onboarding often relate to:

- **Permissions** – Incorrectly configured or missing IAM roles, policies, or service account permissions can prevent Tenable from accessing necessary data or making changes in your cloud environment.
- **Connectivity** – Issues with establishing a connection between AI Exposure and your cloud provider.
- **Configuration** – Errors in settings such as CloudTrail configuration, active regions, or naming conventions.

For detailed troubleshooting steps specific to each cloud provider, refer to the relevant article for each provider. See Integrations for a list of supported providers.

For step-by-step guidance on resolving permission and role errors, see Resolve Cloud Onboarding Permission and Role Errors (AWS, Azure, GCP).

Security

Configure Data Masking

> **Required License:** Data masking requires a Tenable One Advanced license or an AI Governance add-on license.

Enable data masking to hide sensitive values from displaying in the console. Tenable One AI Exposure replaces each masked value with the fixed `<REDACTED>` placeholder, which appears throughout the product.

AI Exposure masks sensitive values that contain personally identifiable information (PII), payment card industry (PCI) data, and access data.

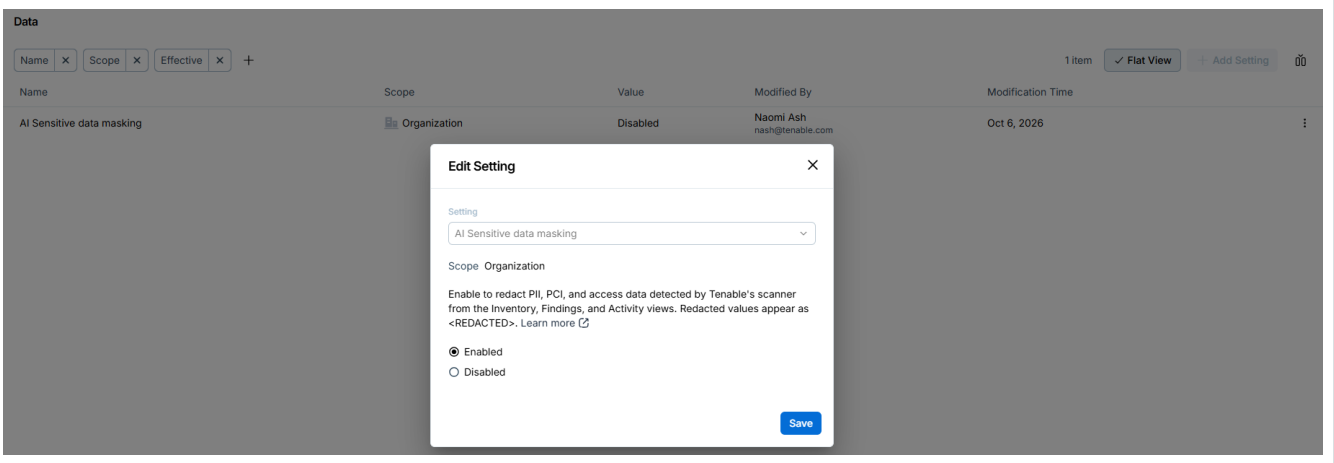
It masks these values in the following areas:

- Activity Detections
- Activity Issues
- Conversations
- Findings generated from PII, PCI, or access data
- Assets, such as agents and skills, where sensitive data (PII, PCI, or access data) is identified

Masking is disabled by default.

To enable masking:

1. Go to **Settings** > **Security** > **Data**.
2. In the **AI Sensitive data masking** row, click the three-dots icon and select **Edit**.
   The **Edit Settings** window appears.
3. Select **Enabled**.



4. Click **Save**.
   AI Exposure enables data masking on sensitive values across **Activity Detections**, **Activity Issues**, and **Conversations**.

The masking setting applies differently to Activity and Posture:

- **Activity** (messages, files, and detections): Masking is not retroactive. When you enable masking, AI Exposure masks only new activity detected after you save the setting. When you disable masking, only new activity appears unmasked. Existing activity remains unchanged.
- **Posture** – Masking is retroactive. When you enable or disable masking, the change applies to all Posture data, including sensitive data detected before the change.

Integrations

The **Integrations** page provides a centralized view of all third-party connections within your organization. From this page, you can monitor the health of your external data sources, identify connection issues, and scale your security ecosystem by adding new integrations.

View Integration Details

To view integration details:

- To locate a specific integration:
  - **Filter** – Click the filters at the top of the table to narrow the list based on specific criteria.+
- To troubleshoot connection issues, check the **Status** and **Issues** columns.
- Click any integration in the table to open the profile slideout panel, where you can see key configuration and connection details.
- For organizations (cloud provider, container registry, code repository), you can also see an **Accounts** tab, which lists key details on all associated accounts managed by the organization, and provides management capabilities per account.

Integrations Table

The Integrations table displays the following information for each connection:

Column	Description
Name	The user-defined name for the specific integration instance.

Column	Description
Scope	The organizational level or account to which the integration is applied.
Type	The specific provider, service, or account. For example, *AWS*, *Jira*, or *ServiceNow*
Category	The functional classification, such as *Cloud Providers*, *SIEM*, or *Identity Providers*.
Creation Time	The date and time the integration was originally configured.
Issues	Displays specific error messages or alerts if a connection is interrupted.
Status	A real-time health indicator, such as *Connected* (green) or *Failed* (red).

Add a New Integration

Expand your visibility by connecting additional resources, tools, and third-party products to Tenable.

To add an integration:

1. On the Integrations page, click **Add Integration** in the top-right corner.
2. In the Integrations Library, search for or select the relevant integration. The Integrations Library includes both organization-level and account-level integrations (such as AWS, Azure, and GCP accounts).

For how-to guides on how to connect these integrations, see the following articles:

Category	Integrations
Cloud Providers	Organizations and accounts for AWS, Alibaba Cloud, Azure, GCP, OCI

Category	Integrations
Identity Providers	Microsoft Entra ID, Google Workspace, Okta, OneLogin, Ping Identity
AI Providers	Anthropic Claude, Google Gemini, Microsoft Copilot, OpenAI ChatGPT
Data Platforms	Snowflake
Container Registries	Container image registries: 3rd-party, JFrog, Cloudsmith
Code Repositories	GitHub, GitLab, Azure Repos, Bitbucket
CI/CD	CI/CD pipelines, Container image CI/CD pipelines: Azure Pipelines, GitHub Actions, GitLab CI/CD, Jenkins Pipelines, Terraform Cloud, Generic
Kubernetes	Via Helm Chart, Amazon EKS, Azure AKS, Google GKE
Ticketing	Jira, ServiceNow
Collaboration	Slack, Microsoft Teams
SIEM	Datadog, QRadar, Splunk, SQS, Webhooks: Microsoft Sentinel, Sumo Logic, Telegram
Network	Network isolated servers

Core Concepts

Product Security and Privacy

This section highlights the major security features of Tenable One AI Exposure.

Hosting Regions

An instance of the AI Exposure service is hosted in each of the following broad geographic regions:

- United States
- Australia
- Brazil
- Canada
- Europe
- India
- Japan
- Singapore
- South Korea
- United Arab Emirates
- United Kingdom
- United States Gov Cloud

Data stored in a given region will stay in that region, and will never be transmitted to a different region.

AI Exposure is a multi-tenant SaaS platform, where each of the service instances mentioned above serves multiple tenants, with logical separation between customers. Alternatively, Tenable does provide support for single-tenant instances upon request, which affects how the solution is priced.

Tenable Console URL

AI Exposure Region	URL
Global (All regions)	https://app.tenable.com
United States Gov Cloud	https://app.tenable.us

Data Segregation

Within an instance, there is full data segregation, ensuring that each customer's data is fully separated on the database level. To support this, Tenable stores each customer's data in an independent, and logically separated, database or set of databases. Such segregation provides the scale and benefits of multi-tenant services, while strictly preventing customers from accessing one another's data.

Data Encryption

All data in transit across open networks is encrypted using TLS 1.2. Similarly all data is encrypted at rest using AES-256.

High Availability and Disaster Recovery

Each AI Exposure service instance is highly available, with all components (for example, compute, database, and networking) spread across multiple availability zones. Tenable uses a load balancer to automatically distribute incoming application traffic across multiple instances and availability zones.

Customer data is continuously backed up once a day, and, additionally, backed up externally via external persistent storage, once a week.

Compliance and Certifications

AI Exposure maintains internal controls that meet the most stringent information security requirements for data protection and privacy. Tenable has achieved the following certifications:

- **SOC 2 Type II** – This report demonstrates Tenable's commitment to the most rigorous security, availability, processing, confidentiality, and privacy standards in the industry, and verifies that our security controls are aligned with the AICPA (The American Institute of Certified Public Accountants).
- **ISO/IEC 27001** – One of the industry's most recognized information security certifications, ISO/IEC 27001:2013 demonstrates that Tenable meets the highest standards for protecting its cloud delivered CNAPP service.

Annual Penetration Tests

Tenable engages with third-party organizations to conduct penetration tests of the production environment, which occur annually, at a minimum. Results are reviewed by Tenable, and high priority findings are tracked to resolution.

Key Management

Tenable has an established key management process in place, using AWS Key Management Service (KMS) to support the organization's use of cryptographic techniques.

Authentication

Tenable supports the following modes of authentication for login to the AI Exposure Console:

- Microsoft Entra ID
- Google SSO
- IdP SAML SSO
- Username and password (See Password Policy.)

Users can log in to the AI Exposure Console via SSO by establishing trust between your external identity provider (IdP) and Tenable. This eases user provisioning by leveraging the existing corporate identities of your users. It does not, however, provide for automatic user provisioning: after trust is established, you still need to add new Tenable users or groups via the console, or via API. For more information about enabling SSO login, see Single Sign-On.

Password Policy

The AI Exposure password policy requires that passwords be at minimum 8 characters long and contain the following:

1. Uppercase letter
2. Lowercase letter
3. Number

Timeout Settings

To enhance account security and reduce the risk of unauthorized access, administrators can configure two types of timeouts for the web Console:

- **Inactivity Timeout** – Ends a session after a period of user inactivity. The default value is **12 hours**.
- **Session Timeout** – Ends a session after a fixed duration, regardless of user activity. *This setting is disabled by default*.

These settings can be adjusted based on your organization's security and compliance needs. For more information, see Console Timeout Settings.

Account Hierarchy and Folders

Tenable One AI Exposure displays your account hierarchy throughout the Console. This hierarchy affects how you manage and interact with the following entities within Tenable (see Account Scopes):

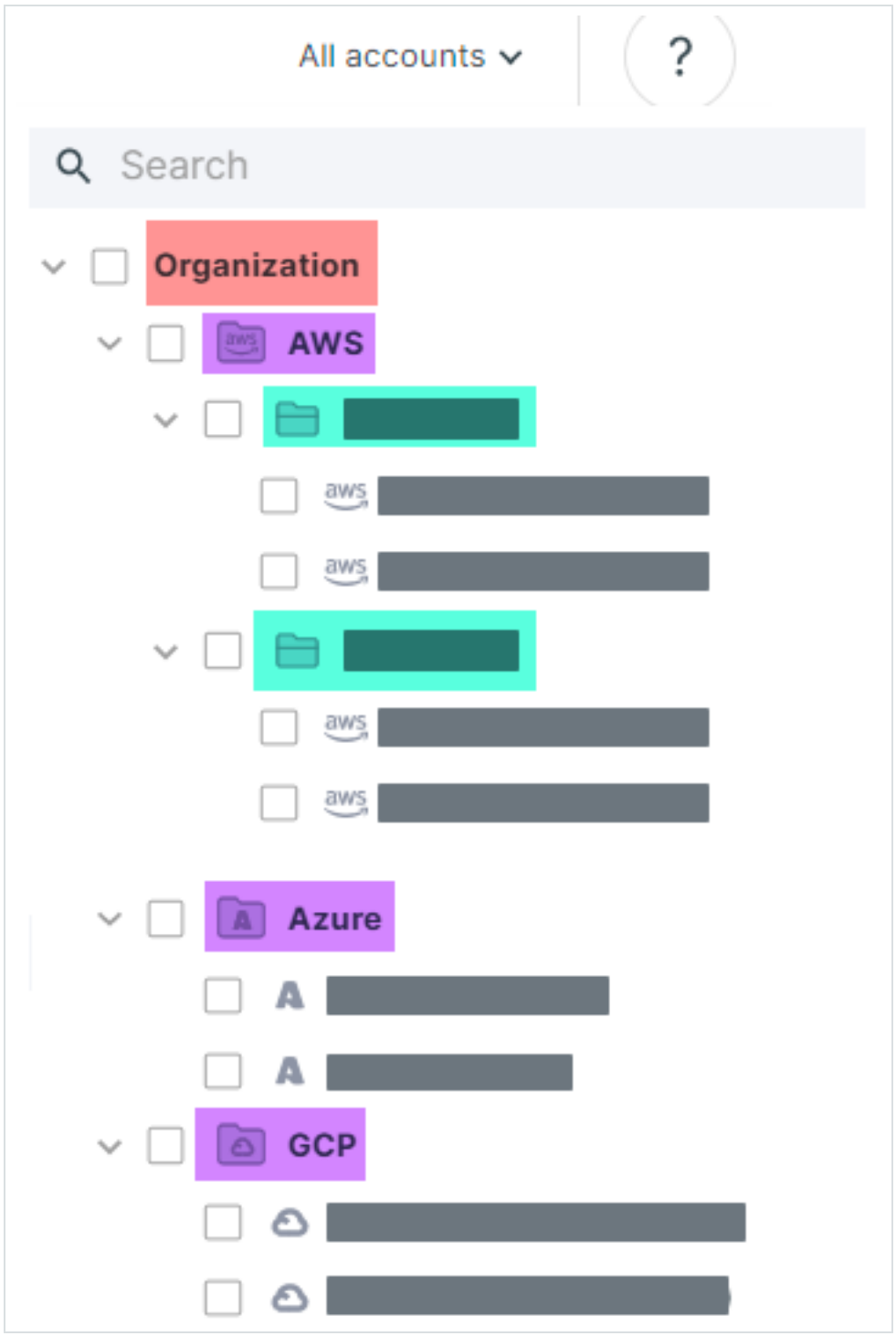
- Projects
- Cloud accounts
- Identity providers
- Code repositories
- Container registries

Tenable automatically creates a top-level **Organization** *folder*, which contains all other folders in your organization. Underneath the Organization folder, additional folders are automatically created when you add your first account belonging to each respective cloud provider (or identity provider).

If your organization has a large number of accounts, it's important to maintain a structured account hierarchy within AI Exposure, using folders. You can create this structure in the following ways:

- (*Recommended*) Automatically Update Folder Structure in Tenable based on the cloud folder structure of the onboarded organization.
- Manually create folders in Tenable to group your onboarded cloud accounts together logically.

Important: Any identity provider tenant that you onboard to AI Exposure will also appear in your organization tree, but you can't manually create folders for them.



Note: You can't delete, rename, or move the Organization, AWS, Alibaba Cloud, Azure, GCP, or OCI parent folders. You can't group accounts from different cloud providers together. AWS Audit log accounts don’t appear in the account folder tree throughout the Console.

Automatically Update Folder Structure

During onboarding for cloud providers, identity providers, and code repositories, you can choose whether to *automatically update the folder structure* in AI Exposure. When this option is **enabled**:

- The folder structure of the onboarded organization is copied into the platform, keeping your account hierarchy intact and continuously synchronized. For example, within AWS, if you move an existing account to a newly-created folder, that change will then be reflected in Tenable.
- Account structure changes are reflected in AI Exposure the next time data is synchronized in your environment.
- Any folders that don't exist in your environment are deleted.
- Any empty folders in your environment are deleted.
- You can't move, edit, or create folders/accounts in the organization within AI Exposure.
- You can only manually add new accounts to the root, **Organization** folder, but not to the specific organization.
- If an account is moved to a different organization in your cloud provider:
    - If the other organization is NOT onboarded to Tenable, the account remains in its current location in Tenable. You can choose to delete the account.
    - If the other organization IS onboarded to Tenable, the account moves to its new location in Tenable.
- AI Exposure user permissions are connected to the account scope they were defined on. For example, if your user has *Collaborator* permissions that were granted on a specific folder-level scope (**Folder 1**), and then **Folder 1** moves to a new location in the cloud, you still retain the same permissions. See Advanced Use Case Examples for more information.

Account Moves and Parent Folder Dependencies

When you enable the *automatically update folder structure* option, AI Exposure moves an account or subfolder when it moves to a different parent folder in your cloud environment. Whether the move

goes ahead depends on how the account or subfolder uses configuration defined on its previous parent folder:

- Custom Policies and Exclusions – The move goes ahead, and the configuration stops applying to the moved account or subfolder.
- Automations, scheduled reports, custom compliance, role assignments, and JIT eligibilities. The move is blocked if the account or subfolder depends on configuration defined outside its new location.

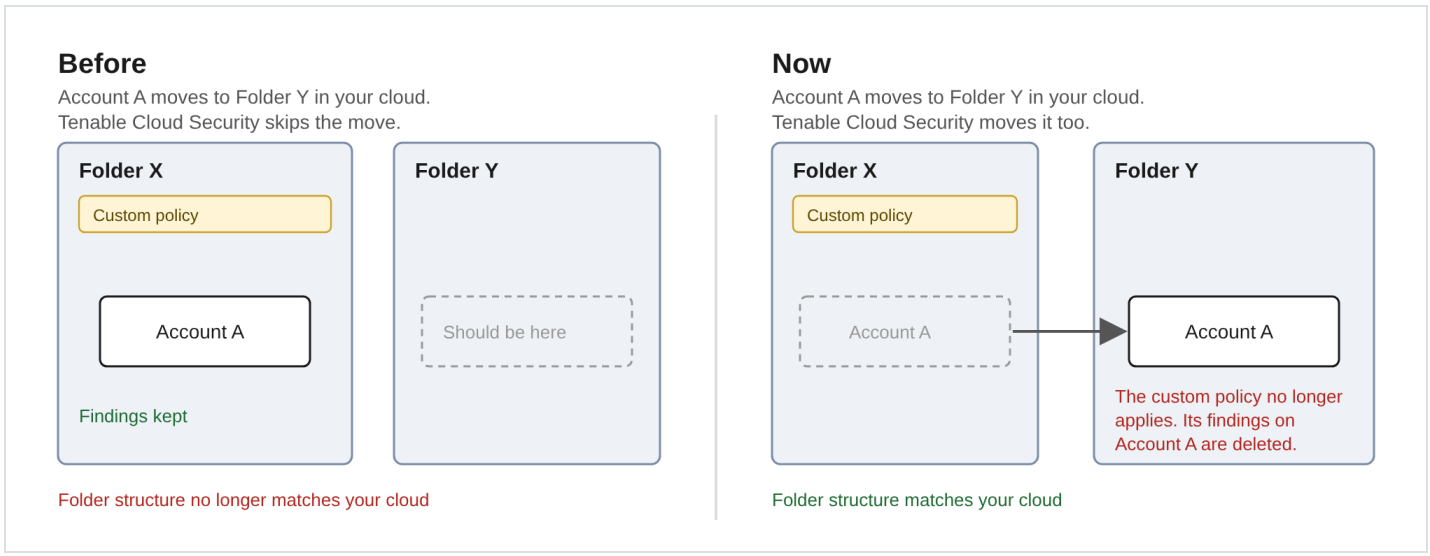
Custom Policies and Exclusions

A custom policy or exclusion on the previous parent folder does not block the move. After the move, it no longer applies to the moved account or subfolder:

- **Custom policies**. Tenable deletes the findings of the custom policy on the moved resources. Custom policies defined on the moved account or subfolder, or on its new parent folders, continue to apply. Findings of built-in policies are not affected.
- **Exclusions** – Findings that the exclusion ignored reopen. Findings whose severity the exclusion changed return to their original severity.

  > **Note:** After a move, some custom policy findings can disappear, and some excluded findings can reopen. Both results are expected.

- **Example** - Custom policy:
  1. **Folder X** has a custom policy that generates findings on **Account A**.
  2. In your cloud environment, you move **Account A** from **Folder X** to **Folder Y**.
  3. ***Result***: **Account A** moves to **Folder Y** in AI Exposure. The custom policy on **Folder X** no longer applies to **Account A**, so Tenable deletes its findings on **Account A**.



Automations, Scheduled Reports, and Other Dependencies

Tenable blocks a move that would break an existing setup. A move is blocked when an item on the moved account or subfolder uses an integration, policy, or role defined outside its new location. A configuration is defined *outside the new location* when it sits on a folder that is not inside the moved account or subfolder and is not above it after the move.

The following table describes the items that can block a move.

Item	Blocks the Move When
Automation	An automation rule that targets the moved account or subfolder is defined outside its new location. Or an automation rule on the moved account or subfolder uses an integration defined outside its new location.
Scheduled report	A scheduled report on the moved account or subfolder uses an integration, a custom compliance, or a custom policy defined outside its new location.
Custom compliance	A custom compliance on the moved account or subfolder includes a custom policy defined outside its new location.
Role	A user, group, or service account has a custom role on the moved account or

Item	Blocks the Move When
assignment	subfolder, and the custom role is defined outside its new location. Or a service account has a role on the moved account or subfolder, and the service account is defined outside its new location.
JIT eligibility	A JIT eligibility on the moved account or subfolder uses an integration defined outside its new location, for example, to send approval requests to Slack. Or a JIT eligibility defined outside its new location targets the moved account or subfolder.

When Tenable blocks a move, the account or subfolder stays in its current folder, and AI Exposure does not display a message in the Console. Until you resolve the dependency, your folder structure in AI Exposure does not match your cloud environment for that account or subfolder. See Example #1 in Advanced Use Case Examples.

Advanced Use Case Examples

- **Example #1** - Automation:
    1. You configured an integration (**Slack**) on a specific folder-level scope (**Folder 1**) that contains multiple children accounts.
    2. In one of the children accounts (**Account 1**), you defined automations that use this Slack integration.
    3. Afterwards, in your AWS environment, you moved **Account 1** to a different folder (**Folder 2**).
    4. ***Result***: Tenable *doesn't move the account to the new folder*, so as not to break the existing automation flow.
- **Example #2** - Permissions:
    1. Your AI Exposure user has *Collaborator* permissions that were granted on a specific folder-level scope (**Folder 1**) that contains multiple children accounts.

2. Afterwards, in your AWS environment, you moved **Account 1** to a different folder (**Folder 2**).
3. ***Result***: Your user will no longer have permissions to **Account 1**, since your permissions were defined on the parent-level scope (**Folder 1**), and not the account itself.

FAQ

> Why is my organization structure not synced with the cloud?

1. Account structure changes are reflected in AI Exposure the next time data is synchronized in your environment.
2. See Example #1 in Advanced Use Case Examples
3. An automation, scheduled report, custom compliance, role assignment, or JIT eligibility depends on a folder outside the new location. See Automations, Scheduled Reports, and Other Dependencies.

> Why can't I edit/delete/move a folder or account in Tenable?

If you enabled the *automatically update folder structure* option during cloud organization onboarding, you can't edit/delete/move folders or accounts in Tenable, since these entities are synchronized from your cloud environment.

Create Account Folders

Create account folders to manually group your onboarded cloud accounts together logically, based on, for example:

- Development or production environments
- Product
- Business units with unique owners

These folders let you nest accounts (and other folders) like you would in existing hierarchies within cloud service providers:

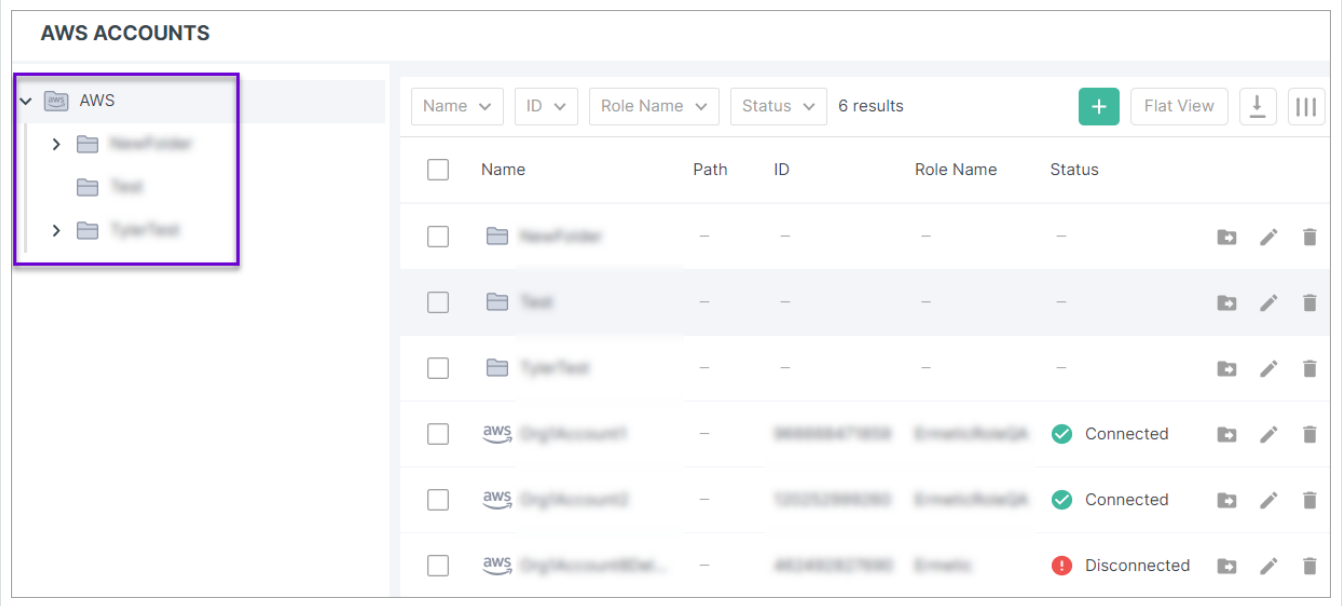
- AWS organizational units (OUs)
- Alibaba Cloud organizations
- Azure management groups
- GCP folders
- OCI tenancies

Custom folders are marked in the tree structure with a folder icon, and accounts are marked with the respective icon of the cloud provider.

To work with folders:

1. In the AI Exposure Console, navigate to **Settings** > **Accounts** and then choose one of the relevant providers.

   Any existing folders appear in the tree on the left-hand side of the page.



2. Navigate to the location where you want to add the folder. For example, if you want to add it under the root AWS folder, select the AWS folder in the tree.

When you select a folder, all accounts (and any nested folders) that belong to the folder appear in the main table.

3. Click + and then **Create folder**.
4. Enter a unique name for the new folder, and then click **CREATE FOLDER**.

   The folder appears in the tree hierarchy on the left, and in the main table of accounts and folders.
5. To rename a folder, click the **Edit** button next to the folder and then enter a new name.
6. To delete a folder, click the **Delete** button next to the folder and confirm deletion.
7. To move a folder, click the **Move** button next to the folder and then choose a new location for it by selecting the relevant folder.

Note: You can't delete, rename, or move the Organization, AWS, Alibaba Cloud, Azure, GCP, or OCI parent folders. You can't group accounts from different cloud providers together.

Account Scopes

An *account scope* represents an onboarded cloud account, identity provider tenant, or IaC repository, or a group of such accounts, and can be any of the following:

- The entire Organization (all accounts onboarded to AI Exposure).
- A group of accounts. For example, all accounts belonging to a specific cloud provider (all AWS accounts) or identity provider (all Microsoft Entra ID tenants), or a group of accounts within a specific cloud provider (grouped by folder).
- A specific account/identity provider tenant.
- A project.
- All IaC organizations, or a subset of individual repositories. This grants access to view code scan results for a specific scope.

You can filter Console data and configure features in the AI Exposure Console on specific *account scopes*.

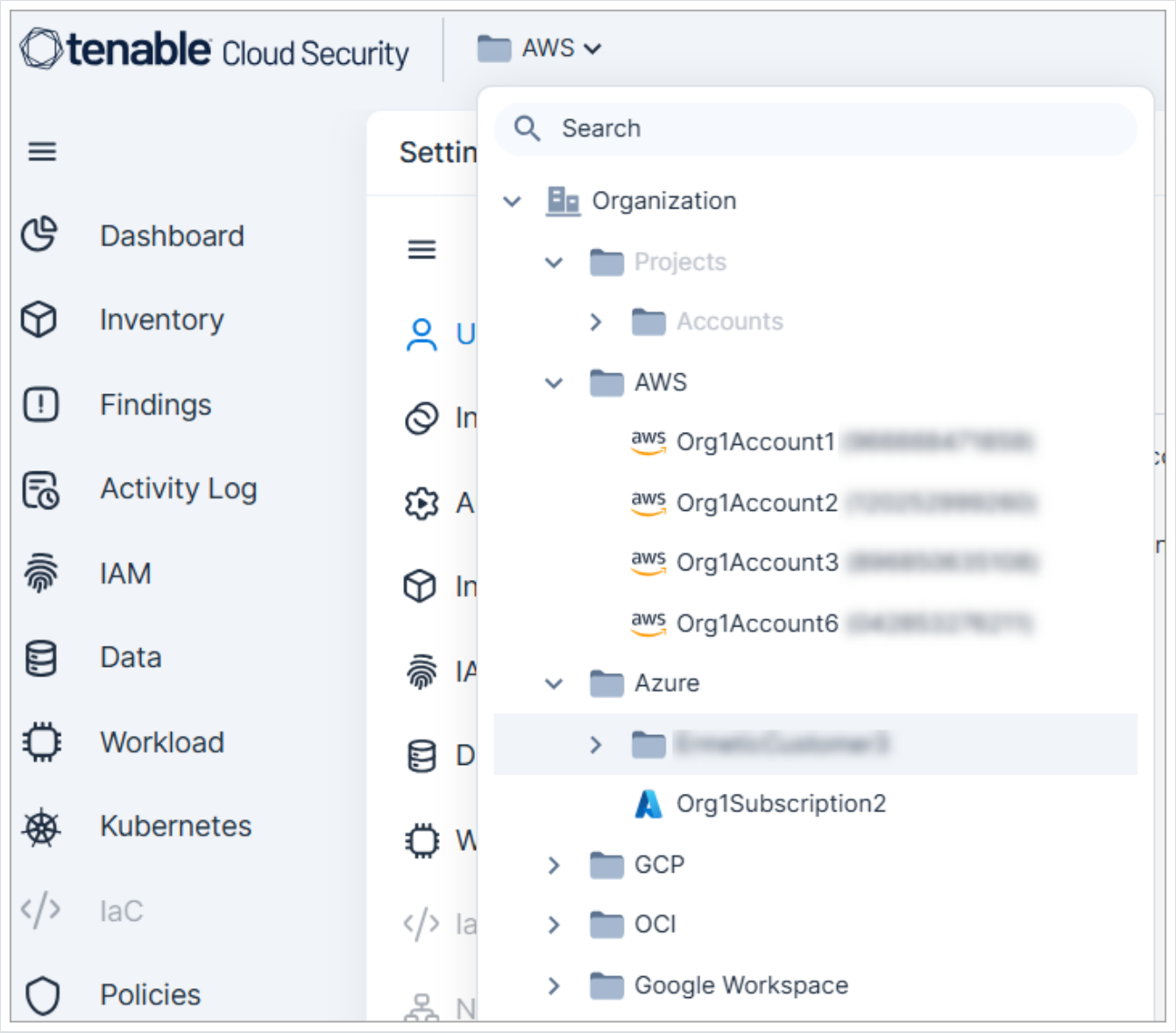
Filter Console Data and Configure Features by Account Scope

View and configure specific features in the AI Exposure Console within a specific account scope. For example, you can create a custom policy to monitor violations in a specific Azure account.

- The account scope you select will persist as you navigate across Console pages. It will remain set to your chosen scope, and won't revert to a default unless you manually change it.
- The *account scope* filter supports selecting a *single scope* at any given time. *This filter does not support selecting multiple account scopes at once.* What can you do instead?
    1. Create a project that includes the desired scopes, and then filter by the project.
    2. Within relevant Console pages, you can use the **Account/s** filter to filter for multiple account scopes at once. For example, in the Findings page, and across the Data/Workload pages. Be aware that you may need to add the filter if it doesn't appear by default.

To view/configure features by account scope:

- From any page in the Console, click on the account scope dropdown and select a scope.



The scope you choose impacts the actions you can perform in various ways. For example, consider the following:

- **Custom policies** – You can only enable or disable a custom policy from the original folder/account that you created it from. For example, if you created a custom policy from the top-level **AWS** folder, you won't be able to enable/disable it from any children folders/accounts within the AWS folder. See Custom Policies for more information.

Supported Features

You can view and configure most Console features by account scope, including, for example, the following:

- Add AI Exposure users
- Add integrations
- Create reports
- View license usage data
- View Kubernetes clusters
- Add JIT eligibilities (cloud accounts only)
- Configure Workload Protection settings (cloud accounts only)
- Enable/disable policies (cloud accounts only)
- Create automation rules (cloud accounts only)
- View Compliance scores (cloud accounts only)
- View IaC code scan results (IaC organizations only)

Account Inheritance

Entities created on the organization level or within a group of accounts (folder) are inherited to all children accounts, including to any children accounts created at a later time. For example, Console users.

How Projects Work

This is a conceptual overview about how projects work. For a how-to guide for configuring projects, see Projects.

Managing many cloud accounts or resources across multiple providers is challenging, especially with frequent account creation and deletion. *Projects* in Tenable One AI Exposure help simplify this by logically grouping accounts or resources, making it easier to manage access.

For example, projects let you view Console data based on your organization's distinct operational groupings of your cloud environment. By organizing accounts or resources into projects, you can align visibility and permissions with your existing organizational structure, ensuring a more intuitive and efficient management experience. Projects also streamline access control by allowing you to grant users permissions specific to the accounts and resources they need, reducing manual effort and improving cloud management.

To get started:

1. Learn about How Projects Work, Supported Features, and common use cases.
2. Add projects and project folders.
3. Grant users Console access to a specific project scope by adding users/groups.

How Projects Work

A project is a logical grouping of resources within your cloud environment, enabling flexible organization and management, even across multiple cloud providers. A single account can belong to multiple projects, allowing you to structure access and visibility according to different operational needs. After creating a project, you can assign Console users permissions to view Console data within its scope. Additionally, depending on the project's configuration, users assigned to a project can also automatically gain access to the accounts within that project's scope.

A project consists of one or more *scope group*. Each scope group is made up of:

- **A group of cloud *Accounts*** – This can be any combination of one or more of the following:
  - Cloud accounts (for example, AWS).
  - Identity provider tenants (for example, Google Workspace).
  - Code repositories (for example, a GitHub organization).

  For each of the above, you can select any scope - the entire root folder (for example, *AWS*), individual folders, or individual accounts. For example, a scope group can comprise all your

AWS and Azure development accounts. Additionally, you can select the entire organization as a scope group.

- (Optional) **One or more logical *Conditions***.
  - Limit the project scope by specifying a pattern that accounts must match to be included.
  - The condition pattern can be based on *account name*, *account tag*, resource tag, or *Azure resource group name*. See Add a Project for details about how to configure these.

When to Use Projects

When deciding whether and how to create projects, consider whether you've chosen to Automatically Update Folder Structure for your cloud accounts.

- **If you enabled this option**, the folder structure of the onboarded organization is copied into the platform as is, and you can't move, edit, or create folders/accounts in the organization. As a result, you may find projects useful for additional flexibility in grouping accounts.
- **If you disabled this option**, you have more control over organizing accounts within each provider's folder structure. In this case, Tenable recommends manually grouping accounts within provider-specific folders whenever possible and using projects only for specific cases where manual grouping doesn't meet your needs.

Common Project Use Cases

This section highlights some common ways organizations can use projects and project folders to streamline cloud account management. For example, you can create projects to:

- **Organize accounts by ownership and responsibility**.
  - Create Projects for Product Groups
  - Create Projects for Business Functions
- **Organize accounts by infrastructure and operations**.
  - Create Projects for Development and Production Accounts
  - Create Projects for Application and Service Boundaries (Azure)

Create Projects for Product Groups

Large organizations often have multiple product teams (for example, *Group A*, *Group B*, *Group C*) that manage their own cloud accounts. Each group may use different account naming conventions or account tags to distinguish their accounts.

How to implement:

1. Add a project for each product group (for example, "Group A Project," "Group B Project").
2. Add conditions to dynamically assign accounts to the correct project by using **account tags** or **name** conventions.
    - Example tag key/value patterns:
        - key is `product`, value is `GroupA`
        - key is `team`, value is `GroupB`
    - Example name patterns:
        - `group-a-prod-001`
        - `group-b-dev-002`
3. Add project folders to organize the projects by region, or other relevant category.
4. Grant users Console access to a specific project scope by adding users/groups. For example:
    - Grant regional administrators access at the project folder level to manage all child projects at once.
    - Grant team-specific access to individual projects.

Create Projects for Business Functions

Many organizations categorize cloud resources based on business functions such as *Finance*, *Compliance*, or *Operations*. By leveraging resource tag patterns, you can dynamically assign accounts to projects based on predefined tag key-value pairs to create projects based on these functions.

How to implement:

1. Add a project for each business function.
2. Add conditions to dynamically assign accounts to the correct project by using **resource tag** patterns.
    - Example tag key/value patterns:
        - key is `business_unit`, value is `finance`
        - key is `compliance_level`, value is `high*`
3. (Optional) Add a project folder to group projects by broader categories.
4. Grant users Console access to a specific project scope by adding users/groups. For example:
    - Grant access at the project folder level to allow broader access across all environments.
    - Grant project-specific access.

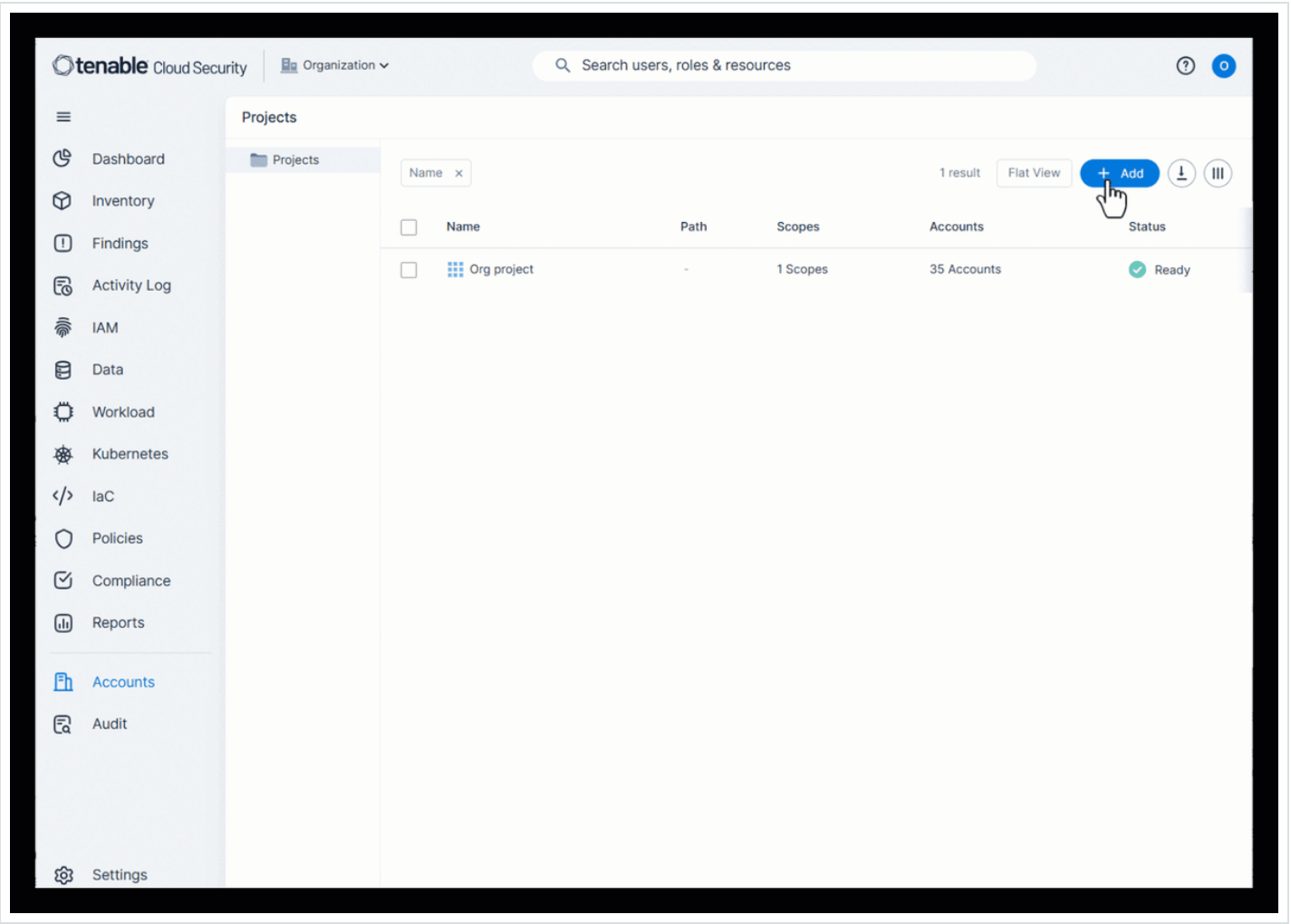
Create Projects for Development and Production Accounts

Many organizations maintain strict separation between development and production environments. To enforce this, you can create projects that group accounts based on their environment type while ensuring that production projects do not include test-related accounts.

How to implement:

1. Add a project for your **development** accounts.
2. Add conditions to dynamically assign accounts to the correct project by using **account tags** or **name** patterns.
    - Example tag key/value patterns:
        - key is `environment`, value is `dev*`
        - key is `stage`, value is `staging*`
    - Example name pattern:
        - `dev*`

3. Exclude test accounts from the project.
    - Example name pattern exclusion:
        - *Is not* `*test`
4. Exclude production accounts from the project.
    - Example tag key/value pattern exclusion:
        - key is not `type`, value is not `prod*`
5. Add a project for your **production** accounts.
6. Add conditions to dynamically assign accounts to the correct project by using account tags or naming conventions.
    - Example **production** tag key/value patterns:
        - key is `environment`, value is `prod*`
        - Example name pattern:
        - `prod*`
7. (Optional) Add a **development** project folder to organize all development projects.
8. (Optional) Add a **production** project folder to organize all development projects.
9. Grant users Console access to a specific project scope by adding users/groups. For example:
    - Grant access at the project folder level to allow broader access across all environments.
    - Grant project-specific access.



Create Projects for Application and Service Boundaries (Azure)

For organizations using Azure, resource groups serve as a key organizational structure for managing cloud assets. By leveraging Azure resource group name patterns, you can create projects that align with operational boundaries, such as application ownership, workload types, or geographic regions.

How to implement:

1. Add a project for each relevant Azure grouping (for example, "Customer-Facing Apps* or *Internal IT Services*).

2. Add conditions to dynamically assign accounts to the correct project by using **Azure resource group name** patterns.
    - Example resource group name patterns:
        - `cust-facing-apps-*` (for externally facing applications)
        - `internal-it-*` (for internal IT services)
3. (Optional) Add a project folder to group projects by broader categories.
4. Grant users Console access to a specific project scope by adding users/groups. For example:
    - Grant access at the project folder level to allow broader access across all environments.
    - Grant project-specific access. For example, grant developers access only to *Customer-Facing Apps* or IT administrators access to *Internal IT Services* projects.

Supported Features

Many AI Exposure features support projects, allowing you to perform actions within a specific project scope. Only users assigned a matching project scope can view/manage these features.

For example, you can perform the following for a project scope:

- User Management
- Create integrations and automations
- Create reports
- Create a custom compliance
- Create API tokens and query the AI Exposure API
- View licensing data
- Create custom policies

So, for example, only a user assigned to *Project A* can create an API token for that scope.

Project Permissions and Capabilities

Project permissions define what actions a user can perform on the resources logically grouped within a project. These permissions can be explicitly granted through direct role assignments or automatically extended via project scope propagation. This section explains how your total project-related permissions are determined and the specific actions they enable.

Project Permissions

Project permissions determine what you can do within a project. They are granted to you directly when an Administrator assigns you a specific role at a project or project folder scope. This role allows you to see and manage the project itself, but it does not automatically give you access to configure the individual scopes inside of it.

Project permissions:

- Primarily provide view-only access for organizing and filtering data.
- Do not allow you to make most configuration changes to settings within the project scope. For example, you can't make configuration changes to built-in policies.

  However, you can still mark resources as sensitive and change finding statuses.

A user's effective permissions for accounts within the project may be higher if they have other direct assignments to those accounts.

Propagation

Propagation is a feature that automatically extends user permissions from a project to also include scopes with the project. When a project is configured with propagation enabled, a project-level role is automatically applied to all eligible scopes inside that project.

> **Important:** Propagation applies only to scopes not filtered by resource-based conditions defined in this project.

How does it work?

- **Without propagation** – Your permissions apply only to the project itself.
- **With propagation** – Your permissions are extended. If you are an Admin on a project with propagation enabled, you will automatically become an Admin on all eligible scopes within that project. This streamlines access management and ensures you have consistent permissions across the resources you need to manage. *This means you can perform configuration changes and other actions on the propagated accounts, based on the role assigned to you at the project level*.

Effective Permissions

When you have multiple role assignments, your final permissions (your *Effective Permission*) are always the highest level of access granted to you. For example, if you are a *Viewer* on a scope but gain *Administrator* access to that same scope through project propagation, your effective permission for that account is *Administrator*. The higher-level permission always takes precedence.

Finding Lifecycle

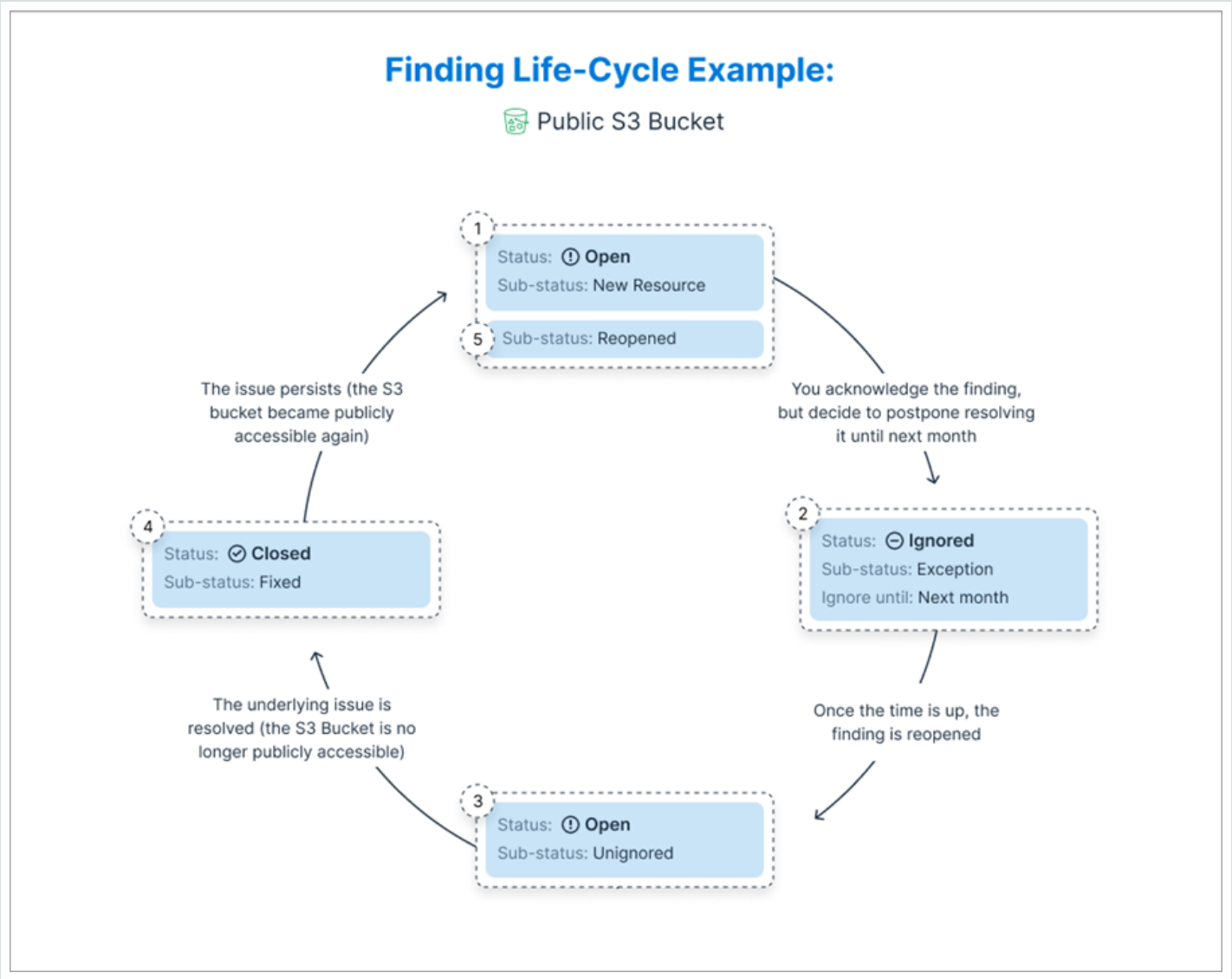
Findings progress through a lifecycle with distinct statuses and sub-statuses, which help you understand the overall state of risk and why a finding has its current status.

This is a conceptual overview of finding statuses and the finding lifecycle.

- For a how-to guide about viewing and managing findings, see Cloud Findings or IaC Findings.
- For a conceptual overview of how finding severity works, see Finding Severity.
- To configure how findings are created (via policies), see Cloud Policies and/or IaC Policies.

Finding Lifecycle Example

This image shows an example of the flow and progress of a finding (*Public S3 Bucket*) detected in your environment. See Finding Status for more information about specific statuses and sub-statuses.

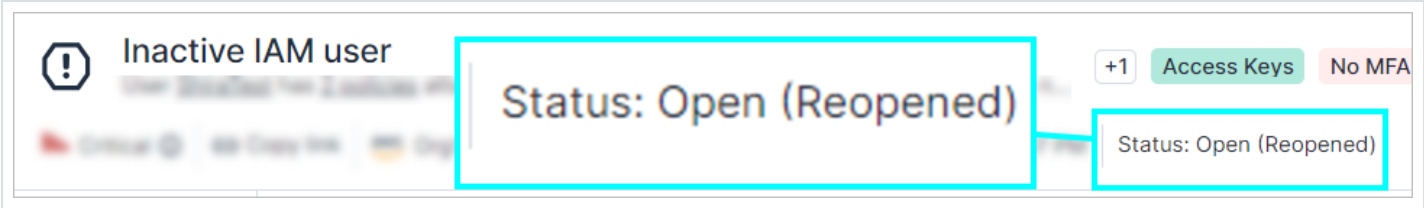


Finding Status

Finding statuses help you understand both:

- The overall state of risk in your organization (for example, via the Trends widget in the Dashboard).
- Why specific findings were open/closed, helping you track the work you do and the progress you make resolving and closing findings.

The status consists of the main **Status** (Open/Ignored/Closed), and a **Sub-Status**, which provides added granularity, and describes the reason why the finding has the current status. In this example, the Status is *Open*, and the Sub-Status is *Reopened*.



Open Findings

Open findings represent the *active* issues detected in your environment. This includes at-risk identities and resources, and hard-to-spot toxic combinations.

This table lists possible sub-statuses for Open findings. A sub-status provides added granularity, and describes the reason why the finding has the current status.

Sub-Status	Definition
New resource	The resource was created in the past week and matched the policy rules. If the creation time is not available, and the resource was seen in the most recent scan (within the last week), but not in previous scans before that, it's considered a new resource.
Existing resource	Tenable scanned this resource before, but this is the first time it matched with the policy rules. If it's the first scan after the account was onboarded, and the resource creation time is not available, the resource is also considered an existing resource.
Reopened	The finding transitioned from **Closed** to **Open**: • *System* - The issue persists. It was previously resolved, but is now happening again.

Sub-Status	Definition
	• *Manual* - The finding was manually closed, but the user reopened it manually.
Unignored	The finding transitioned from **Ignored** to **Open** when the exclusion ignoring it was updated, disabled, deleted, or expired.
Anomaly	Tenable detected an anomaly based on the identity or resource activity. All anomaly policies are assigned this sub-status.

Ignored Findings

Ignored findings represent issues that you may not want to handle right away. The associated resources are being excluded, either permanently, or for a set period of time.

This table lists possible sub-statuses for Ignored findings. A sub-status provides added granularity, and describes the reason why the finding has the current status.

Sub-Status	Definition
Exception	The finding is accepted temporarily until remediation is completed.
False positive	The finding was verified as incorrect or irrelevant.
By design	The configuration is intentional and required for functionality.

Ignored findings are managed through exclusions, which let you ignore findings or adjust severity based on business needs. Learn how to create pattern-based exclusions from ignored findings and audit and manage your exclusions.

Closed Findings

Closed findings represent issues that have been closed, either manually by a user, or automatically by Tenable.

This table lists possible sub-statuses for Closed findings. A sub-status provides added granularity, and describes the reason why the finding has the current status.

Sub-Status	Definition
Fixed	The finding was resolved: • The resource doesn't match the policy rules anymore. • The resource was deleted according to Tenable's policy recommendation. For example, an inactive GCP service account that was deleted. See Findings With Resource Deletion Recommendations for a list of relevant finding types.
False positive	Finding was marked as a false positive by Tenable.
Manually closed	A user manually marked the finding as *Closed*.
Resource deleted	The resource was deleted, and Tenable's policy doesn't recommend deletion.
Self resolved	The state of the resource or its permissions have changed, and Tenable needs to perform another evaluation cycle to determine whether the issue persists. For example: • An overprivileged identity's permissions have changed. • An Inactive IAM role that became active again. • A user was added to an overprivileged IAM group (Reanalyzing due to newly created member added to the group). • A permission set has been assigned to a new account.

Connect

AI Platforms

Connect Microsoft Copilot

Use this procedure to integrate Microsoft Copilot with Tenable One AI Exposure.

Prerequisites

- A Global Administrator or Power Platform Administrator role within your Microsoft Entra ID environment.
- A registered application called Tenable within your Microsoft Entra ID environment.
- AI Exposure supports the following Microsoft Copilot license SKUs:
    - `a69133fb-7e57-40ce-9a69-6c8551bb7854` - Microsoft 365 Copilot for Business
    - `a809996b-059e-42e2-9866-db24b99a9782` - Microsoft 365 Copilot
    - `ad9c22b3-52d7-4e7e-973c-88121ea96436` - Microsoft 365 Copilot (Education Faculty)
    - `639dec6b-bb19-468b-871c-c5c441c4b0cb` - Microsoft 365 Copilot (Enterprise)
    - `9a18296a-025f-4e37-9ffa-30bf8d1ce775`- Microsoft 365 E7 (The Frontier Suite)
    - `15f2e9fc-b782-4f73-bf51-81d8b7fff6f4` - Microsoft Copilot for Sales

Set Up Microsoft Entra Graph API Access

To allow Microsoft Entra Graph API to send conversations to AI Exposure, run a deployment script in Azure CLI or Azure Cloud Shell.

1. In AI Exposure, navigate to **Settings > Integrations** and click **Add Integration**.
2. In the **Integrations Library**, select **Microsoft Copilot**. The **Add Integration** wizard opens.
3. On the **Configuration** page:

a. Enter a **Name** for your integration. The Console displays this name.

b. Select one of the following options:

- **Use existing Microsoft Entra ID integration (Recommended)** - Select an existing Microsoft Entra ID or create a new one.
- **Do not use Microsoft Entra ID integration** - Enter Tenant ID.

> **Note:** Tenable recommends that you connect a Microsoft Entra tenant to enable identity visibility for synchronized user conversations.

c. In the **Access Verification** section, click **Verify**. The system redirects you to log in to your Microsoft Entra ID tenant to verify access.

d. In the **Deployment** section, copy the script that appears in the wizard and run it in Azure CLI or Azure Cloud Shell to grant AI Exposure the required permissions.

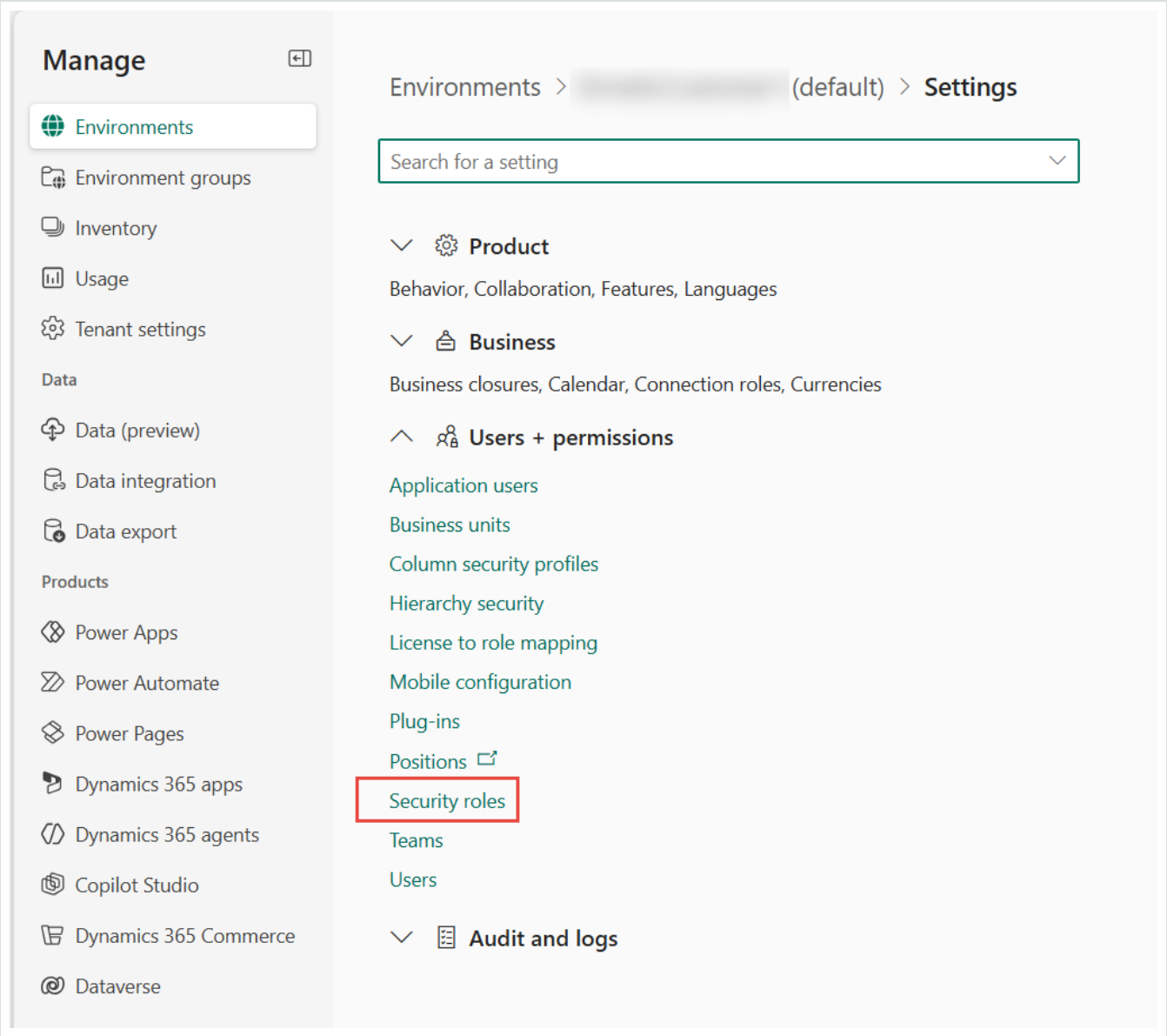
After this step, create a security role and application user for the Tenable application.

Configure Power Platform Security Roles and Application User

> **Important:** Repeat these configuration steps for each environment you want to connect.

Create a Custom Security Role

1. Log in to the Power Platform admin center.
2. In the left navigation bar, select **Manage**.
3. Navigate to the environment you want to connect.
4. Navigate to **Settings**.
5. Click **Users + permissions > Security roles**.



6. Click **New role**.

> **Note:** You must be a member of the Microsoft Entra ID environment to perform this step. You can verify that you are a member on the environment details page. If you are not a member, in the upper-right corner of the environment details page, select **Membership** and add yourself as a member.

7. In the **Role Name** box, enter **Tenable Copilot Reader**.
8. In the **Business Unit** section, select a business unit from the list or create a new one. Then, copy the business unit name for future use.

9. Select **Applies to Tenable Copilot Reader**.
10. In the **Description** and **Summary of Core Table Privileges** boxes, provide any text that fits your use case.
11. From the **Member's privilege inheritance** drop-down list, select **Direct User (Basic) access level and Team privileges**.
12. Select the **Include App Opener privileges for running Model-Driven apps** checkbox.
13. Click **Save**.
14. Navigate to **Settings** > **Security roles**, and select the newly created **Tenable Copilot Reader** role. The role page appears.
15. Set **Read** access in the **Organization** scope for the following tables:

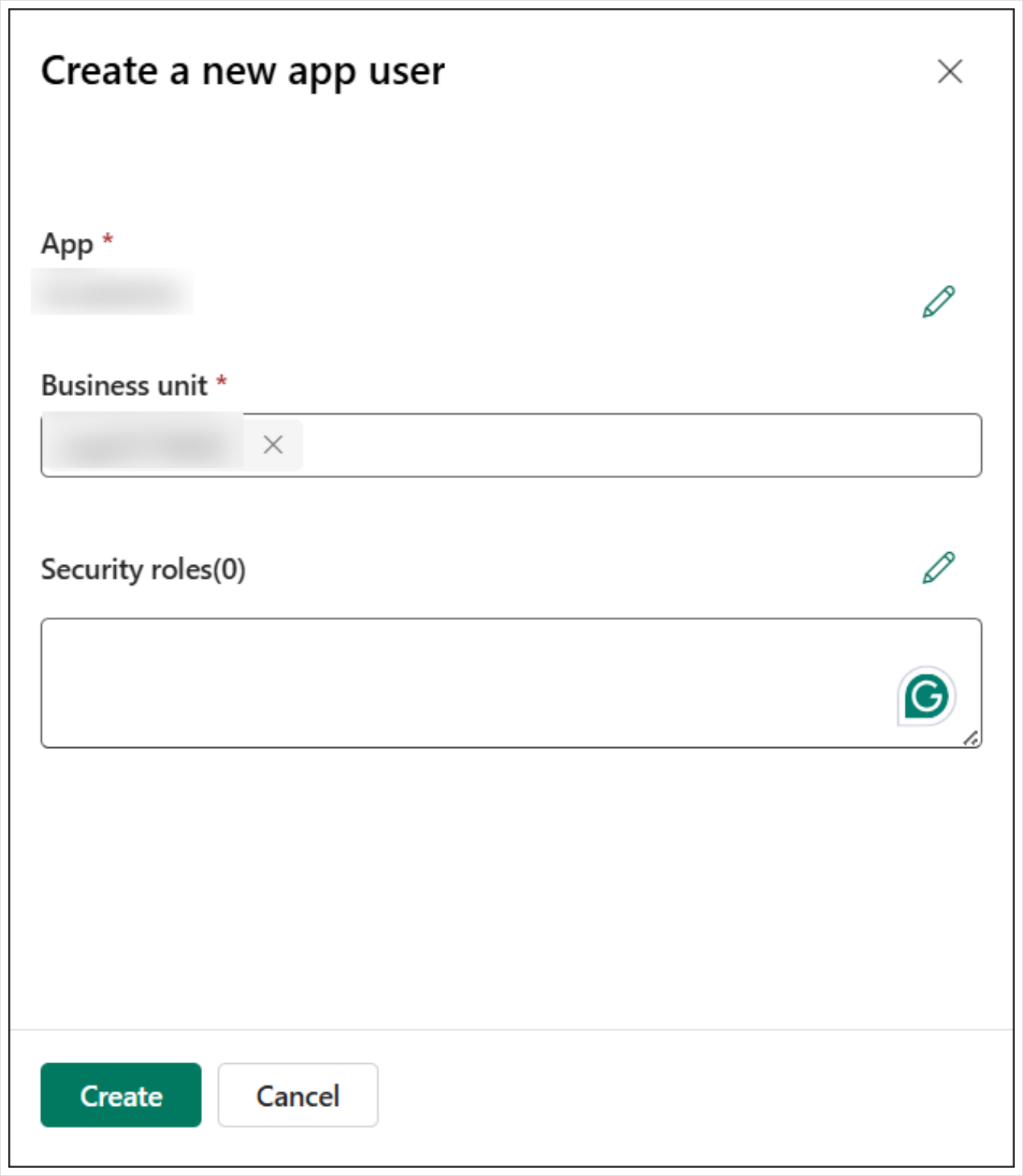
Table	Name	Permissions
Agent	bot	Read (Organization)
Agent component	botcomponent	Read (Organization)
Agent component collection	botcomponent collection	Read (Organization)
Connection Reference	connectionreference	Read (Organization)
Security Role	role	Read (Organization)
User	systemuser	Read (Organization)

16. Click **Save**.

Create an Application User

1. Log in to the Power Platform admin center.
2. Go to **Manage** > **Environments** and select your target environment.
3. Click **Settings**.
4. In the **Users + permissions** section, select **Application users**.

5. Click **+ New app user**.
6. Click **+ Add an app** and search for **Tenable One Cloud Exposure Copilot**.



7. In the **Business Unit** section, select the same business unit you used when configuring the selected security role.
8. In the **Security role** section, select **Tenable Copilot Reader** role and click **Save**.
9. Click **Create**.
10. After configuring Power Platform by creating a security role and application user, click **Next** in the Console to proceed with the integration setup.

Connect Microsoft Copilot

1. In the AI Exposure wizard, click **Next** to continue.
2. On the **Scopes Page**, select one of the following options:
    - **Sync all current and future environments (recommended)**

      > **Important:** Selecting the **Sync all current and future environments (recommended)** option does not automatically configure access in Power Platform. AI Exposure synchronizes an environment only after you create the security role and application user in that specific environment. This requirement applies to both existing environments and any environments you add in the future. AI Exposure cannot synchronize data from the environment until you complete this configuration.

    - **Include specific folders and environments**
    - **Exclude specific folders and environments**
3. Click **Finish**.

Next Steps

After the Microsoft Copilot integration is complete, it appears in the **Settings > Integrations** table. From here, you can manage your integration and view the integration status.

> **Note:** By default, when you connect Microsoft Copilot, AI Exposure fetches 14 days of historical conversation data. This default varies by AI provider and can also vary depending on the complexity of your configuration. For example, when you connect Google Gemini, AI Exposure fetches 1 day of historical conversation data by default. For information about how long AI Exposure retains chats, detections, and findings after fetching them, see the **Data Retention** section in the FAQ.

Connect OpenAI ChatGPT

Use this procedure to integrate OpenAI ChatGPT with Tenable One AI Exposure to identify posture findings, activity detections, and other AI-related exposures within your organization.

Prerequisites

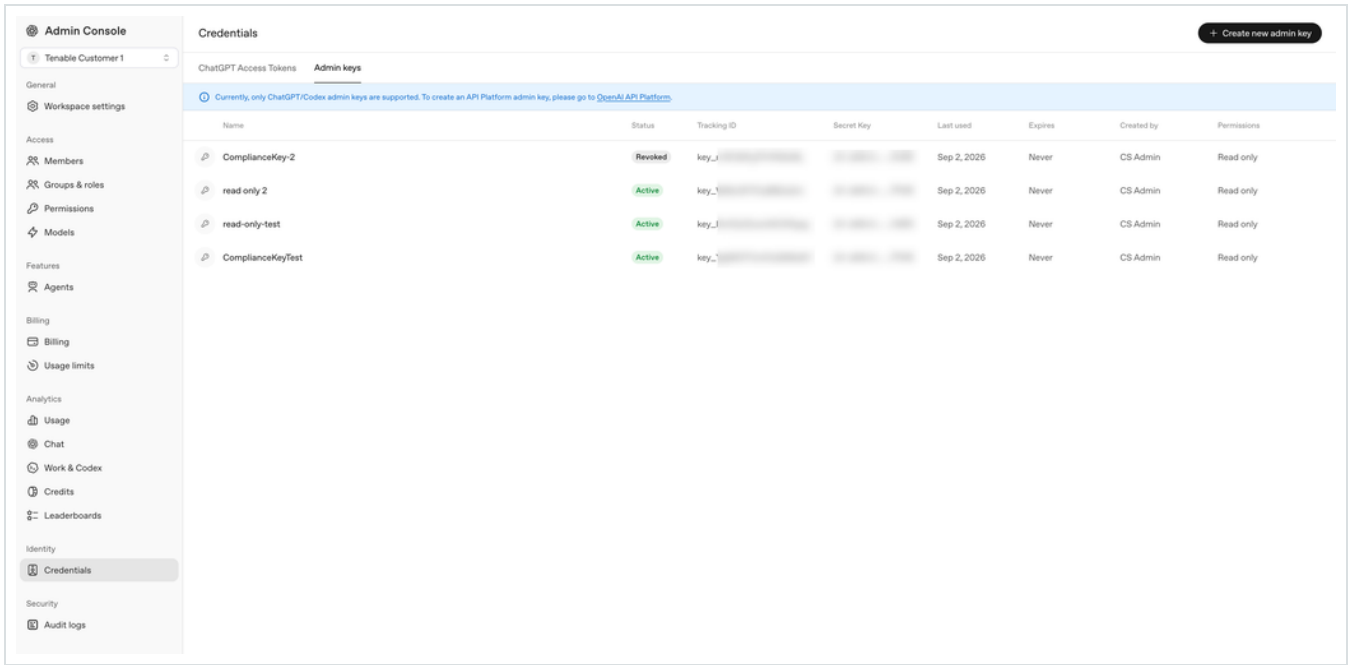
Ensure that you have:

- An Enterprise license.
- An **Owner** role in your ChatGPT workspace.

Create an Admin Key

> **Required AI Exposure User Role:** You must have the **Owner** role in your ChatGPT workspace to create an admin key.

1. Access ChatGPT Enterprise
2. Navigate to the relevant ChatGPT workspace.
3. In the left navigation bar, click **Credentials**.



4. Click the **Admin keys** tab.
5. Click **Create new admin key** and enter a name for the admin key.

6. Select the permission as **Read only**.
7. Click **Submit**.
8. Copy and save the API key.

> **Note:** You can view or copy the API key only once. Make sure you store it securely.

Locate Your Organization ID and Workspace ID

1. Access ChatGPT Enterprise.
2. Navigate to the relevant ChatGPT workspace.
3. In the left navigation bar, click **Workspace settings**.
4. From the Workspace details section, copy the **Organization ID** and **Workspace ID**.

> **Note:** The **Organization ID** and **Workspace ID** are required during the integration steps in AI Exposure. See Connect ChatGPT Enterprise.

Connect ChatGPT Enterprise

To integrate ChatGPT:

1. In AI Exposure, navigate to **Settings > Integrations** and click **Add Integration**.
2. In the Integrations Library, select **OpenAI ChatGPT**. The Add Integration wizard opens.
3. Enter a **Name** for your integration. The Console displays this name.
4. Enter your OpenAI **Organization ID**.
5. Enter the OpenAI **Workspace ID**.
6. Enter the Admin key you saved earlier.
7. Click **Finish**.

Next steps:

After you integrate ChatGPT, it appears in the table in **Settings** > **Integrations**. From here, you can manage your integration and view integration status.

Note: By default, when you connect OpenAI ChatGPT, AI Exposure fetches 14 days of historical conversation data. This default varies by AI provider and can also vary depending on the complexity of your configuration. For example, when you connect Google Gemini, AI Exposure fetches 1 day of historical conversation data by default. For information about how long AI Exposure retains chats, detections, and findings after fetching them, see the **Data Retention** section in the FAQ.

Connect Google Gemini

Use this procedure to integrate Google Gemini with Tenable One AI Exposure to monitor your environment and surface posture findings, detect activity, and identify related security risks.

Prerequisites

- Ensure you have the following:
  - Google Vault add-on license.

    Note: AI Exposure supports any Google Workspace tier that includes Google Vault, whether it is built into the plan (Business Plus or Enterprise) or purchased as an individual user add-on (Business Starter or Standard). For more information, see the Google Vault license documentation.
  - Google Gemini features enabled.

To integrate with Google Gemini:

1. In AI Exposure, navigate to **Settings > Integrations** and click **Add Integration**.
2. In the **Integrations Library**, select **Google Gemini**. The Add Integration wizard opens.
3. Enter a **Name** for your integration. The Console displays this name.
4. In the **Deployment** section, select one of the following deployment options to create a service account for Tenable:

   If you already onboarded a project from this GCP organization, the service account has already been created, and this step appears as completed.

   While not mandatory, Tenable recommends creating a dedicated project for the service account for the following reasons:

- GCP calculates API rate limits per project. Creating the service account in the same project as other service accounts increases the risk of GCP blocking your requests due to rate limits.
- Using an existing project makes it difficult to isolate usage and track costs generated by the Tenable service account.

- **Use existing** – From the drop-down list, select an existing Google Workspace integration to use its service account.
- **Cloud Shell**:
    1. In the Google Cloud Console, create a new project for Tenable.
    2. In the top right corner of the console, click the Activate Cloud Shell icon for the newly created project.
    3. Copy the script displayed in the AI Exposure wizard and run it in your Cloud Shell.
    4. Wait until the script finishes running, and then copy the **Service Account Email** from the output.
    5. In the AI Exposure wizard, go to the **Post Deployment GCP Settings** section and enter the service account email in the **Service Account Email** field.
    6. In the Google Cloud Console, navigate to **IAM & Admin > Labels**, click **+ Add label**, and add the key/value pair that appears in the AI Exposure wizard.
- **Manual**:
    1. In the Google Cloud Console, create a new project for Tenable.
    2. In the newly created project, navigate to **IAM & Admin** > **Roles** and then click **+Create Role**.
    3. Enter a **Title**, **Description**, and **ID**.
    4. Click **+ Add Permissions**, enter the following permissions in the **Filter** and click **Add**:

- `resourcemanager.projects.get`
- `serviceusage.services.enable`
- `serviceusage.services.list`

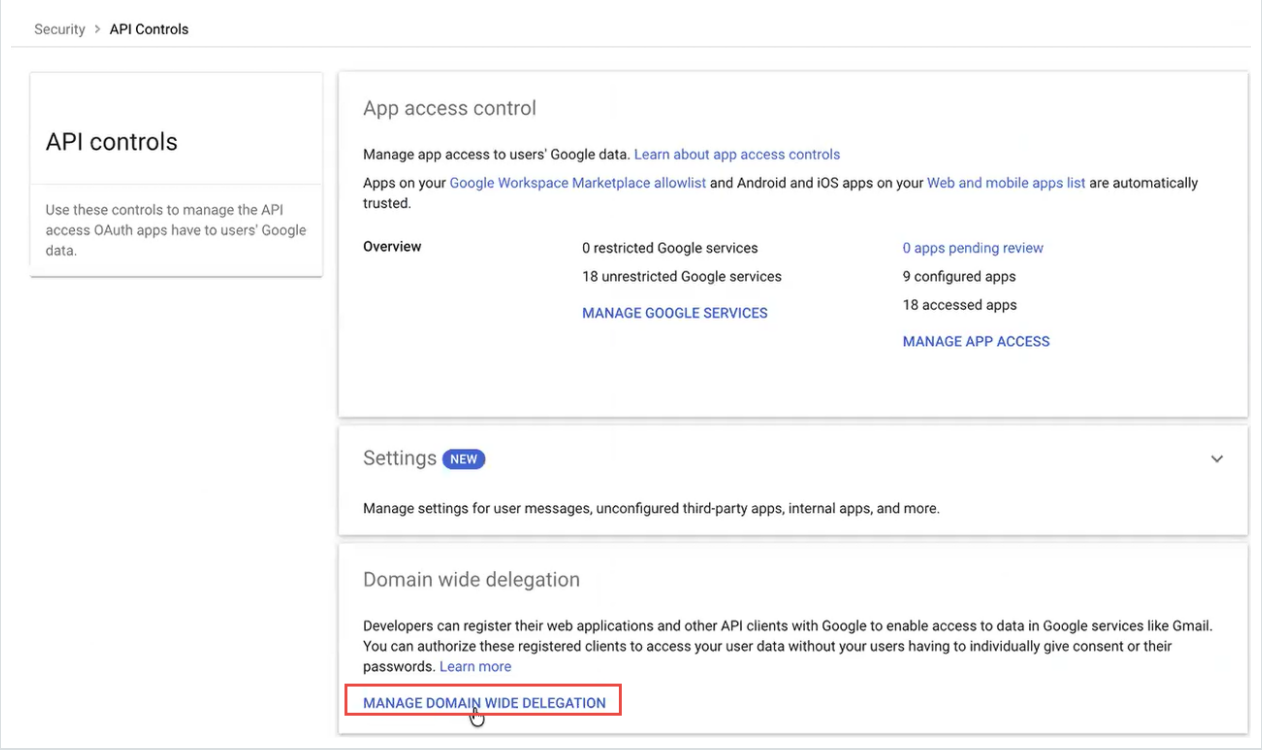
For more information about why these permissions are needed, see Google Required Permissions.

5. Click **Create** to finish creating the role.
6. Click the **Service Accounts** tab and then click **+ Create service account**.
7. Enter a **Service account name**, **ID**, and **Description**, then click **Create and continue**.
8. Select the custom role you created, click **Continue**, and then click **Done**.
9. Select the newly created service account, click the **Principals with access** tab, and then click **+ Grant access**.

   > **Important:** If you are unable to grant access, an organization policy with a domain restriction constraint that may prevent you from selecting Tenable as a principal in IAM policies. This prevents Tenable from impersonating the created service account. If this is the case, follow the procedure described in Add Tenable as an Allowed Domain.

10. In the **New principals** field, enter **ermeticapp@sil-prd.iam.gserviceaccount.com** and select the **Service Account Token Creator** role.
11. Click **Save**.
12. In the AI Exposure wizard, in the **Post Deployment GCP Settings** section, enter the service account email in the **Service Account Email** field. You can get this email ID from the **Email** field visible under **IAM & Admin** > **Service Accounts**.
13. Go to **IAM & Admin** > **Labels**, click **+ Add label**, and add the key-value pair that appears in the AI Exposure wizard.
14. Click **Save** to finish.
15. Navigate to **APIs & Services** > **Enabled APIs & services**, select **Service Usage API** and click **ENABLE**.

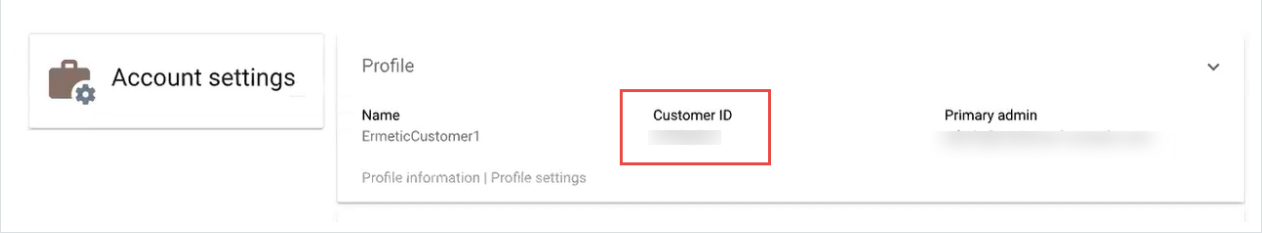
5. **Grant permissions to the Google Workspace via domain-wide delegation** : Perform these steps to generate the customer ID and admin user email.
    1. In the Google Cloud console, navigate to the service account that you created in the AI Exposure wizard.
    2. On the **Details** tab, click to expand the **Advanced settings** section.
    3. Copy the **Client ID**, and then click **View Google Workspace Admin Console**.
    4. In the Google Workspace Admin console, navigate to **Security** > **Access and data control** > **API controls**.
    5. Click **Manage Domain Wide Delegation** and then click **Add new**.



    6. Paste the **Client ID** that you copied earlier in Step 5(3).
    7. Copy and paste the following **OAuth scopes**:

```
https://www.googleapis.com/auth/apps.licensing
https://www.googleapis.com/auth/devstorage.read_only
https://www.googleapis.com/auth/drive.metadata.readonly
https://www.googleapis.com/auth/ediscovery
```

8. Click **Authorize**.
9. Navigate to **Account** > **Account settings** and copy the **Customer ID** from the Profile section.



6. In the AI Exposure wizard, in the **Post Deployment Google Workspace Settings** section, paste the **Customer ID**.
7. In the AI Exposure wizard, enter the primary administrator email address in the **Admin user email** field.
    - The user must have the *Super Admin* role
    - To assign or view users with this role, navigate to **Account** > **Admin roles**, hover over **Super Admin**, and click **Assign admin** or **View admins**.
    - AI Exposure's actual permissions are limited to the OAuth scopes you granted earlier.
8. Click **Finish**.

Next steps

After you complete the steps, the Google Gemini integration appears in the **Settings** > **Integrations** table. From this table, you can manage your integration and view the integration status.

Note: By default, when you connect Google Gemini, AI Exposure fetches 1 day of historical conversation data. This default varies by AI provider and can also vary depending on the complexity of your configuration. For example, when you connect Microsoft Copilot, AI Exposure fetches 14 days of historical conversation data by default. For information about how long AI Exposure retains chats, detections, and findings after fetching them, see the **Data Retention** section in the FAQ.

Note: Due to Google export limitations, AI Exposure syncs Google Gemini activity once daily for the preceding 24-hour window. As a result, in some cases, a Gemini activity event may take up to 48 hours to appear in AI Exposure.

Data Synchronization Limitations

AI Exposure synchronizes Google Gemini data through Google Vault exports rather than a Gemini API. As a result, some Gemini content does not appear in the AI Exposure console.

Gems

- AI Exposure synchronizes a Gem only after you save it to Google Drive and share it. Gems that are not saved and shared do not appear.
- Knowledge files attached to a Gem appear in the Gem's profile only if you add them from Google Drive. AI Exposure does not synchronize files uploaded directly from a local computer or files not saved in Google Drive.

Conversations

- AI Exposure does not synchronize files uploaded during a Gemini conversation. Google Vault excludes these files from exports, including file names and indicators that a file was attached.
- If your prompt contains only an uploaded file, the message appears without content. AI Exposure still synchronizes the full response from Gemini.
- AI Exposure does not scan conversation file attachments for sensitive data. However, if Gemini copies text from an uploaded file into its response, AI Exposure analyzes that text, which can trigger security detections.

Connect Anthropic Claude

Use this procedure to integrate Anthropic Claude with Tenable One AI Exposure to monitor all conversations with Claude and surface posture findings, activity detections, and related security risks.

Prerequisites

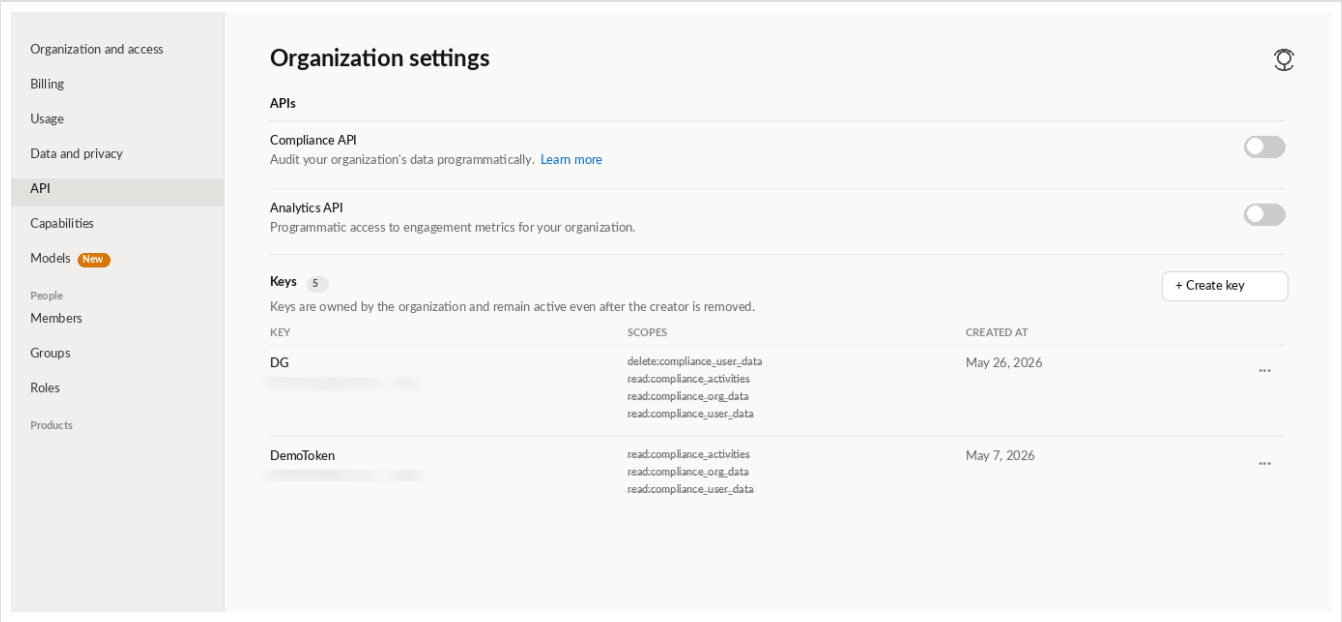
Ensure that you have:

- An active **Claude Enterprise** plan.
- The **Primary Owner** role in Claude Enterprise.

Note: You must be a **Primary Owner** to enable the **Compliance API**.

Create the Compliance API Key

1. In Claude Enterprise, navigate to **Organization settings** > **API**.



2. (**Primary Owner**) In the **APIs** section, enable the **Compliance API** access toggle.
3. (**Primary Owner** or **Organization Owner**) In the **Keys** section, click **Create Key** to create new compliance access keys.

   The **Create API Key** window appears.
4. Select the following scopes:
   - *read:compliance_activities*
   - *read:compliance_org_data*
   - *read:compliance_user_data*
5. Click **Create**.

   The system generates a unique API key.
6. Save the generated API key for use with the integration.

For more information, see Access the Compliance API in the Claude Enterprise User documentation.

Connect Anthropic Claude

To integrate Claude:

1. In AI Exposure, navigate to **Settings > Integrations** and click **Add Integration**.
2. In the **Integrations Library**, select **Anthropic Claude**.
   The Add Integration wizard opens.
3. Enter a **Name** for your integration.
   The Console displays this name.
4. Enter your **Compliance API Key**.
5. Click **Finish**.

Next steps:
After you integrate Claude, it appears in the **Settings** > **Integrations** table. From here, you can manage your integration and view the integration status.

> **Note:** By default, when you connect Anthropic Claude, AI Exposure fetches 14 days of historical conversation data. This default varies by AI provider and can also vary depending on the complexity of your configuration. For example, when you connect Google Gemini, AI Exposure fetches 1 day of historical conversation data by default. For information about how long AI Exposure retains chats, detections, and findings after fetching them, see the **Data Retention** section in the FAQ.

Connect Homegrown AI Applications

Tenable One AI Exposure monitors custom-built homegrown AI applications (such as chatbots, copilots, and agents), whether they connect directly to a self-hosted model, a third-party LLM API, or a custom orchestration layer.

To integrate a homegrown application, you connect it to AI Exposure through an API and configure it to send prompts and responses to the platform as they occur.
AI Exposure structures these messages into conversations to provide context and visibility. The

platform then analyzes these messages for risk and surfaces activity detections in your console, in the same way it monitors managed cloud AI services.

> **Note:** The Homegrown AI application feature is currently available at no additional cost with the AI Governance add-on. Tenable will notify you before this feature becomes billable.

Prerequisites

Ensure that you have the following:

- A Tenable One Foundation or Advanced license for AI Exposure with an AI Governance add-on license.
- **Required permissions**:
  - Permissions to manage integrations in AI Exposure.
  - The **AI Conversation** permission, to view conversations in the console.
- The ability to modify the application code, so you can add minimal instrumentation where the application processes prompts and responses to send that activity to AI Exposure.

Step 1: Create an Integration for a Homegrown AI Application

You can use a single integration for one or more homegrown AI applications.

To create a homegrown AI application integration:

1. In the AI Exposure console, go to **Settings** > **Integrations** > **Add Integration**.
2. In the **Integrations Library**, select **Homegrown AI Application**.
   The **Create Homegrown AI Application** wizard opens.
3. Enter a **Name** for your integration.
   The console displays this name.

   > **Note:** The name need not be application-specific. You can use the same API authentication key for multiple homegrown applications.

4. Click **Finish**.

   AI Exposure creates the Homegrown AI Application integration and displays the following details:

   - **Account ID** – The integration ID, which the application includes in every request.
   - **API URL** – The endpoint to which your application sends the data.
   - **Secret** – The API key required to authenticate the request.

     > **Caution:** Before you close the window, make sure that you copy the **Secret** and store it securely. You cannot view it again once the window is closed.

5. Click **Done**.

> **Note:** When you create a new integration, it is automatically assigned to the **Homegrown AI Applications** scope. Each integration is treated as its own tenant.

Step 2: Authenticate API Requests

Store the **Secret** securely in your application. Include it as a bearer token in the `Authorization` header of every request (including mutations and queries) that you send to the API URL:

```
Authorization: Bearer <secret>
```

- `secret` – The secret API key generated when you created the integration.

Step 3: Send Conversation Data from Your AI Application

Your homegrown AI application sends three types of messages to the API: prompts (user input), responses (model output), and system prompts.

The application uses the `InsertHomegrownAiApplicationMessages` mutation to send prompts and responses to the AI Exposure platform, which reconstructs the individual messages into complete conversations for visibility and investigation, and also inspects them for risks.

Request Parameters

The mutation accepts the following request-level fields in `input`:

Field	Required	Description
`AccountId`	Yes	The account (integration) to which the messages belong.
`Messages`	Yes	An array of message objects. The array must contain at least one message. Otherwise, the API returns the error `Messages cannot be empty`. See the message object fields below.

Message Object Fields

Each object in `Messages` includes the following fields:

Field	Required	Description
`ApplicationName`	Yes	Label that identifies which application sent this message. This is useful for correlating conversations with a specific application, especially when an integration contains multiple applications.
`ConversationId`	Yes	A stable identifier that groups messages belonging to the same conversation or session.
`ConversationName`	No	A human-readable name for the conversation that appears in the console.
`Content`	Yes	The text of the prompt, response, or system prompt.
`Type`	Yes	The message type: `Prompt` for user input, `Response` for model output, or `SystemPrompt` for the system-level instructions.
`Time`	Yes	The timestamp when the prompt or response

Field	Required	Description
		occurred in your application. Format: ISO-8601, for example, `2026-09-28T14:03:00Z`.
`ModelName`	No	The model that generated the response, for example, "gpt-4o".
`Identity`	No	The end user or service behind the message. An object with `Name` and `Id` fields. If you send `Identity`, `Id` is required.
`ExternalId`	No	Your identifier for the message. The API returns this identifier in the response so you can correlate it with your own records.

Note: The response includes a server-assigned `Id` and the `ExternalId` for each message. Save these identifiers to review the message analysis results later.

Example Request (GraphQL)

MUTATION

```
InsertHomegrownAiApplicationMessages(
  input: {
    AccountId: "<accountId>"
    Messages: [
      {
        ApplicationName: "Support Chatbot"
        ConversationId: "conv-12345"
        ConversationName: "Password reset help"
        ExternalId: "msg-001"
        Identity: { Id: "user-789", Name: "Jane Doe" }
        ModelName: "gpt-4o"
        Time: "2026-09-30T10:15:00Z"
        Type: Prompt
        Content: "How do I reset my password?"
      }
```

```
        {
          ApplicationName: "Support Chatbot"
          ConversationId: "conv-12345"
          ExternalId: "msg-002"
          ModelName: "gpt-4o"
          Time: "2026-09-30T10:15:03Z"
          Type: Response
          Content: "Go to Settings > Security and click Reset Password."
        }
      ]
    }
  ) {
    Messages {
      ExternalId
      Id
    }
  }
}
```

Step 4: Retrieve Analysis Results (Optional)

You can query analysis results via API or view them directly in the console. To query analysis results using the API, use the `GetHomegrownAiApplicationMessageResult` query.

Request Parameters

Field	Required	Description
`Id`	Yes	The message ID received from the `InsertHomegrownAiApplicationMessages` mutation response.

Response Fields

The API response returns:

- `Id` – The message ID from the original message.
- `Status` – The analysis status, which progresses from `Pending` to `InProgress` to `Completed`, or to `Failed` if the analysis does not complete successfully.

- `Detections` – When the `Status` changes to `Completed`, this field lists anything flagged for that message.

  Each detection includes:

  - `Id` – The detection ID.
  - `ContentType` – The type of content that triggered the detection.
  - `Rule` – The name of the matched rule.
  - `RuleId` – The ID of the matched rule.
  - `Severity` – The severity level of the detection.
  - `Evidence` – The content that supports the detection.

> **Note:** If the analysis finds no risks in the message, the `Detections` field is empty.

Example Request (GraphQL)

GraphQL

```
query {
  GetHomegrownAiApplicationMessageResult(Id: "<message-id>") {
    Id
    Status
    Detections {
      Id
      ContentType
      Rule
      RuleId
      Severity
      Evidence
    }
  }
}
```

Step 5: Verify the Integration

To confirm the integration is working correctly:

- Send a few test messages from your application.
- Sign in to the AI Exposure console and go to the **Conversations** page. After a short processing delay, the test conversations appear in the console.

  > **Note:** You must have the **AI Conversation** permission to view the **Conversations** page.

- If data does not appear in the console, confirm the following items:
  - The `Authorization` header is present and includes the correct secret.
  - The `AccountId` matches your integration.
  - Each message includes all required fields: `ApplicationName`, `Content`, `ConversationId`, `Time`, and `Type`.

View Analysis Results in the Console

After AI Exposure processes the messages, you can view the results from the analysis in the AI Exposure console on these pages:

- **AI Activity Detections** – Shows individual detections. Each detection shows the content type (for example, exposed credentials, PII, or jailbreak attempt), its severity, the identity that triggered it, and a link to the full conversation for context. For more information, see AI Activity Detections.
- **AI Activity Issues** – Shows related detections grouped together so recurring or related issues can be triaged as a single unit. For more information, see AI Activity Issues.
- **Conversations** – Shows the reconstructed prompt or response history behind any detection. To view conversations, you must have the **AI Conversation** permission. For more information, see AI Conversations.

AWS

AWS Overview

Connect your entire AWS organization or individual accounts in Tenable One AI Exposure to get full visibility and risk assessment for all cloud identities and resources associated with the organization/account, including information about permissions, account usage, and security configurations. Tenable collects inventory and configuration data from AWS API, and activity data from AWS CloudTrail logs.

- Connect an AWS Account
- Connect an AWS Organization

After connecting, AI Exposure displays a status for each account, indicating, for example, whether Tenable can connect to the account, and helping you troubleshoot potential connection issues.

See Account Architecture for a visual overview of the IAM trust relationship that is established, including required permissions. See AWS FAQ and Troubleshooting for a list of frequently asked questions related to connecting AWS.

Considerations for Connecting an Organization versus Individual Accounts

When deciding whether to connect your entire AWS organization as opposed to individual accounts, it's important to consider how this decision impacts features in AI Exposure. Tenable recommends connecting your entire organization to ensure that the management account is connected to Tenable, and to avoid losing visibility related to the following features/capabilities:

- **AWS Identity Center (formerly AWS SSO)** - *Affects visibility into users, groups, permission sets, and their effective use, as well as least-privilege recommendations.*
- **Service control policy (SCP) and Resource control policy (RCP)** - *Limited entitlement visibility.*
- **Cross account visibility** - *Tenable wont be able to differentiate between accounts that are part of your organization (but not connected) and those that are not.*
- **Least privilige** - *Tenable wont be able to provide the most accurate recommendations.*

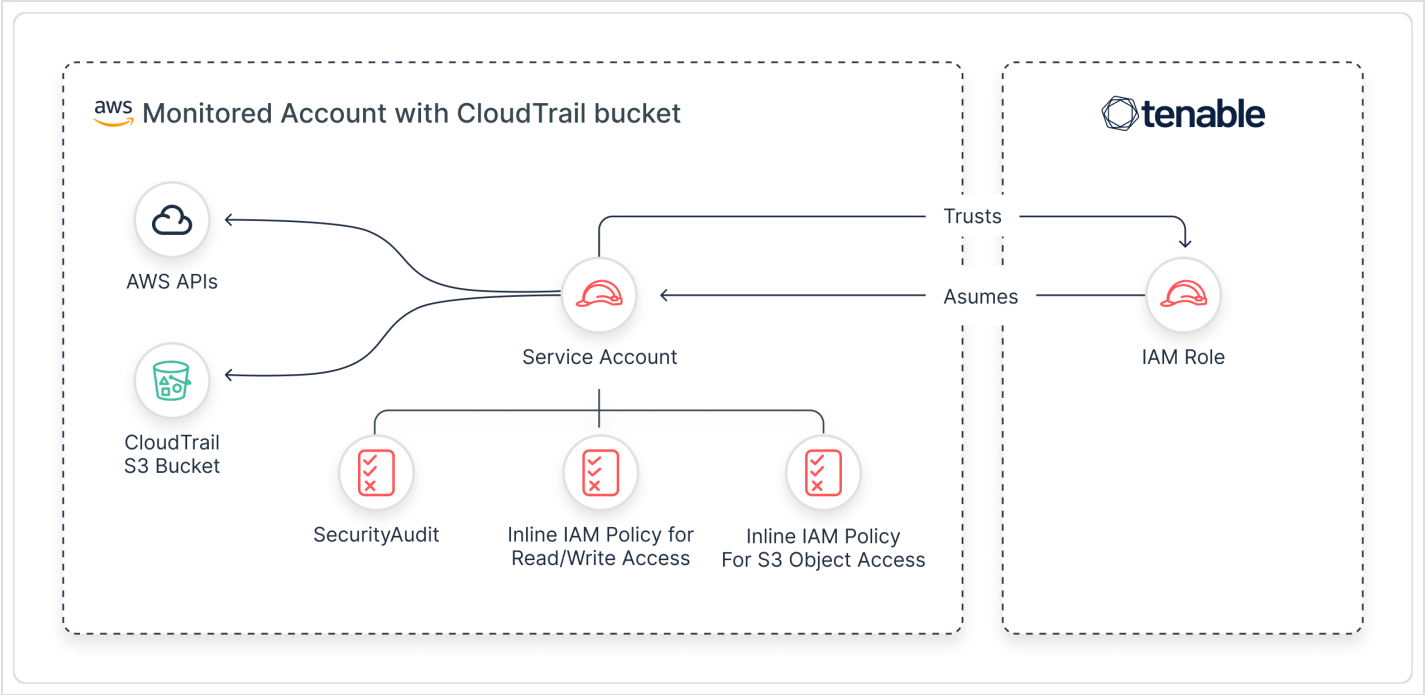
Account Architecture

Accounts with Monitoring/Remediation Permissions

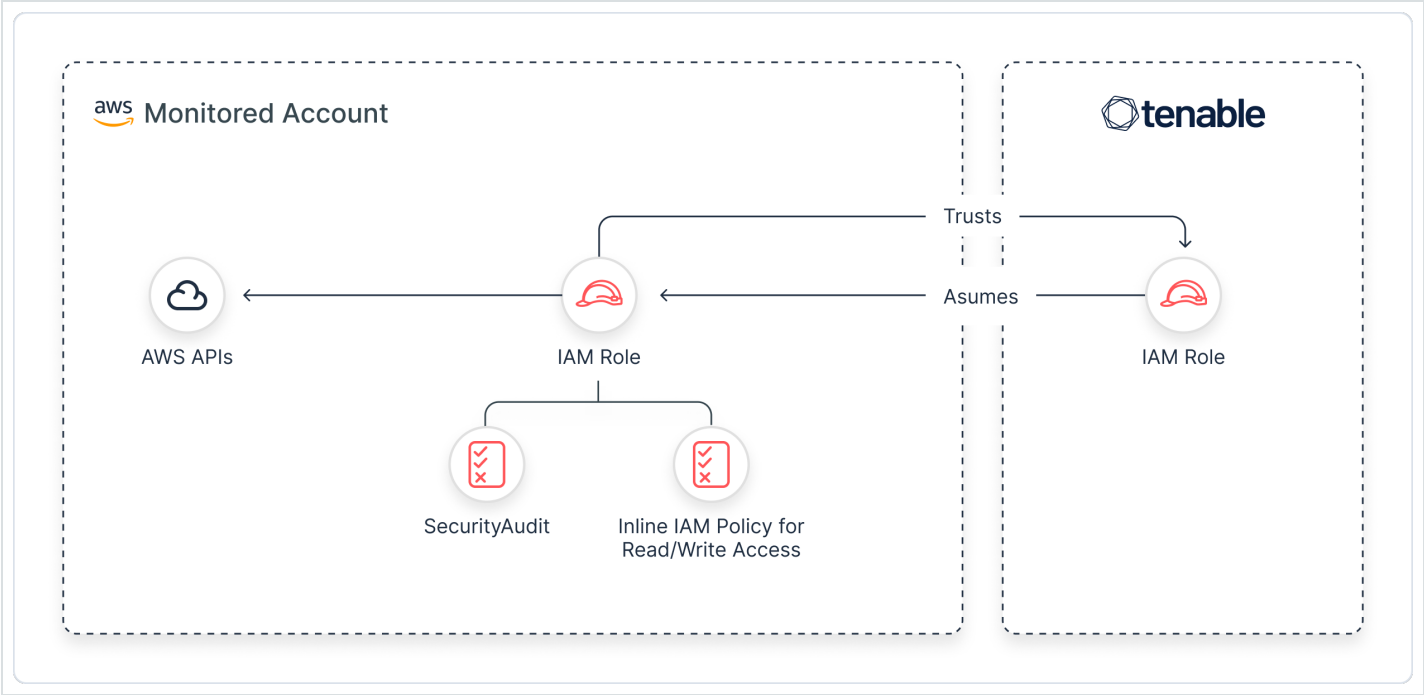
The following diagrams outline the architecture for accounts with Monitoring/Remediation permissions, highlighting the differences between accounts that are connected to a CloudTrail and those that aren't. See AWS CloudTrail for more information.

These diagrams show the trust relationship established between the IAM role associated with the account you connected, and AI Exposure, which uses its own IAM role to interact with and collect data from your environment via granted permissions.

CloudTrail Connected



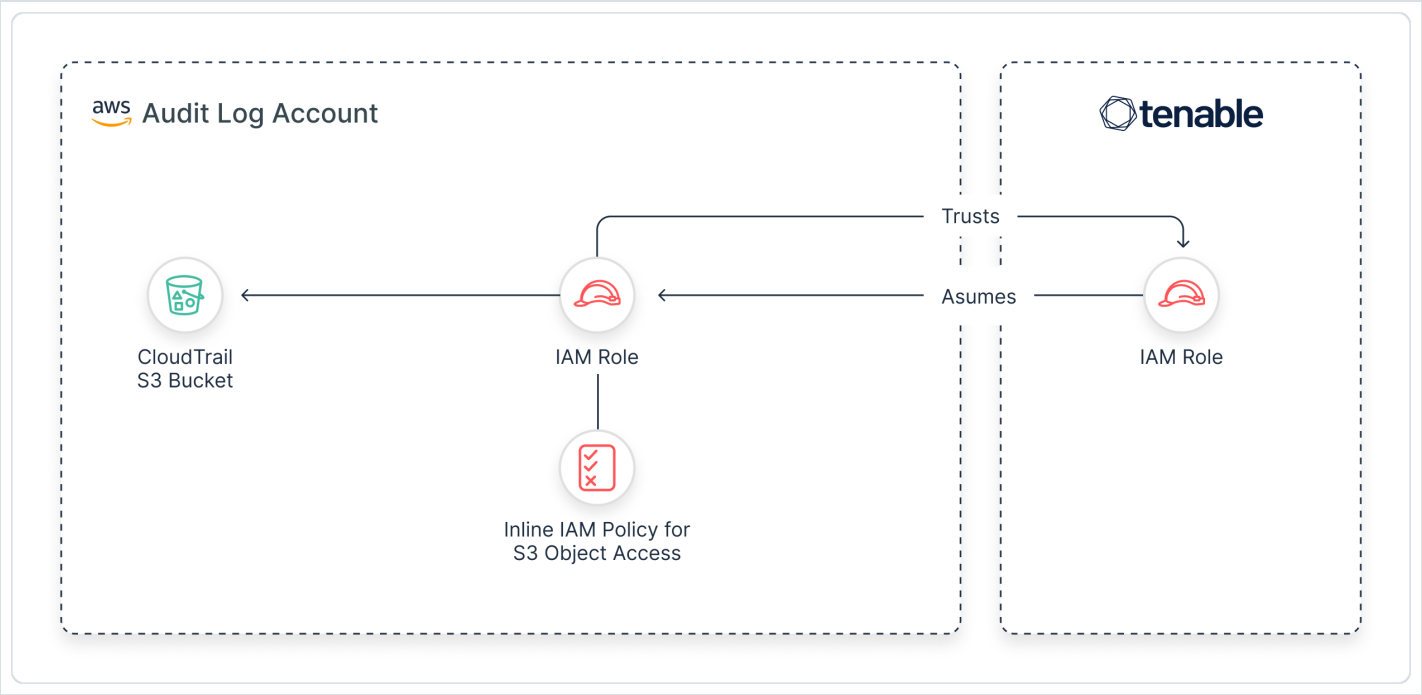
No CloudTrail Connected



Accounts with CloudTrail Permissions

This diagram shows the trust relationship established between the IAM role associated with the account you connect, and AI Exposure, which uses its own IAM role to interact with and collect data from your connected AWS accounts.

Note: An *audit log account* is an account where only **CloudTrail** permissions were enabled/granted, without **Monitoring** permissions. Such an account is dedicated to collecting activity logs and will not be monitored for security purposes . Although AI Exposure supports connecting accounts in such a way, it is recommended to connect all accounts with **Monitoring** permissions, to provide full security visibility for your cloud assets.



AWS Required Permissions

To provide full visibility into your account, Tenable One AI Exposure needs to collect relevant metadata using both an AWS-managed policy and an inline policy that are attached to the dedicated role you create for Tenable in IAM when you connect an account or organization:

- **Monitoring** permissions:
  - **SecurityAudit** permissions. AWS-managed policy, which grants access to read security configuration metadata.
  - Custom Tenable Monitoring permissions (read-only). Inline policy, which grants Tenable additional read-only permissions not included in the SecurityAudit policy.

    To learn more about why Tenable needs both the SecurityAudit policy and a custom, inline policy, see Need for Both Custom Policy and SecurityAudit Policy.
- (Optional) Custom Tenable **Remediation** permissions (read-write). Inline policy, which grants Tenable management permissions, allowing Tenable to make changes in your environment. For example, this allows Tenable to automatically remediate findings directly in AWS (If you

choose not to grant management permissions, you can still manually remediate findings by providing one-time credentials on demand).

- **CloudTrail (S3)** permissions. See AWS CloudTrail for more information.

If you use service control policies (SCPs) or resource control policies (RCPs) in your AWS organization, make sure to add exclusions to any existing SCP or RCP to ensure that the dedicated IAM role you create for AI Exposure is not included. See Access to Us-East-1 Region for more information.

Appendix I: AWS IAM Policies

- Tenable Monitoring Policy (Read-Only)
- Tenable Remediation Policy (Read-Write)
- CloudTrail Policy
- Data Resources Scanning Policy (Data Protection)
- EC2 Instance Scanning Workload Protection Policy
- ECR Scanning Workload Protection Policy
- Terraform Policy
- Amazon Bedrock Invocation Logging
- JIT Policy for AWS Account Access
- JIT Policy for Application Access

Tenable Monitoring Policy (Read-Only)

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "acm:Describe*",
        "acm:List*",
        "aoss:BatchGet*",
```

```
            "aoss:List*",
            "appsync:List*",
            "athena:GetWorkGroup",
            "athena:List*",
            "autoscaling:Describe*",
            "batch:Describe*",
            "batch:List*",
            "bedrock:Get*",
            "bedrock:List*",
            "bedrock-agentcore:GetAgentRuntime",
            "bedrock-agentcore:GetAgentRuntimeEndpoint",
            "bedrock-agentcore:GetApiKeyCredentialProvider",
            "bedrock-agentcore:GetGateway",
            "bedrock-agentcore:GetGatewayTarget",
            "bedrock-agentcore:GetHarness",
            "bedrock-agentcore:GetMemory",
            "bedrock-agentcore:GetOauth2CredentialProvider",
            "bedrock-agentcore:GetPaymentCredentialProvider",
            "bedrock-agentcore:GetWorkloadIdentity",
            "bedrock-agentcore:ListWorkloadIdentities",
            "bedrock-agentcore:ListApiKeyCredentialProviders",
            "bedrock-agentcore:ListOauth2CredentialProviders",
            "cloudformation:Describe*",
            "cloudformation:Get*",
            "cloudformation:List*",
            "cloudfront:Get*",
            "cloudfront:ListDistributions*",
            "cloudtrail:Describe*",
            "cloudtrail:Get*",
            "cloudtrail:List*",
            "cloudtrail:LookupEvents",
            "cloudwatch:Describe*",
            "cloudwatch:GetMetric*",
            "cloudwatch:ListMetrics",
            "codebuild:BatchGet*",
            "codebuild:List*",
            "cognito-idp:ListResourcesForWebACL",
            "cognito-identity:Describe*",
            "cognito-identity:List*",
            "cognito-idp:List*",
            "cognito-sync:GetCognitoEvents",
            "config:Describe*",
            "dax:Describe*",
            "directconnect:Describe*",
            "dms:Describe*",
            "docdb-elastic:Get*",
            "docdb-elastic:List*",
```

```
            "dynamodb:Describe*",
            "dynamodb:GetResourcePolicy",
            "dynamodb:List*",
            "ec2:Describe*",
            "ec2:GetTransitGatewayRouteTablePropagations",
            "ec2:SearchTransitGatewayRoutes",
            "ecr:Describe*",
            "ecr:GetRegistryScanningConfiguration",
            "ecr:GetRepositoryPolicy",
            "ecr:List*",
            "ecr:StartImageScan",
            "ecr-public:Describe*",
            "ecr-public:GetRepositoryPolicy",
            "ecr-public:List*",
            "ecs:Describe*",
            "ecs:List*",
            "eks:Describe*",
            "eks:List*",
            "elasticache:Describe*",
            "elasticache:List*",
            "elasticbeanstalk:Describe*",
            "elasticbeanstalk:List*",
            "elasticfilesystem:Describe*",
            "elasticloadbalancing:Describe*",
            "elasticmapreduce:Describe*",
            "elasticmapreduce:List*",
            "es:Describe*",
            "es:List*",
            "events:ListRules",
            "firehose:Describe*",
            "firehose:List*",
            "glue:BatchGet*",
            "glue:Get*",
            "glue:List*",
            "guardduty:GetDetector",
            "guardduty:ListDetectors",
            "iam:Generate*",
            "iam:Get*",
            "iam:List*",
            "identitystore:Describe*",
            "identitystore:List*",
            "inspector2:List*",
            "iot:GetTopicRule",
            "kafka:ListClustersV2",
            "kms:Describe*",
            "kms:GetKey*",
            "kms:List*",
```

```
            "kinesis:Describe*",
            "kinesis:List*",
            "lambda:Get*Policy",
            "lambda:GetAccountSettings",
            "lambda:List*",
            "logs:Describe*",
            "mq:DescribeBroker",
            "mq:ListBrokers",
            "organizations:Describe*",
            "organizations:List*",
            "rds:Describe*",
            "rds:List*",
            "redshift:Describe*",
            "redshift:List*",
            "redshift-serverless:List*",
            "route53:Get*",
            "route53:List*",
            "route53domains:Get*",
            "route53domains:List*",
            "route53resolver:Get*",
            "route53resolver:List*",
            "s3:Describe*",
            "s3:GetAccessPoint*",
            "s3:GetAccountPublicAccessBlock",
            "s3:GetBucket*",
            "s3:GetEncryptionConfiguration",
            "s3:GetJobTagging",
            "s3:GetLifecycleConfiguration",
            "s3:ListAccessPoints",
            "s3:ListAllMyBuckets",
            "s3:ListBucketVersions",
            "s3:ListJobs",
            "s3:ListTagsForResource",
            "sagemaker:Describe*",
            "sagemaker:List*",
            "secretsmanager:Describe*",
            "secretsmanager:GetResourcePolicy",
            "secretsmanager:List*",
            "sns:Get*",
            "sns:List*",
            "sqs:Get*",
            "sqs:List*",
            "ssm:Describe*",
            "ssm:List*",
            "sso:Describe*",
            "sso:Get*",
            "sso:List*",
```

```
        "sso-directory:List*",
        "sso-directory:Search*",
        "states:List*",
        "sts:DecodeAuthorizationMessage",
        "tag:Get*",
        "timestream:List*",
        "timestream:Get*",
        "timestream:Describe*",
        "wafv2:Get*",
        "wafv2:List*"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "arn:aws:s3:::elasticbeanstalk-*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "apigateway:GET",
        "apigateway:ListRoutingRules"
      ],
      "Resource": [
        "arn:aws:apigateway:*::/apis",
        "arn:aws:apigateway:*::/apis/*/authorizers",
        "arn:aws:apigateway:*::/apis/*/integrations",
        "arn:aws:apigateway:*::/apis/*/routes",
        "arn:aws:apigateway:*::/domainnames",
        "arn:aws:apigateway:*::/domainnames/*/basepathmappings",
        "arn:aws:apigateway:*:*:/domainnames/*/routingrules/*",
        "arn:aws:apigateway:*::/restapis",
        "arn:aws:apigateway:*::/restapis/*/authorizers",
        "arn:aws:apigateway:*::/restapis/*/resources",
        "arn:aws:apigateway:*::/restapis/*/stages"
      ]
    }
  ]
}
```

Tenable Remediation Policy (Read-Write)

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteSecurityGroup",
        "ec2:ModifyInstanceMetadataOptions",
        "ec2:ModifyVpcEndpoint",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ecr:DeleteRepositoryPolicy",
        "ecr:SetRepositoryPolicy",
        "iam:AddUserToGroup",
        "iam:AttachGroupPolicy",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:CreatePolicy",
        "iam:CreatePolicyVersion",
        "iam:DeactivateMFADevice",
        "iam:DeleteAccessKey",
        "iam:DeleteGroup",
        "iam:DeleteGroupPolicy",
        "iam:DeleteLoginProfile",
        "iam:DeletePolicy",
        "iam:DeletePolicyVersion",
        "iam:DeleteRole",
        "iam:DeleteRolePermissionsBoundary",
        "iam:DeleteRolePolicy",
        "iam:DeleteServerCertificate",
        "iam:DeleteServiceSpecificCredential",
        "iam:DeleteSigningCertificate",
        "iam:DeleteSSHPublicKey",
        "iam:DeleteUser",
        "iam:DeleteUserPermissionsBoundary",
        "iam:DeleteUserPolicy",
        "iam:DetachGroupPolicy",
        "iam:DetachRolePolicy",
        "iam:DetachUserPolicy",
        "iam:PutGroupPolicy",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:RemoveRoleFromInstanceProfile",
```

```
        "iam:RemoveUserFromGroup",
        "iam:UpdateAccessKey",
        "iam:UpdateAssumeRolePolicy",
        "s3:DeleteBucketPolicy",
        "s3:PutBucketPolicy",
        "secretsmanager:DeleteResourcePolicy",
        "secretsmanager:PutResourcePolicy",
        "sso:DeleteAccountAssignment",
        "sso:DeleteInlinePolicyFromPermissionSet",
        "sso:DeletePermissionSet",
        "sso:DetachManagedPolicyFromPermissionSet",
        "sso:ProvisionPermissionSet",
        "sso:PutInlinePolicyToPermissionSet"
      ],
      "Resource": "*"
    }
  ]
}
```

CloudTrail Policy

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowS3LogAccess",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::YOUR_CLOUDTRAIL_BUCKET_NAME",
        "arn:aws:s3:::YOUR_CLOUDTRAIL_BUCKET_NAME/*"
      ]
    },
    {
      "Sid": "AllowKMSDecrypt",
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "arn:aws:kms:REGION:ACCOUNT_ID:key/KMS_KEY_UUID"
    }
  ]
}
```

Data Resources Scanning Policy (Data Protection)

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:Scan",
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:Encrypt",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "rds:CopyDBClusterSnapshot",
        "rds:CopyDBSnapshot",
        "rds:CreateDBClusterSnapshot",
        "rds:CreateDBSnapshot",
        "rds:ModifyDBClusterSnapshotAttribute",
        "rds:ModifyDBSnapshotAttribute",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "rds:AddTagsToResource",
      "Resource": [
        "arn:aws:rds:*:*:snapshot:*",
        "arn:aws:rds:*:*:cluster-snapshot:*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/TenableContext": "DataAnalysis"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "rds:DeleteDBSnapshot",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
```



```
            "rds:snapshot-tag/TenableContext": "DataAnalysis"
          }
        }
      },
      {
        "Effect": "Allow",
        "Action": "rds:DeleteDBClusterSnapshot",
        "Resource": "*",
        "Condition": {
          "StringEquals": {
            "rds:cluster-snapshot-tag/TenableContext": "DataAnalysis"
          }
        }
      }
    ]
  }
```

EC2 Instance Scanning (Workload Protection)

In the below IAM policy, the `ec2:CopySnapshot` appears three times. Each of these entries is required for a different purpose:

1. **Copy with Request Tag** (Condition: `aws:RequestTag/ErmeticContext`)
    - Allows copying a snapshot only if a specific request tag is provided.
    - Ensures that the destination snapshot is automatically tagged.
    - **Use case** – Instances and AMIs where tagging of new snapshots is required.
2. **Copy any Snapshot as Source** (`Resource: arn:aws:ec2:*::snapshot/snap-*`)
    - Allows using any existing snapshot as a source for copying.
    - **Use case** – Private AMIs that need to copy an existing snapshot.
3. **Copy with Resource Tag** (Condition: `aws:ResourceTag/ErmeticContext`)
    - Allows copying snapshots that already have a specific resource tag.
    - **Use case** – Instances where only snapshots with a specific tag are permitted for copying.

For more details on AWS's handling of source vs destination snapshots in IAM statements, see: Enhancing Resource-Level Permissions for Copying Amazon EBS Snapshots.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateSnapshot",
      "Resource": "arn:aws:ec2:*:*:volume/*"
    },
    {
      "Effect": "Allow",
      "Action": "kms:CreateAlias",
      "Resource": "arn:aws:kms:*:*:alias/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CopySnapshot",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "kms:CreateKey",
        "kms:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/ErmeticContext": "WorkloadAnalysis"
        }
      }
    },
    {
      "Effect": "Deny",
      "Action": "kms:TagResource",
      "Resource": "*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/ErmeticContext": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CopySnapshot",
      "Resource": "arn:aws:ec2:*::snapshot/snap-*"
    },
    {
```

```
      "Effect": "Allow",
      "Action": [
        "ec2:CopySnapshot",
        "ec2:DeleteSnapshot",
        "ec2:ModifySnapshotAttribute",
        "kms:CreateAlias",
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:EnableKeyRotation",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:ReEncryptFrom",
        "kms:ReEncryptTo",
        "kms:RevokeGrant",
        "kms:ScheduleKeyDeletion"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/ErmeticContext": "WorkloadAnalysis"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:Decrypt",
        "kms:ReEncryptFrom"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:ViaService": "ec2.*.amazonaws.com"
        }
      }
    }
  ]
}
```

ECR Scanning Workload Protection Policy

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": [
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer",
        "ecr:BatchGetImage"
      ],
      "Resource": "*"
    }
  ]
}
```

Terraform Policy

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::<bucket_name>",
        "arn:aws:s3:::<bucket_name>/*",
      ]
    }
  ]
}
```

Where `<bucket_name>` is the name of the relevant S3 bucket.

Amazon Bedrock Invocation Logging

> **Note:** The policy below should include every Amazon S3 bucket and every AWS KMS key that Amazon Bedrock uses as a logging destination, across all regions you monitor.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::bucketName",
        "arn:aws:s3:::bucketName/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "kms:Decrypt",
      "Resource": "bucketKeyArn"
    }
  ]
}
```

Where <bucketName> is the name of the relevant S3 bucket.

JIT Policy for AWS Account Access

Use these policies to allow Tenable One AI Exposure to manage JIT access to AWS accounts and permission sets through AWS Identity Center.

Use only one policy per environment, depending on whether AWS Identity Center is managed directly from the Management Account for Account Access or via a Delegated Administrator Account for Account Access.

Management Account for Account Access

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
```



```
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListRoles",
                "iam:ListPolicies"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:GetRole",
                "iam:ListAttachedRolePolicies",
                "iam:ListRolePolicies",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetSAMLProvider",
                "iam:UpdateSAMLProvider"
            ],
            "Resource": "arn:aws:iam::*:saml-provider/AWSSSO_*_DO_NOT_DELETE"
        },
        {
            "Effect": "Allow",
            "Action": [
                "identitystore:Describe*",
                "identitystore:List*",
                "sso:AttachManagedPolicyToPermissionSet",
                "sso:CreateAccountAssignment",
                "sso:CreatePermissionSet",
                "sso:DeleteAccountAssignment",
                "sso:DeletePermissionSet",
                "sso:Describe*",
                "sso:DetachManagedPolicyFromPermissionSet",
                "sso:Get*",
                "sso:List*",
                "sso:ProvisionPermissionSet",
                "sso:PutInlinePolicyToPermissionSet",
                "sso-directory:List*",
                "sso-directory:Search*"
```

```
            ],
            "Resource": "*"
        }
    ]
}
```

Delegated Administrator Account for Account Access

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sso:AttachManagedPolicyToPermissionSet",
                "sso:CreateAccountAssignment",
                "sso:CreatePermissionSet",
                "sso:DeleteAccountAssignment",
                "sso:DeletePermissionSet",
                "sso:DetachManagedPolicyFromPermissionSet",
                "sso:ProvisionPermissionSet",
                "sso:PutInlinePolicyToPermissionSet"
            ],
            "Resource": "*"
        }
    ]
}
```

JIT Policy for Application Access

Use these policies to allow Tenable One AI Exposure to manage JIT access to applications managed by AWS Identity Center.

Use only one policy per environment, depending on whether AWS Identity Center is managed directly from the Management Account for Application Access or via a Delegated Administrator Account for Application Access.

Management Account for Application Access

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "identitystore:Describe*",
        "identitystore:List*",
        "sso:CreateApplicationAssignment",
        "sso:DeleteApplicationAssignment",
        "sso:Describe*",
        "sso:Get*",
        "sso:List*",
        "sso-directory:List*",
        "sso-directory:Search*"
      ],
      "Resource": "*"
    }
  ]
}
```

Delegated Administrator Account for Application Access

JSON

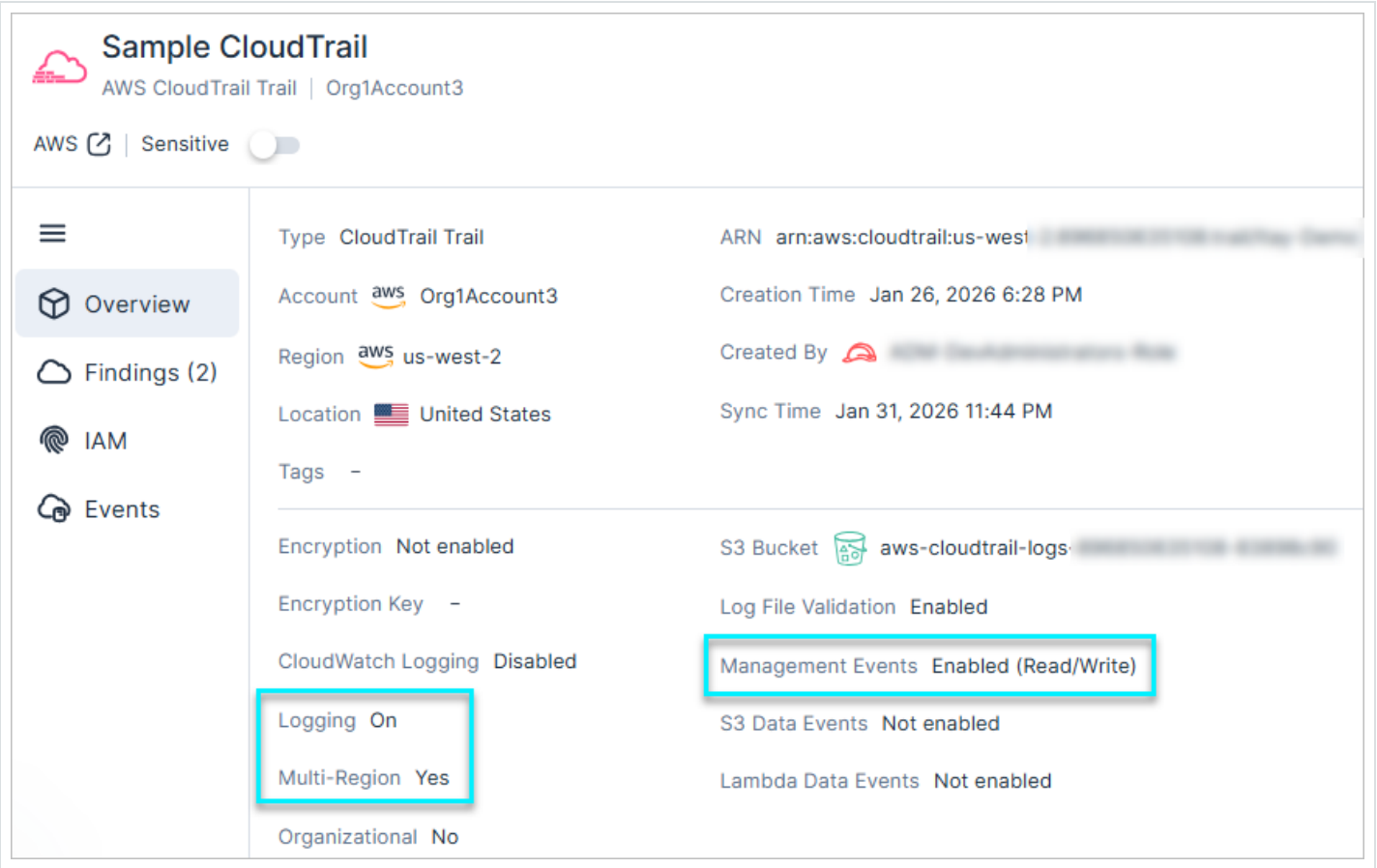
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso:CreateApplicationAssignment",
        "sso:DeleteApplicationAssignment",
      ],
      "Resource": "*"
    }
  ]
}
```

AWS CloudTrail

As part of the monitoring process, Tenable One AI Exposure needs to read data from a CloudTrail that logs activity for the connected account. During the account connection process, you must choose a trail to use, and then grant Tenable access to the S3 bucket where the trail is located via an IAM role. Follow the guidelines in the account and organization connection steps.

During connection, Tenable identifies and displays a list of valid trails that are:

- **Multi-region** – See AWS FAQ for more information about why a multi-region trail is needed.
- **Configured to log management read and write events**.
- **Enabled for logging**.



Each connected account generally has one associated CloudTrail, but there may be accounts with two or more trails.

If the S3 bucket where the CloudTrail files are stored is not in the same account as the account that you're connecting, you need to independently connect that account as well before you can choose it as a CloudTrail for the other account. If you use a separate AWS account as a “log archive account” to log activity for other accounts, Tenable recommends following this best practice:

- Connect log archive accounts with both **Monitoring** AND **CloudTrail** permissions, to provide full visibility into all of your AWS accounts. If, however, for some reason you don’t want AI Exposure to scan such accounts for security monitoring, you can connect it with **CloudTrail** permissions only.

Benefits of Granting CloudTrail Access

It is recommended to always grant Tenable access to the S3 bucket containing your CloudTrail when connecting accounts. Doing so provides several important benefits, including:

- *Cloud Threat Detection*:
    - Visibility into activity performed by identities within your cloud environment (Cloud Events).
    - Continuous risk analysis that checks for anomalies against behavioral baselines (Anomaly Detection).
- Visibility into effective use of permissions based on activity (used permissions).
- Fine-grained least-privilege recommendations based on usage. See Enable Granular Recommendations Based on Data Events for details.

Enable Granular Recommendations Based on Data Events

To enable action- and resource-granular recommendations within AI Exposure, enable CloudTrail data read/write event logging for S3 buckets/objects and Lambda functions, and then select the relevant trail/s in AI Exposure.
This ensures that, in addition to viewing generic information about access to a given AWS service, you can also analyze much more valuable information about:

- when a given identity used a specific action in the service
- exactly which resource within the service the identity used

In turn, this allows AI Exposure to provide specific, least-privilege recommendations related to this data. For example, Tenable can provide least-privilege recommendations down to the specific S3 bucket used by an application.

You can configure AI Exposure to work with your CloudTrail in one of the following ways, depending on whether you have data events enabled:

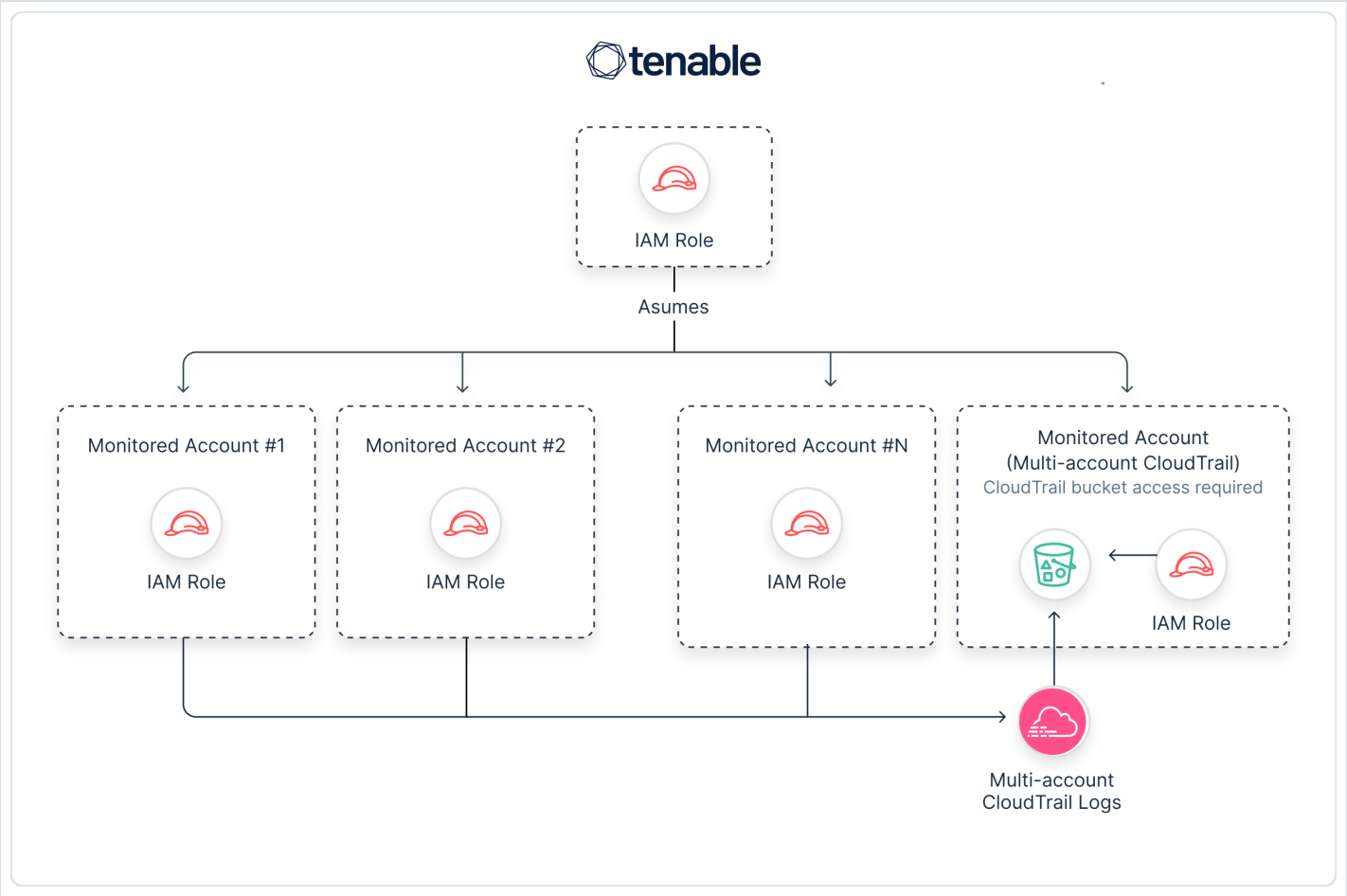
- If you use a single CloudTrail with both management events AND data events (either S3, Lambda, or both) enabled, select that trail from the **Management events** dropdown. The **S3 Data events** and/or **Lambda Data events** field will be automatically populated with the CloudTrail information that you select here.
- If you use separate trails for management events and data events (either S3, Lambda, or both), select the CloudTrail with management events enabled from the **Management events** dropdown, and the data event trail/s in the respective field.

CloudTrail Deployment

The following diagrams show how CloudTrail can be deployed in environments with multiple accounts, highlighting the differences between environments that maintain a dedicated CloudTrail (*organizational trail*) for multiple accounts, and those that have individual CloudTrails for each account.

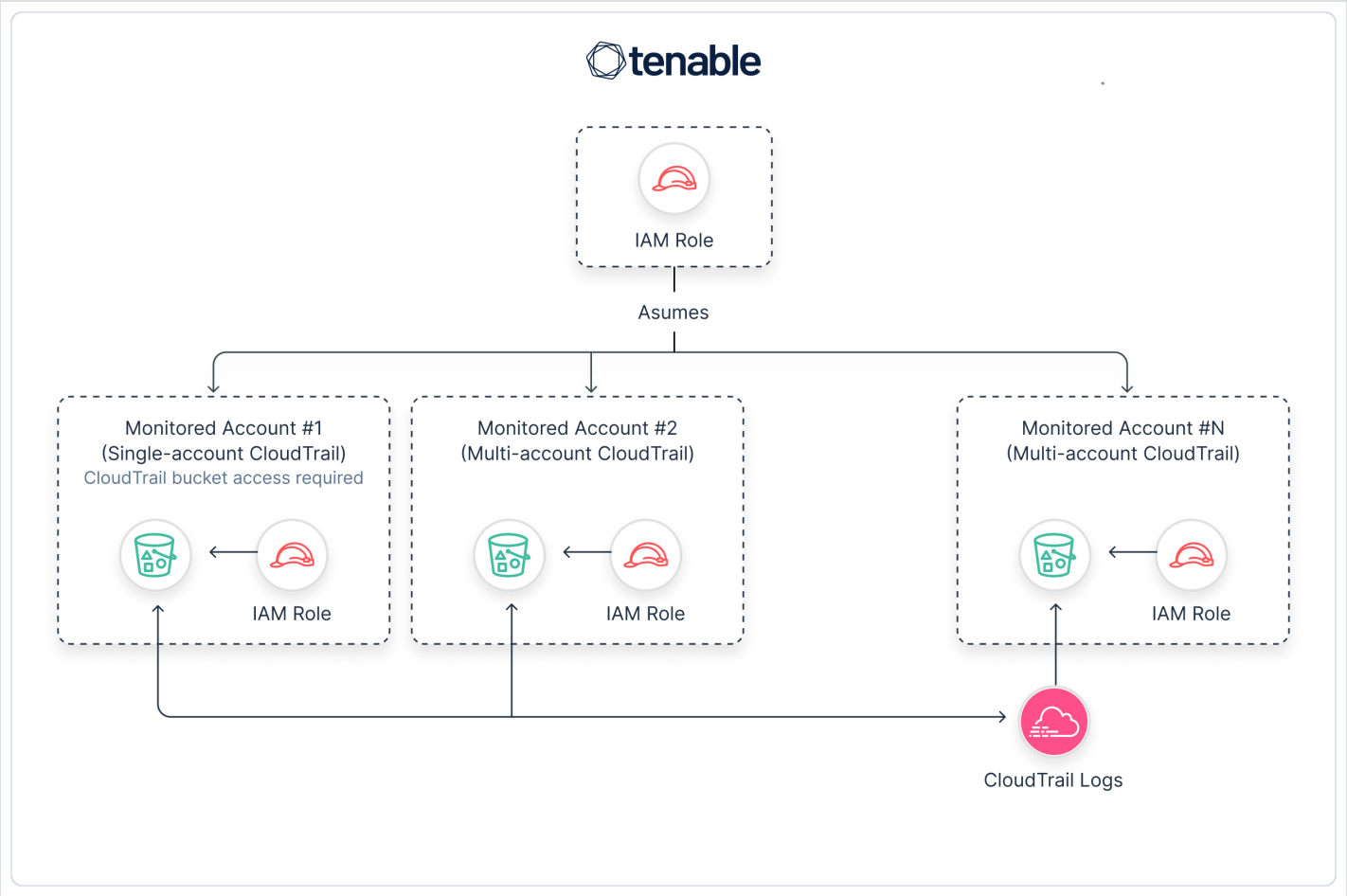
Dedicated Organization Trail for Multiple Accounts

In this scenario, a separate, dedicated AWS account is used as a *log archive account*, containing an organizational trail which logs activity for other accounts. This dedicated account should be independently connected to AI Exposure with Monitoring permissions, and its organizational trail can then be used as the shared CloudTrail for other accounts that you connect to Tenable. If you are connecting an entire organization, complete the process, and then edit the relevant account and grant Tenable CloudTrail permissions via the IAM role.



Single CloudTrail Bucket per Account

In this scenario, each connected account connects to an independent CloudTrail (identically named across accounts).



KMS Key in Different Account

If the KMS key for the CloudTrail is located in a different AWS account than the one you're currently adding, you need to grant AI Exposure access to the key.

To grant access to a KMS key located in a different account:

1. Navigate to the AWS account where the CloudTrail KMS key is located.
2. Navigate to **KMS > Customer managed keys** and open the relevant KMS key.
3. **Edit** the key policy and add the following statement to the "Statement" section:

```
JSON

{
```

```
    "Sid": "Allow an external account to use this KMS key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "{ErmeticRoleARN}"
    },
    "Action": "kms:Decrypt",
    "Resource": "*"
}
```

Where `ErmeticRoleARN` is the Role ARN of the role you created earlier in this wizard.

4. Click **Save Changes**.

Connect an AWS Account

Use this procedure to onboard an individual account. If you are onboarding your entire AWS organization, you will need to first follow this procedure to onboard the management account individually before continuing to onboard the organization.

To onboard an AWS account:

> **Note:** During the wizard you will need to navigate back and forth between the Tenable One AI Exposure Console and the AWS Management Console.

1. Navigate to **Settings** > **Integrations** and click **Add Integration**.
2. In the Integrations Library, select **AWS Account**.
3. In **Account Details**, complete these steps:
    1. Enter a **Name** for your account to be displayed in in the AI Exposure Console.

        > **Note:** You can choose whether to use the same naming convention in both the AWS Management Console and the AI Exposure Console. If you do use different names, make sure you can map the account names across the different consoles.

    2. Verify that the appropriate **AWS Partition** is selected (AWS Global or AWS China). The partition that your AWS account belongs to. A partition is a group of AWS Regions. For more information, refer to AWS Documentation.
    3. Select all relevant **Active Regions** where you have resources deployed.

> **Note:** Verify that you select only the specific regions used by your organization. Unselected regions will be ignored. Enable all regions not disabled or blocked by SCPs or RCPs for scanning. If your deployment expands to additional regions at a later stage, you will need to edit the account in AI Exposure and add those regions.

4. Click **Next**.

4. In **Permissions**, choose which permissions to grant to Tenable that are required for different features to function.

> **Note:** You can modify your selection after the initial onboarding. See AWS Required Permissions to learn more about why Tenable needs these permissions granted.

- **Monitoring (read-only)** – Gain full visibility for all cloud assets, including information about permissions, account usage, and security configurations. Additional permissions may be required to read the CloudTrail for the onboarded account. For more information about required permissions, see the documentation.
- **Data Protection** – Scan and classify cloud resources for sensitive data.

  > **Note:** This feature is relevant if you're working with AI Exposure Data Protection. See Data Protection for more information. See Data Resources Scanning Policy (Data Protection) to view the policy in JSON format.

- **EC2 Instance and AMI Scanning (Workload and Data Protection)**: Scan EC2 instances and AMI (private and public machine images) for vulnerabilities, misconfigurations, secrets and sensitive data. For more information about required permissions, see the documentation.

  > **Important:**
  > - This feature is relevant if you're working with AI Exposure Workload Protection. See Workload Protection for more information. See EC2 Instance Scanning (Workload Protection) to view the policy in JSON format.
  > - Tenable added exclusion rules by default to prevent scanning AMIs that are identified as **backup AMIs** based on their tags.

- **ECR Scanning (Workload Protection)** – Scan container registries for vulnerabilities and misconfigurations.

  > **Note:** Relevant if you're working with AI Exposure Workload Protection (requires Standard/Enterprise license). See Workload Protection for more information. See ECR Scanning Workload Protection Policy to view the policy in JSON format.

- **Remediation (read-write)** – Allow Tenable to make changes in your environment. This lets you automatically remediate findings with one click, for example (One-click remediation is still available via OTP without these permissions). For more information about required permissions, see the documentation.
- **Just-in-time Access for Account Assignments (AWS Identity Center)** – Grant users access to accounts for a predetermined period of time and on an as-needed basis. If the account you are onboarding is the management account, or has permissions to manage AWS Identity Center, additional permissions are required. For more information about required permissions, see the documentation.
- **Just-in-Time Access for Application Assignments (AWS Identity Center)** – Grant users temporary access to *applications* managed by AWS Identity Center, for a predetermined period of time and on an as-needed basis. If the account you are onboarding is the management account, or has permissions to manage AWS Identity Center, additional permissions are required. For more information about required permissions, see the documentation.
- **CloudTrail (S3)** – To analyze cloud activity logs, permissions are required to read from the S3 bucket storing CloudTrail data. If the bucket belongs to the account you are currently onboarding, select this option. For more information, see AWS CloudTrail.

  1. Enter the **Bucket name** where the trail data is stored.
  2. Indicate whether the trail bucket is **encrypted with AWS KMS**, and if so, enter the **KMS key ARN**.

  If the bucket belongs to a different account, you will need to do one of the following after completing this wizard:

1. [*When only onboarding* ***individual accounts***] Onboard the other account separately and grant Tenable **CloudTrail** permissions via the IAM role.
2. [*When onboarding your* ***entire organization***] Complete organization onboarding, and then edit the relevant account and grant Tenable **CloudTrail** permissions via the IAM role.

- **Amazon Bedrock Model Invocation Logs (S3)** – To monitor AI activity in Amazon Bedrock, you need permissions to read from the S3 bucket that stores your model invocation logs. To monitor AI activity in Amazon Bedrock, permissions are required to read from the S3 buckets storing the model invocation logs. For more information, see Enable Amazon Bedrock Activity Monitoring.

  > **Note:** Before using this feature, turn on model invocation logging in Amazon Bedrock. See Step 1: Enable Amazon Bedrock Model Invocation Logging.

  > **Note:** Amazon Bedrock activity monitoring is a runtime capability that completes the AI Security posture management (AI-SPM) coverage for Amazon Bedrock and Bedrock assets in Tenable One AI Exposure. Amazon Bedrock activity monitoring is currently available at no additional cost with the AI Governance add-on license.

5. Click **Next**.
6. Create a new **IAM role** using either CloudFormation (via the AWS Console, or the AWS CLI) or manually in the AWS Console:
   - **CloudFormation (AWS Console)**:
     1. Log in to the AWS account that you want to onboard.
     2. Click here to create a Stack, and then perform the following steps in the AWS Create stack wizard:

        > **Important:** You can use the link provided here, or the link in the wizard. However, if you use the link provide here, verify that the true/false values for each of the Tenable Policies reflect the permissions that you chose in step 2 of the wizard.

     3. (Optional) Choose a different name for the IAM role by modifying the **RoleName** parameter.

4. Select *I acknowledge that AWS CloudFormation might create IAM resources with custom names* and then click **Create Stack**.
5. Wait until the Stack creation is complete. You can click on the **Refresh** button to track progress.
6. Navigate to the **Outputs** tab and copy the Value that corresponds with the **TenableRoleArn** key.
7. Paste the IAM **Role ARN** in the wizard and then click **Next**.

- **CloudFormation (AWS CLI)**:
  1. Open a new shell session with the latest version of the AWS CLI. Administrator privileges are required to create the CloudFormation stack.
  2. Copy the command that appears in step B of the wizard, and run it in your shell.

     Important: The following is a command example, but be aware that the parameters and values may differ depending on the permissions you selected.

     Bash

     ```
     aws cloudformation create-stack --stack-name TenableStack \
       --template-url https://tenable-utilities.s3.us-east-
     2.amazonaws.com/Onboarding/AWS/CloudFormation/Template.json \
       --capabilities CAPABILITY_NAMED_IAM \
       --parameters \
         ParameterKey=RoleName,ParameterValue=TenableRole \
         ParameterKey=RoleExternalId,ParameterValue=ba2edce3-d9e1-4ae4-8b33-ecd3961aed8c \
         ParameterKey=RoleTrustedPrincipalId,ParameterValue=<aws_account_id> \
         ParameterKey=RoleMonitoringPolicy,ParameterValue=true \
         ParameterKey=RoleRemediationPolicy,ParameterValue=false \
         ParameterKey=RoleJitPolicy,ParameterValue=false \
         ParameterKey=RoleWorkloadProtectionPolicy,ParameterValue=true \
         ParameterKey=CloudTrailBucketName,ParameterValue=- \
         ParameterKey=CloudTrailKeyArn,ParameterValue=-
     aws cloudformation wait stack-create-complete --stack-name TenableStack
     aws cloudformation describe-stacks --stack-name TenableStack --query "Stacks[].Outputs"
     ```

  3. After completing stack creation, copy the **OutputValue** that corresponds with the

TenableRoleArn key from the shell.

4. Paste the IAM **Role ARN** in the wizard and then click **Next**.

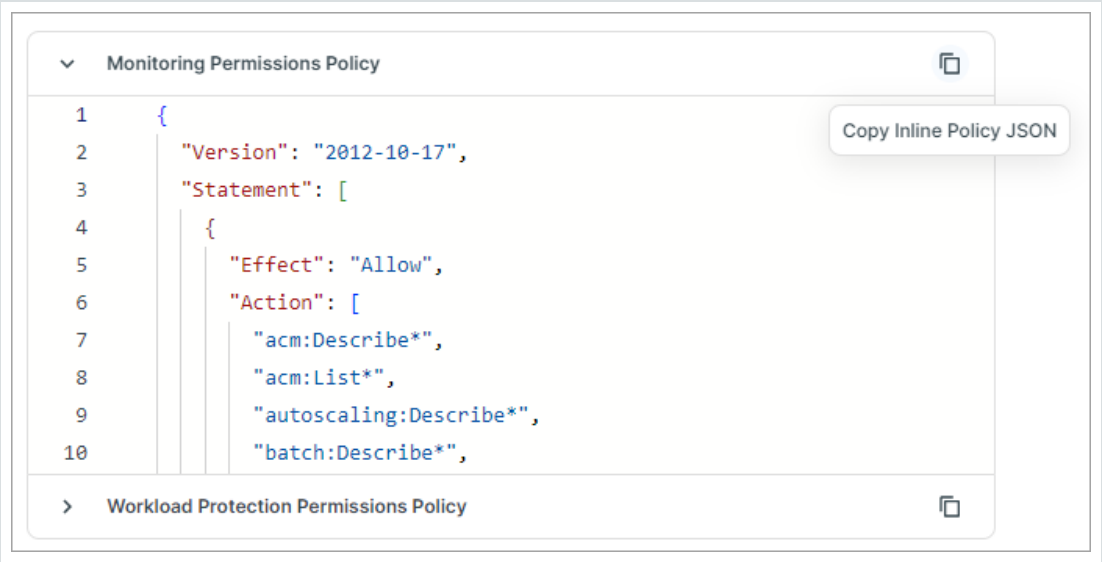
- **Manual (AWS Console)**:

1. In the AWS Management Console, navigate to **IAM > Roles** and click **Create role**.
2. For the trusted entity type, select **AWS account**.
3. For the AWS account, select **Another AWS account** and then enter one of the following numbers as the Account ID, depending on your AWS environment type, and reflecting the value that appears in Step 1 of the wizard:
   - Public Cloud: **081802104111**
   - US Gov Cloud: **757023926892**

   This is Tenable's account ID. The ID must be exactly twelve-digits; make sure not to include any extra spaces.
4. Under Options, check **Require external ID**.
5. Enter the Role External ID provided in step 3 of the Add Account wizard.

   > **Note:** The Role External ID is a unique identifier that AI Exposure assigns to your customer account. This ID will be the same for each account you create for your organization. For more information, refer to https://docs.aws.amazon.com/IAM/latest/UserGuide/confused-deputy.html.

6. In the list of policies, search for and select the **SecurityAudit permissions** policy and then finish creating the role. See AWS Required Permissions to learn more about why Tenable needs these permissions granted.
7. Open the newly created role.
8. For each of the policies that appear in step 3 (*IAM Role*) of the wizard in the AI Exposure Console, perform the following to create an inline policy:
   1. Click **Add permissions > Create inline policy**.
   2. Copy the policy that appears in the wizard and paste it in the JSON editor. For example:



3. Click **Next** and then finish creating the policy.

9. Paste the IAM **Role ARN** in the wizard and then click **Next**.

7. **Select a CloudTrail**. Select a CloudTrail for management events (required) and S3/Lambda data events (Step 5 in wizard). See AWS CloudTrail for important information and best practices related to granting Tenable access to trails.

    1. Under **Management events**, select a primary CloudTrail with management events enabled for AI Exposure to read activity logs from:

        > **Note:** Only valid trails are displayed here. For more information, see AWS CloudTrail.

        - If you use a single CloudTrail with both management events AND data events (either S3, Lambda, or both) enabled, select that trail from the dropdown. The **S3 Data events** and/or **Lambda Data events** field will be automatically populated with the CloudTrail information that you select here.
        - If you use separate trails for management events and data events (either S3, Lambda, or both), select the CloudTrail with management events enabled here, and the data event trail/s in the respective field.

    2. (Optional) Under **S3 Data events** and/or **Lambda Data events**, select the relevant CloudTrail. See Enable Granular Recommendations Based on Data Events for more information.

3. If you haven't yet granted permissions to the S3 bucket where the trail logs are stored, follow the on-screen instructions to do so.
4. If the KMS key for the CloudTrail is located in a different AWS account than the one that contains the S3 bucket, you need to grant AI Exposure access to the key.

8. Click **Finish**.

Next steps:

After your account is added successfully, the account appears in the table in *Accounts* > *AWS*. From here you can manage your account and view account details to see, for example, which features are enabled and whether the required permissions were granted.

Data about your account resources will start to appear in AI Exposure. The time it takes for all data to appear varies depending on the size of your cloud environment.

Onboard an AWS China Account

Onboard individual AWS China accounts to AI Exposure. When you onboard your account, AI Exposure doesn't copy any data from your account. Tenable only copies configuration metadata and CloudTrail event logs (optional). This information is saved in the region where you deployed AI Exposure.

- Onboarding is available for individual accounts only, and not organizations.
- AWS China accounts support the following features and functionality:
  - CIEM/CSPM
  - Data Protection via onsite scanning (Enterprise license)
  - Workload Protection via onsite scanning (Enterprise license)
- Tenable does not deploy servers in AWS China. Instead, asset configurations (and optionally, event logs) are copied from AWS China to another region in which Tenable is deployed (for example, the United States). This data is then stored alongside data synchronized from any of your non-China accounts.

To onboard an AWS China account:

1. **Create an IAM user**:
    1. In the AWS Management Console for one of your China accounts, navigate to **IAM > Users**.

        > **Note:** If you have more than one China account, you can create the user in any of your accounts. It doesn't matter which one.

    2. Click **Create user**.
    3. Enter a meaningful **User name**.
    4. Verify that the *Provide user access to the AWS Management Console* checkbox is **not** selected.
    5. Click **Next**.
    6. On the *Set permissions* page, click **Next** without making any configuration changes.
    7. Review the user details and then click **Create user**.
2. **Add an inline policy**:
    1. Find and click on the user you just created in the Users table.
    2. Under Permissions, click **Add permissions > Create inline policy**.
    3. In the Policy editor, click **JSON**, and then paste the following code into the editor:

        JSON

        ```
        {
          "Version": "2012-10-17",
          "Statement": [
            {
              "Effect": "Allow",
              "Action": "sts:AssumeRole",
              "Resource": "arn:aws-cn:iam::*:role/tenable-cs-role"
            }
          ]
        }
        ```

        > **Note:** `tenable-cs-role` is used as the role name in the above policy, but you can change the name if needed. Save this role name (default: `tenable-cs-role`), since you will need it later during account onboarding.

4. Click **Next**.
5. Enter a meaningul **Policy name** and then click **Create policy**.

3. **Create an access key**:

> **Note:** You can create a single access key for multiple accounts. There is no need to repeat this step for each additional account.

   1. For the user you created, under Security credentials, click **Create access key**.
   2. Select **Third-party service** and then click **Next** (select the checkbox to confirm).
   3. Click **Create access key**.
   4. On the Retrieve access keys page, securely save the **Access key** and **Secret access key** values and then click **Done**.
4. Contact Technical Support and securely provide them with the access key and secret for the IAM role you created.
5. With this information, Support will then enable AWS China to be used as a partition during account onboarding.
6. Connect your AWS China account, keeping in mind the following:
   - In step 1 of the onboarding wizard, under *AWS Partition*, select **China**.
   - In step 3 of the onboarding wizard, ensure that the IAM role you create is given the same name as the role in the policy you created earlier (default: `tenable-cs-role`).

Next steps:

After your account is added successfully, the account appears in the table in Accounts > AWS. From here you can manage your account and view account details to see, for example, which features are enabled and whether the required permissions were granted.

Data about your account resources will start to appear in AI Exposure. The time it takes for all data to appear varies depending on the size of your cloud environment.

Connect an AWS Organization

Connect an AWS Organization

Connect your entire AWS organization to expedite and automate the connection process in cloud environments with many accounts. Doing so allows you to:

- Simultaneously connect all accounts to Tenable at once.
- Automatically connect new accounts added in AWS at a later stage.
- Ensure visibility related to the full range of platform features (see Considerations for Connecting an Organization versus Individual Accounts).

Prerequisite

Onboard your organization's management account to Tenable One AI Exposure with the Connect an AWS Account account procedure.

Connect an Organization

To connect an AWS organization:

Be aware that during the wizard you will need to navigate back and forth between the AI Exposure Console and the AWS Management Console.

1. In the AI Exposure Console, navigate to **Settings > Integrations** and click **Add Integration**.
2. In the Integrations Library, select **AWS Organization**.
3. In **Select a management account**, select the management account you already onboarded. See Prerequisite.

   If you did not onboard your organizations management account, it will not be displayed in the dropdown.
4. In **Organization Details**, perform these steps:
   1. Verify that the **Organization Name** and **Role Name** are correct.

      > **Note:** The Organization Name is the ID of the organization, and can be found in the AWS Organizations console. If you previously connected individual accounts to AI Exposure,

> make sure that the name of the IAM role you choose here is different than any role names used for those accounts. After deploying the StackSet later on in this wizard, you can safely remove any other roles that were used.

2. Select the **CloudTrail Name** to be used in all member accounts, assuming you are using a default name for member accounts. If you aren't using a default name for CloudTrails in all member accounts, you can still configure CloudTrail for individual accounts, after connecting an organization. You can enter a wildcard character (*) in this field (e.g. `Organization-Trail-*` would select `Organization-Trail-1234`).

   > **Important:** After connecting the organization, you still need to grant Tenable access to the S3 bucket containing the trail. To do so, in AI Exposure, edit the relevant account where the bucket is located and grant Tenable CloudTrail permissions via the IAM role. If the bucket is located in your management account, you may have already done this when you connected that account.

3. Select all relevant **Active Regions** where you have resources deployed.

   Verify that you select only the specific regions used by your organization. Unselected regions will be ignored. Enable all regions not disabled or blocked by SCPs or RCPs for scanning. If your deployment expands to additional regions at a later stage, you will need to edit the account in AI Exposure and add those regions.

4. Choose whether to **automatically update folder structure**.

   Copy your AWS organizational unit folder structure into the platform, keeping your account hierarchy intact and continuously synchronized. Learn more about account hierarchy.

5. Click **Next**.
6. In **Permissions**, choose which permissions to grant to Tenable that are required for different features to function. To learn more, see AWS Required Permissions.
   - **Monitoring (read-only)** – Gain full visibility for all cloud assets, including information about permissions, account usage, and security configurations. Additional permissions may be required to read the CloudTrail for the onboarded account.
   - **Data Protection** – Scan and classify cloud resources for sensitive data.

> **Note:** This feature is relevant if you're working with AI Exposure Data Protection. See Data Protection for more information. See Data Resources Scanning Policy (Data Protection) to view the policy in JSON format.

- **EC2 Instance and AMI Scanning (Workload and Data Protection)**. Scan EC2 instances and AMI (private and public machine images) for vulnerabilities, misconfigurations, secrets and sensitive data. For more information about required permissions, see the documentation.

  > **Important:**
  > - This feature is relevant if you're working with AI Exposure Workload Protection. See Workload Protection for more information. See EC2 Instance Scanning (Workload Protection) to view the policy in JSON format.
  > - Tenable added exclusion rules by default to prevent scanning AMIs that are identified as **backup AMIs** based on their tags.

- **ECR Scanning (Workload Protection)** – Scan container registries for vulnerabilities and misconfigurations.

  Relevant if you're working with AI Exposure Workload Protection (requires Standard/Enterprise license. See Workload Protection for more information. See ECR Scanning Workload Protection Policy to view the policy in JSON format.

- **Remediation (read-write)** – Allow Tenable to make changes in your environment. This lets you automatically remediate findings with one click. For more information about required permissions, see the documentation.

7. Click **Next**.
8. **Create an IAM Role**, using **CloudFormation** (via either the AWS Console, or the AWS CLI):
   - **CloudFormation (AWS Console):**
     1. Log in to the AWS management account for your organization.
     2. Navigate to **CloudFormation > StackSets**.
     3. Click **Create StackSet**.
     4. In Step 1 (Choose a template), keep the default values in the *Permissions* and *Prerequisite - Prepare Template* sections, and, in the **Specify Template** section,

do one of the following depending on your deployment type. For both types, use the following S3 URL / template: `https://tenable-utilities.s3.us-east-2.amazonaws.com/Onboarding/AWS/CloudFormation/Template.json`

- *Standard AWS Organization (Commercial)*: Choose **Amazon S3 URL** and enter the above URL.
- *AWS GovCloud (US) Organization*: Choose **Upload a template file**. Download the above template as a JSON file, and then upload it here.

5. Click **Next**.
6. In Step 2 (Specify StackSet details), enter a **StackSet name**, and, optionally, a description.
7. Enter the parameter values listed in the Add AWS Organization wizard in the AI Exposure Console.
8. Click **Next**.
9. In Step 3 (Configure StackSet options), keep the default values as they are, and click **Next**.
10. In Step 4 (Set deployment options), choose either **Deploy to organization** or **Deploy to organizational units (OUs)**, as relevant. Keep the other default values as they are.
11. In the **Specify Regions** section, choose a single region (IAM roles aren't regional).
12. Click **Next**.
13. In Step 5 (Review), review the StackSet configurations. Select I acknowledge that AWS CloudFormation might create IAM resources with custom names and then click **Submit**.
14. Wait until the Stack creation is complete. You can click on the **Refresh** button to track progress.
15. [AI Exposure Console] Click **Next**.

- **CloudFormation (AWS CLI):**
    1. Log in to the AWS management account for your organization.
    2. Open a new shell session with the latest version of the AWS CLI. Administrator privileges are required to create the CloudFormation stack
    3. Copy the command that appears in the AI Exposure Console, and run it in your shell.
3. In the AWS Management Console, navigate to **CloudFormation > StackSets** and open the newly created StackSet.
4. Wait until the Stack creation is complete. You can click on the **Refresh** button to track progress.
5. [AI Exposure Console] Click **Next**.

9. In **Configure Scopes**, choose which Organizational Units (OUs) and accounts to onboard.
    - **Sync all accounts (recommended)**
    - **Include specific OUs and accounts**
    - **Exclude specific OUs and accounts**

    > **Note:** If you include/exclude an entire OU, all current and future accounts within the OU are included/excluded. If you include/exclude specific accounts, only the selected accounts will be included/excluded.

10. Click **Finish**.

Next Steps

After your organization is added successfully:

- You can see the organization in the *Organization* > **Accounts** page.
- You can see accounts that belong to the organization in the *Accounts* > **AWS** page. From here you can manage your account and view account details to see, for example, which features are enabled and whether the required permissions were granted.

Data about account resources will start to appear in AI Exposure. The time it takes for all data to appear varies depending on the size of your cloud environment.

AWS FAQ and Troubleshooting

This article contains:

- A list of frequently asked questions related to onboarding AWS to Tenable One AI Exposure.
- Account status and troubleshooting information.

Access to Us-East-1 Region

> Why does Tenable need to access the US East (N. Virginia) (us-east-1) region if I don't have resources deployed there? Why can't I have a service control policy (or other mechanism) that blocks permissions in that region?

Even though you may have granted Tenable all required permissions within regions that your organization is using, since some AWS services are global, Tenable must have permissions to query the global endpoint (us-east-1). For more information, refer to relevant AWS documentation here{target=_blank} and here{target=_blank}.

If you use service control policies (SCPs) in your AWS organization, make sure to add exclusions to any existing SCP to ensure that the dedicated IAM role you create for Tenable is not included.

AWS Console Access to Account

> I am seeing alerts (for example, in GuardDuty) that Tenable is trying to gain AWS console access to my account. Why would an API-based tool like AI Exposure require such access?

Generally speaking, AI Exposure only pulls information via the API. However, some data (for example, Lambda triggers and AWS SSO) is not available using Amazon's publicly documented API. To get this information, Tenable uses API calls that are typically used by the AWS console, resulting in the alerts that you're seeing. These are essentially undocumented APIs. The alerts are completely normal, and are in fact the expected behavior. Tenable never accesses your console

manually at any point. All access is strictly via the API.

Exclude an OU or Account from Organization

> How can I exclude a specific OU or account from an organization that I already onboarded?

To modify your organization's scope and remove specific entities:

1. In the Console, navigate to **Settings** > **Integrations**.
2. Click on the three dots menu next to the organization, and click **Edit**.
3. Click **Next** to navigate to the last step in the wizard (Scopes).
4. Select **Exclude specific OUs and accounts** and then select the relevant OU or account.
5. Click **Finish**. It will be removed from the Console the next time Tenable syncs data in your environment.

GetObject Permission for Elastic Beanstalk Buckets

> Why does Tenable need the GetObject permission for Elastic Beanstalk buckets in onboarded accounts?

The Elastic Beanstalk configuration is stored in an S3 bucket. As a result, there is no alternative way of accessing configuration for this service other than via this permission.

Need for Both Custom Policy and SecurityAudit Policy

> Why does Tenable need me to add both a custom, read-only inline policy and the AWS-managed SecurityAudit policy, when almost all of the permissions in the inline policy exist in the SecurityAudit policy?

Tenable continuously adds new features and functionality to its offering. To support this, the custom inline policy is updated by Tenable from time to time. The SecurityAudit policy contains an even broader permission set, and, together with the inline policy, ensures support for the rapidly expanding set of features that are added to AI Exposure. To ensure complete and ongoing support

for all current and future functionality in Tenable, and to give you the flexibility of not having to constantly track/update the permission set, both policies are needed. For step-by-step guidance on resolving AWS role and permission errors, see Resolve Cloud Onboarding Permission and Role Errors (AWS, Azure, GCP).

New AWS Services and Permissions

> When AWS adds new services or permissions to their offering, how soon are they reflected in Tenable?

As soon as the new services or permissions become available, but it may take up to one week before they are displayed in the AI Exposure Console. The process of detecting such changes is done programmatically, and not manually.

Update the Integration Name for the Organization

> Can I change the display name of my AWS organization integration in AI Exposure?

Yes. This is useful if you have multiple organizations and want clearer identification.

To update the name:

1. In the AI Exposure Console, navigate to **Settings** > **Integrations**.
2. Next to the relevant integration, click the three dots menu, and then **Edit**.
3. Navigate to step 2 in the wizard and update the **Organization Name** field.
4. Click **Next** to navigate to the last step in the wizard and then click **Update**.

ECS Task Definitions in Inventory

> Why don't I see all of my ECS Task Definitions in the Asset Inventory?

To keep your inventory focused and up to date, Tenable only synchronizes Task Definitions that meet at least one of the following criteria:

- The status is **Active**.
- The definition is **Inactive** but is currently referenced by an active ECS service or task.

Inactive and unused Task Definitions are automatically excluded from the inventory to ensure your data reflects your actual attack surface. Any findings associated with these excluded resources are automatically closed.

Multi-Region CloudTrail

> Why does the CloudTrail that Tenable needs to read data from have to be multi-region?

AI Exposure requires the continuous auditing of management events in all regions for, among other reasons, the ability to recommend removing unused permissions. To provide such recommendations with complete confidence, Tenable needs visibility into the full range of logs, across the entire environment, to ensure that such actions/permissions aren't being used.

Account Status and Troubleshooting

AI Exposure displays a **Status** for each account on the Accounts > AWS page, indicating, for example, whether Tenable can connect to the account, and helping you troubleshoot potential onboarding issues.

Status	Description
Access denied	AI Exposure wasn't able to synchronize one or more resource types. Although there are various reasons why this might happen, it is likely because you need to update the AI Exposure read-only policy (added during account onboarding) in AWS.
Account not found	
Connected	AI Exposure successfully connected to the account, and the account is up

Status	Description
	and running.
Connected with issues	The cluster is connected, but there are specific issues that need to be addressed: • JIT permissions not granted • Data Resources Scanning Policy (Data Protection) not granted • EC2 Instance scanning permissions (Workload Protection) not granted • ECR scanning permissions (Workload Protection) not granted • Terraform (S3) permissions not granted • Missing permissions required for reading events
Deleting... this may take up to an hour	You deleted the account in AI Exposure, and the process hasn't completed yet.
Disconnected	There is an issue with the IAM role that you created during account onboarding to delegate permissions to AI Exposure. It may have been deleted, or there was a change in the trust policy that prevents Tenable from assuming the role.
Invalid permissions	There is an issue with the IAM role that you created during account onboarding to delegate permissions to AI Exposure. Some permissions are missing. Please add the required permissions to the IAM role.
Failed to query regions	AI Exposure was unable to query the active regions that you selected in account onboarding. One or more of the regions may be disabled. Modify the region list or add an exclusion for the IAM Role from your SCPs and RCPs. Refer to the relevant AWS documentation for more information.

Status	Description
Pending deletion	The account is pending closure in AWS. It will eventually be deleted. Resources and findings associated with accounts pending deletion are hidden in AI Exposure.
Read-only policy is incorrect	The AI Exposure read-only policy is missing one or more of the following actions: • AwsCloudTrail.Actions.DescribeTrails • AwsCloudTrail.Actions.GetEventSelectors • AwsCloudTrail.Actions.GetTrail • AwsCloudTrail.Actions.GetTrailStatus
Suspended	The account is suspended in AWS. It will eventually be deleted. Resources and findings of suspended accounts are hidden in AI Exposure.

CloudTrail Status

See AWS CloudTrail for more information about CloudTrail-related issues.

Status	Description
Connected	Analyzing CloudTrail logs
Duplicate events	CloudTrail contains duplicate events. Please ensure the trail is configured correctly. This can happen if you configure multiple trails for the same account that cover overlapping event types.
Invalid CloudTrail configured	Invalid CloudTrail configured. Please select a valid trail or modify its configuration.

Status	Description
Missing permissions	Missing permissions to the CloudTrail service (cannot fetch list of trails).
Missing permissions to bucket	Missing permissions to read CloudTrail events from the target S3 bucket (may belong to a different account).
Not configured	CloudTrail logs aren't being analyzed. Please configure a valid trail.

Enable Amazon Bedrock Activity Monitoring

Chat assistants, agents, and custom applications that use Amazon Bedrock on Amazon Web Services (AWS) to invoke a large language model (LLM) generate a continuous stream of prompts and model responses. When enabled, Amazon Bedrock model invocation logging records these interactions as raw logs, but it does not inspect them for security risks.

Tenable One AI Exposure monitors these Amazon Bedrock model invocation logs. The platform catalogs the interactions in the logs, inspects them for security risks, and shows the results in the AI Exposure console.

To view activity detections for your AI applications, navigate to the **Activity Detections** page in AI Exposure. For more information, see AI Activity Detections.

Supported APIs and Models

AI Exposure supports the following Amazon Bedrock model invocation APIs:

API	Description	Supported Models
`Converse`	The standard Amazon Bedrock API for model	All models

API	Description	Supported Models
	invocation that sends messages to an Amazon Bedrock model through a consistent interface.	available through Amazon Bedrock.
`InvokeModel`	A direct invocation of a specific model hosted in Amazon Bedrock.	Currently, Anthropic models only.

Note: AI Exposure processes only model invocation logs that contain text-only content blocks into messages. AI Exposure skips any logs that contain non-text content blocks, such as images or tool calls.

Prerequisites

Before you enable Amazon Bedrock activity monitoring in AI Exposure, ensure that you have the following:

- **A connected AWS account** – To onboard an AWS account, see Connect an AWS Account.
- **Required Permissions**:
  - Permissions to modify Amazon Bedrock settings in the regions that you want to monitor, which allows you to enable model invocation logging.
- An Amazon S3 bucket to receive the Amazon Bedrock invocation logs. You can use a new or existing bucket.

Step 1: Enable Amazon Bedrock Model Invocation Logging

Complete the following steps for each AWS region where you use Amazon Bedrock.

1. Sign in to the Amazon Bedrock console for your region.
2. In the left navigation pane, click **Settings**.

3. In the **Model invocation logging** section, turn on the **Model invocation logging** toggle.
4. For both input and output content, select **Text** as the data type.
5. Select an Amazon S3 bucket as the logging destination. Note the bucket name and, if the bucket is encrypted with an AWS KMS key, the KMS key ARN.
6. Click **Save settings**.

For more information, see the Amazon Bedrock documentation.

> **Note:** AWS provisions Amazon Bedrock separately for each region in each account. Therefore, you must enable model invocation logging for every Amazon Bedrock instance in each AWS region where you deploy your account.

Step 2: Grant AI Exposure Access to the Amazon S3 Bucket

The IAM role associated with your account connection requires the following permissions to retrieve data from the Amazon S3 bucket:

- `s3:GetBucketLocation`
- `s3:GetObject`
- `s3:ListBucket`
- `kms:Decrypt` (required only if the bucket is encrypted with an AWS KMS customer managed key)

> **Note:** Restrict these permissions to the designated log bucket and any specific key prefix that you use. If your existing connector role already has global read-only access to data buckets, you do not need to take further action. Otherwise, update your IAM permissions or bucket policy to grant access.

For more information about permissions, see AWS Required Permissions.

To enable Amazon Bedrock monitoring on a connected AWS account:

1. Navigate to **Settings > Integrations**.
   The **Integrations** page appears.

2. In the row of the account for which you want to enable Amazon Bedrock monitoring, click the three-dots icon, and then select **Edit**.
3. In the **Permissions** step, enable **Bedrock Model Invocation Logging (S3)**, and then select the regions where you want to monitor Amazon Bedrock logs.

   > **Note:** You should only select AWS regions where Amazon Bedrock is available and that are already enabled in this AWS account's integration settings. If other regions are selected, it results in an issue for this AWS account connection.

4. In the **IAM Role** step, update the existing IAM role with the Amazon Bedrock permissions by using either the **CloudFormation (AWS CLI)** or the **Manual (AWS Console)** methods.

Update the IAM role using CloudFormation (AWS CLI):

1. Open a new shell session with the latest version of the AWS CLI. Administrator privileges are required to update the CloudFormation stack.
2. Copy the command that appears in the wizard, and run it in your shell.
3. Wait until the stack update is complete. The command updates the existing role, so it does not return a **TenableRoleArn** output in the shell.
4. Click **Next**, and then click **Finish**.

To update the IAM role manually (AWS Console):

1. In the AWS Management Console, navigate to **IAM > Roles**, and select the role created during onboarding.
2. On the **Permissions** tab, click **Add permissions > Create inline policy**.
3. Click **JSON**, and paste the policy that appears in the wizard. Replace `bucketName` with the name of your S3 bucket and `bucketKeyArn` with your KMS key ARN. If the bucket is not encrypted with a KMS key, remove the `kms:Decrypt` statement.

   > **Note:** The policy must include every Amazon S3 bucket and every AWS KMS key that Amazon Bedrock uses as a model invocation logging destination, across all the regions that you monitor.

JSON

```
{
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetBucketLocation",
      "s3:GetObject",
      "s3:ListBucket"
    ],
    "Resource": [
      "arn:aws:s3:::bucketName",
      "arn:aws:s3:::bucketName/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "bucketKeyArn"
  }
]
}
```

4. Click **Next**, enter a name for the policy, and then click **Create policy**.
5. Click **Next**, and then click **Finish**.

KMS Key in Different Account

If the KMS key that encrypts your Amazon Bedrock log bucket is located in a different AWS account than the one that is already connected, you need to grant AI Exposure access to the key.

To grant access to a KMS key located in a different account:

1. Navigate to the AWS account where the Amazon Bedrock log bucket KMS key is located.
2. Navigate to **KMS > Customer managed keys** and open the relevant KMS key.
3. Edit the key policy and add the following statement to the `Statement` section:

JSON

```
{
    "Sid": "Allow an external account to use this KMS key",
    "Effect": "Allow",
    "Principal": {
        "AWS": "{TenableRoleARN}"
    },
    "Action": "kms:Decrypt",
    "Resource": "*"
}
```

Replace `tenableRoleArn` with the ARN of the IAM role for your account connection. To find the ARN, sign in to the account that you connected, and then navigate to **IAM > Roles** and open the role you created during onboarding.

4. Save your changes.

Step 3: Verify Logging

After you configure logging and access, new interactions appear in the AI Exposure console shortly after they occur in Amazon Bedrock.

If Amazon Bedrock logging was already enabled before you set up monitoring, AI Exposure first syncs the logs from the previous 14 days. New interactions appear after this initial sync is complete.

> **How conversations are displayed:** Amazon Bedrock does not provide a session ID, so AI Exposure cannot group related calls into a single conversation. Most Amazon Bedrock conversations appear as a single turn (one prompt and its response). However, Claude Code does provide a session ID on the model invocation log so related calls can be grouped into a conversation.

Troubleshoot Missing Data

If data does not appear in the console after you enable logging, confirm the following items:

- The region where logging occurs is selected as an **Active Region** on the AWS account. For more information, see Connect an AWS Account.

- The Amazon S3 bucket contains new log objects. Verify the bucket directly in the AWS Management Console.
- The IAM role for the account has the `s3:GetBucketLocation`, `s3:GetObject`, and `s3:ListBucket` permissions for the bucket.
- Model invocation logging is enabled in every region where Amazon Bedrock calls occur. Model invocation logging is regional.
- Text content logging is enabled and not just metadata logging.

View Logging Details in the Console

You can view Amazon Bedrock logs in the AI Exposure console on the following pages:

> **Note:** AI Exposure assigns Amazon Bedrock interactions to the AWS scope.

- **AI Activity Detections** – Displays individual detections, including the content type (for example, exposed credentials, PII, or jailbreak attempt), its severity, triggering identity, and a link to the full conversation for context. For more information, see AI Activity Detections.
- **AI Activity Issues** – Displays related detections grouped together so you can triage recurring or related issues as a single unit. For more information, see AI Activity Issues.
- **Conversations** – Displays the reconstructed prompt or response history behind any detections. For more information, see AI Conversations.

> **Note:** AI Exposure determines conversation titles as follows:
>
> - **Claude Code conversations** – Claude Code makes a separate invocation in the same session to generate a title. AI Exposure reads that invocation log and uses the generated title.
> - **Single-turn conversations:** AI Exposure uses the first seven words of the prompt as the title.

Azure

Azure Overview

Connect your entire Azure organization (root management group) or individual subscriptions in Tenable One AI Exposure to get visibility and risk assessment for all resources associated with the subscriptions, including information about subscription usage and security configurations. Tenable collects inventory and configuration data from Azure APIs.

Identity-related visibility, such as users, permissions, and access relationships, requires a separate Microsoft Entra ID connection.

After connecting, Tenable displays a status for each subscription, indicating, for example, whether Tenable can connect to the account and helping you troubleshoot potential issues.

Connection Considerations

When connecting Azure to AI Exposure, it's important to consider how your connection choices affect coverage and available insights.

Azure resource connectivity enables visibility into cloud infrastructure, configuration risks, and security posture. *Connecting Microsoft Entra ID in addition to Azure* enables identity-related visibility, including users, permissions, and least-privilege analysis, and provides a more complete risk assessment across your Microsoft cloud environment.

You can connect individual subscriptions or your entire Azure organization (root management group), depending on how your environment is structured and managed. Tenable recommends connecting the entire Azure organization and configuring Microsoft Entra ID to ensure comprehensive visibility across both cloud resources and identities, and to include all current and future subscriptions.

Azure Required Permissions

The following permissions are required to connect Microsoft Entra ID and Azure subscriptions/organizations to Tenable One AI Exposure. For step-by-step guidance on resolving Azure permission and role errors, see Resolve Cloud Onboarding Permission and Role Errors (AWS, Azure, GCP).



Microsoft Entra ID Permissions

Deploying the required configuration for the AI Exposure Connector application in Microsoft Entra ID grants Tenable the following permissions:

- **Read all access reviews** (`AccessReview.Read.All`). Allows the app to read access reviews, reviewers, decisions and settings in the organization, without a signed-in user.
- **Read all audit log data** (`AuditLog.Read.All`). Allows the app to read and query your audit log activities, without a signed-in user.
- **Read directory data** (`Directory.Read.All`). Allows the app to read data in your organization's directory, such as users, groups and apps, without a signed-in user.
- **Read your organization's policies** (`Policy.Read.All`). Allows the app to read all your organization's policies without a signed in user.
- **Read assignment schedules for access to Azure AD groups** (`PrivilegedAssignmentSchedule.Read.AzureADGroup`). Allows the app to read time-based assignment schedules for access to Microsoft Entra ID groups, without a signed-in user.
- **Read eligibility schedules for access to Azure AD groups** (`PrivilegedEligibilitySchedule.Read.AzureADGroup`). Allows the app to read time-based eligibility schedules for access to Microsoft Entra ID groups, without a signed-in user.
- **View users' basic profile** (`profile`). Allows the app to see your users' basic profile (e.g., name, picture, user name, email address).
- **Read role management data for all RBAC providers** (`RoleManagement.Read.All`). Allows the app to read role-based access control (RBAC) settings for all RBAC providers without a signed-in user. This includes reading role definitions and role assignments.
- **Read all policies in PIM for Groups** (`RoleManagementPolicy.Read.AzureADGroup`). Allows the app to read policies in Privileged Identity Management for Groups, without a signed-in user.

These permissions are needed for Tenable to gather and report data related to relevant Microsoft Entra ID resources.

Important: Running the deployment script creates or updates a service principal in your tenant. The service principal represents the AI Exposure Connector application within your directory and enables it to access the required Microsoft Entra ID and Azure resources, based on the permissions and roles you assign.

For more information about application and service principal objects in Microsoft Entra ID, refer to Microsoft documentation.

Update Permissions for Tenable App

You may need to update permissions for the AI Exposure Connector app due to changes made by Microsoft, or to support new services introduced by Tenable. Since AI Exposure operates agentlessly with read-only access, these permissions cannot be updated automatically. Any updates must be made manually within your Azure account, by updating permissions.

1. Log in to the Azure portal for the relevant tenant.
2. Navigate to **Microsoft Entra ID**
3. Under Manage, click **Enterprise applications**
4. Search for and select the **AI Exposure Connector** app.
5. Navigate to **Security** > **Permissions**.
6. Click **Grant admin consent for...**
7. On the Microsoft account sign in page, pick an admin account belonging to the tenant Tenable.

Azure Permissions

This table lists the permissions (Azure roles) required to connect Azure to AI Exposure for each of the following AI Exposure capabilities.

Capability	Description	Azure Role	Notes
Monitoring	Gain visibility	• `Reader` • `Key Vault Reader`	• The

Capability	Description	Azure Role	Notes
(read-only)	into cloud assets, including subscription usage and security configurations.	• `Azure Kubernetes Service Cluster User Role` • `Azure Kubernetes Service RBAC Reader` • `Cognitive Services Data Reader`	**Key Vault Reader** role only allows read access to metadata of key vaults and its certificates, keys, and secrets. It doesn't grant access to read sensiti

Capability	Description	Azure Role	Notes
			ve values such as secret contents or key material. For more information, refer to the relevant Microsoft documentation. • The two **Kuber**

Capability	Description	Azure Role	Notes
			netes roles provide visibility and risk assessment for cloud identities and resources associated with AKS clusters. For more information about conne

Capability	Description	Azure Role	Notes
			cting AKS clusters and requirements, including 1) additional permissions required for full IAM visibility, and 2) network access requirements, see Conn

Capability	Description	Azure Role	Notes
			ect an Azure AKS Cluster. • Tenable uses the **Cognitive Services Data Reader** to list AI Foundry resources by reading metadata only.
Data	Scan and	• `Storage Blob Data Reader` built-in role	See Data

Capability	Description	Azure Role	Notes

Resources Scanning (Data Protection)	classify cloud resources for sensitive data. See Data Protection for more information.	• `Tenable Data Scanning` custom role, with the following permissions:
		  • `Microsoft.Storage/storageAccounts/privateEndpointConnections/write`
		  • `Microsoft.Sql/servers/databases/write`
			Protection documentation for more information.

Workload Protection	Scan virtual machines for vulnerabilities and misconfigurations.	• `Disk Snapshot Contributor` built-in role
		
		As an alternative to the built-in role, you can grant a custom role with the following permissions instead:
		  • `Microsoft.Compute/snapshots/beginGetAccess/action`
		  • `Microsoft.Compute/disks/beginGetAccess/action`
		  • `Microsoft.Compute/snapshots/write`
		  • `Microsoft.Compute/snapshots/endGetAccess/action`
		  • `Microsoft.Compute/snapshots/delete`
		
		To scan Windows virtual machines with **BitLocker** or Linux virtual machines with **DM-Crypt** (Ubuntu only) disk encryption, also grant:
			Using this feature requires the Standard/Enterprise license. Key Vault permissions can be granted per subscription or per key vault. See Connect Workloads for the

Capability	Description	Azure Role	Notes
		• `Key Vault Secrets User` built-in role, or the `Microsoft.KeyVault/vaults/secrets/getSecret/action` custom permission To scan a **BitLocker** encryption secret using a key from the key vault (KEK), also grant: • `Key Vault Crypto User` built-in role, or the `Microsoft.KeyVault/vaults/keys/unwrap/action` custom permission	procedure to grant these permissions.
Remediation (read-write)	Allow Tenable to make changes in your environment. This lets you automatically remediate findings with one click, for example (One-click remediation is still	`Owner`	

Capability	Description	Azure Role	Notes
	available via OTP without these permissions).		
Just-in-time Access	Grant users access to cloud accounts for a predetermined period of time and on an as-needed basis. To use this capability, you must also onboard your Microsoft Entra ID	`User Access Administrator`	

Capability	Description	Azure Role	Notes
	integration.		
IaC - Trace Issues Back to Code		`Storage Blob Data Reader`	This permission can only be enabled by editing the account, after connecting it successfully.

Important: Running the deployment script creates or updates a service principal in your tenant. The service principal represents the AI Exposure Connector application within your directory and enables it to access the required Microsoft Entra ID and Azure resources, based on the permissions and roles you assign.

For more information about application and service principal objects in Microsoft Entra ID, refer to Microsoft documentation.

Connect a Microsoft Entra ID Tenant

Connect a Microsoft Entra (formerly Azure Active Directory) tenant to Tenable One AI Exposure to enable identity-related visibility and analysis. This connection provides insight into identities, permissions, and access relationships across your Microsoft cloud environment.

Connect Microsoft Entra ID to enable identity visibility, identity posture management, and entitlement management

The Microsoft Entra ID connection enables visibility into the following assets:

- Users and groups
- Applications and application registrations
- Administrative roles
- Role assignments and access relationships

Note: Connecting Microsoft Entra ID does not grant AI Exposure access to Azure subscriptions or resources. Azure subscriptions and organizations are connected separately. This section does not relate to integrating an identity provider for AI Exposure Console login via SSO. To configure SSO for Console access, see Single Sign-On. This connection is required for CIEM, but is recommended for all license types to maximize your security posture.

Connect a Microsoft Entra ID Tenant

Note: For the public cloud, the deployment script creates a service principal that allows Tenable's multi-tenant app to pull data from Graph API. The China cloud requires manual app registration to pull the data.

FedRAMP: If you use Tenable One AI Exposure in a FedRAMP environment, make sure to connect integrations only to FedRAMP authorized services and endpoints. You are responsible for confirming that each service you connect meets your FedRAMP requirements. Sending data to a service outside your authorization boundary can put your organization out of compliance with FedRAMP requirements.

To connect a Microsoft Entra ID tenant:

1. In the AI Exposure Console, navigate to **Settings > Integrations** and click **+ Add Integration**.
2. Select **Microsoft Entra ID**.
3. Enter a **Name** for the integration.
4. Enter the Microsoft Entra ID **Tenant ID**.
5. Select the Azure Cloud **Environment**:
    - **Public** – Use this for tenants hosted in the global Microsoft Entra ID cloud. The deployment script creates a service principal that allows Tenable's multi-tenant app to

pull data from Graph API. If selected:

1. Click **Verify Tenant Access**. You will be redirected to sign in to your Microsoft Entra ID tenant to verify access.

   > **Note:** You must be either a member of the tenant organization.

2. When finished, return to this wizard and complete the steps.

- **China** – Use this for tenants hosted in the **Azure China** cloud environment. This requires manually registering an application. The deployment script creates a service principal that allows the app to pull data from Graph API. If selected:
  1. Create a dedicated app registration.
  2. Enter the **Application (Client) ID**.
  3. Enter the **Client Secret**.

6. Under **Deployment**, copy the provided PowerShell script to Azure CLI or Azure Cloud Shell to create a service principal and grant the required Microsoft Graph permissions.
7. Click **Finish**.

Manual App Registration (China Only)

Azure China operates in a separate cloud environment and requires a dedicated application registration to authenticate with AI Exposure using a client secret.

To register a dedicated application for China Cloud authentication:

1. Log in to your Entra ID tenant.
2. Navigate to **App registrations** and then click **+ New registration**.
3. Enter a **Name** for the application. For example, *AI Exposure China*.
4. Leave all other settings as is, and then click **Register**.
5. In the newly created app, navigate to **API permissions** and then click **+ Add a permission**.

> **Note:** The `User.Read` permission, which is configured by default, is not needed. You can leave it as is, or delete it.

6. Click **Microsoft Graph** and then **Application permissions**.
7. Search for and select the following permissions and then click **Add permissions**.
    - `AuditLog.Read.All`
    - `Directory.Read.All`
    - `Policy.Read.All`
    - `PrivilegedAssignmentSchedule.Read.AzureADGroup`
    - `PrivilegedEligibilitySchedule.Read.AzureADGroup`
    - `RoleManagementPolicy.Read.AzureADGroup`
    - `RoleManagement.Read.All`
8. Click **Certificates & Secrets** and then, under Client Secrets, click **+ New client secret**.
    - Enter a **Description** for the secret.
    - Define when the secret **Expires**.
    - When finished, click **Add**.

    > **Note:** Choose any expiration period that complies with your organizational policies. When the secret expires, create a new one, then edit and update the value in Tenable.

9. Copy the secret **Value**. *You will need to enter this value in the AI Exposure Console.*
10. Click **Overview** and copy the **Application (client) ID** value. *You will need to enter this value in the AI Exposure Console.*
11. Click **Settings** at the top of the portal, and in Directories + subscriptions, find and copy the **Directory ID** of your tenant. *You will need to enter this value in the AI Exposure Console.*
12. Go to the AI Exposure Console and complete the Connect a Microsoft Entra ID Tenant procedure.

Next Steps

After the Microsoft Entra ID tenant is connected:

- Identity data begins to appear in AI Exposure, including users, groups, roles, and access relationships.
- Identity-related risks and insights become available, including permissions analysis and Just-in-Time access visibility.

To gain visibility into Azure resources, configurations, and workloads, connect your Azure organization or subscriptions.

Connect an Azure Organization

Connect your entire Azure organization to expedite and automate the integration process in cloud environments with many accounts. Doing so allows you to:

- Automatically connect all current and future subscriptions under the Azure organization, eliminating the need to add subscriptions individually.
- Ensure consistent visibility and coverage across the Azure environment, preventing potential blind spots.

Prerequisites

Before you begin:

- Ensure you can access the Azure organization (root management group) you want to connect.
- Ensure you have permissions to create or use an application identity in Microsoft Entra ID for authentication to Azure APIs.
- (Public environments only) To verify tenant access, ensure you are either a member of the tenant organization or a guest user with the Global Administrator role. You can only be a guest user if you have integrated Microsoft Entra ID with the Tenable One AI Exposure Console.

> **Note:** Tenable recommends configuring your Microsoft Entra ID tenants to enable identity-related visibility and risk analysis.

Connect an Organization

FedRAMP: If you use Tenable One AI Exposure in a FedRAMP environment, make sure to connect integrations only to FedRAMP authorized services and endpoints. You are responsible for confirming that each service you connect meets your FedRAMP requirements. Sending data to a service outside your authorization boundary can put your organization out of compliance with FedRAMP requirements.

To connect an Azure organization:

1. In the AI Exposure Console, navigate to **Settings > Integrations** and click **+ Add integration**.
2. In the Integrations Library, click **Azure Organization**. The Azure Organization wizard opens.
3. In the **Configuration** step (step 1 of 2):
    1. Enter a name for the integration.
    2. Select the relevant Azure Cloud environment: **Public** or **China**.
        - **Public** – The deployment script creates a service principal in your tenant tied to Tenable's multi-tenant app, which is used to pull data via the Microsoft Graph API.
        - **China** – You will need to manually create a dedicated app registration in Microsoft Entra ID, as instructed in the Application section of the wizard. The deployment script creates a service principal tied to the app registration, which is used to pull data via the Microsoft Graph API.
    3. Under **Microsoft Entra ID**, select whether to use an existing Microsoft Entra ID integration. It is recommended to connect Microsoft Entra ID to enable full identity visibility.
        - If an integration does not exist, you can click **+ Add** to add it now.
        - If selecting **Do not use Microsoft Entra ID integration**, enter the **Tenant ID** associated with the relevant Azure organization to allow Tenable to identify the correct organization.
    4. Under **Access Verification**, click **Verify**. You are redirected to sign in to your Microsoft Entra ID tenant. This step ensures that the user creating the integration is a member of a target tenant or a guest user with the Global Administrator role, and is only required for public environments.

5. (Chinese environments only) Under **Application**, create a dedicated app registration in Microsoft Entra ID by following these instructions, making sure to copy and save the relevant values as instructed. This step is only required if you chose not to use an existing Entra ID integration above.
    - After creating the app registration, enter the application (client) ID and the client secret.
6. Under **Capabilities**, select the capabilities to enable. Your selection determines the required permissions and dynamically updates the deployment script. Tenable recommends enabling all capabilities to provide the most comprehensive security coverage. For more information, see Azure Permissions.
7. Under **Deployment**, select one of the following deployment options:
    - **PowerShell**. *Script-based deployment*. Copy the script that appears in the wizard and run it in Azure CLI or Azure Cloud Shell to grant AI Exposure the required permissions.
        - To assign roles, you must have the `Microsoft.Authorization/roleAssignments/*` permission on the root management group scope in Azure. This permission is granted by the `Owner` or `User Access Administrator` roles. For step-by-step guidance on resolving Azure role and permission errors, see Resolve Cloud Onboarding Permission and Role Errors (AWS, Azure, GCP).
        - If you don't have this permission/role, but you have the `Global Administrator` role in Microsoft Entra ID, you can temporarily elevate your access to gain management permissions over all Azure subscriptions and management groups.
    - **Manual**. *Manually, via the Azure portal*. See Manually Deploy an Azure Organization for step-by-step instructions on creating custom roles and assigning permissions.
8. Under **Post Deployment**, enter the primary domain name and the service principal ID.

> **Note: How to retrieve values** - *PowerShell*: Copy/paste the values from the script output. - *Manual*: See Manually Deploy an Azure Organization for how to retrieve these values. **Shared integration values** - These values must be identical across the organization and all its member subscriptions. - When an organization is connected, these fields can only be updated at the organization level. Changes will automatically propagate to all member subscriptions.

9. When finished, click **Next**.

4. In the **Scopes** step (step 2 of 2):
    1. (Optional) Select Automatically update compartments structure to mirror your compartment's structure as folders within Tenable, preserving the hierarchy and keeping the view synchronized. For more information, see Account Hierarchy and Folders.
    2. Under **Scopes**, choose which compartments to onboard:
        - **Sync all current and future subscriptions (recommended)**
        - **Include specific groups and subscriptions**
        - **Exclude specific groups and subscriptions**

        > **Note:** If you include/exclude an entire folder, all current and future projects within the group are included/excluded. If you include/exclude specific projects in a folder, only the selected projects will be included/excluded.

    > **Note:** During onboarding, AI Exposure detects every subscription in the organization, including canceled and deleted subscriptions. AI Exposure automatically filters out canceled and deleted subscriptions and does not onboard them. As a result, the number of detected subscriptions can be higher than the number that appear on the Accounts page.

5. Click **Finish**.

Manually Deploy an Azure Organization

Manually deploy your Azure organization via the Azure portal. This procedure is relevant if you selected **Manual** for the *Deployment* type when connecting your Azure organization.

1. Log in to the Azure portal for the organization that you want to connect.
2. (Only relevant if you chose **Do not use Microsoft Entra ID integration** above when you connected the organization.) Perform the following:
    - Obtain the **Service Principal ID**:
        1. Run the following command using the Azure CLI or Azure Shell: `az ad sp create --id 2608e51d-866a-43c9-99ab-3e44347ccb38 --query id`
        2. Copy and save the **Service Principal ID**. *You will need to enter this value in the AI Exposure Console* when connecting your organization.
    - Obtain the **Primary Domain Name**.
        1. Navigate to **Microsoft Entra ID**.
        2. Navigate to **Overview** > **Basic information** and locate the **Primary domain**. Copy and save the value. *You will need to enter this value in the AI Exposure Console* when connecting your organization.
3. Navigate to the Access control (IAM) tab within the root management group
4. Create a custom role called `Tenable Data Scanning` and add the following permissions to it:
    - `Microsoft.Storage/storageAccounts/privateEndpointConnections/write`
    - `Microsoft.Sql/servers/databases/write`
5. Assign roles to the AI Exposure Connector app by repeating the steps below for all roles related to the capabilities you want to use.
    1. Click on **Add > Add role assignment**.
    2. Search for and select a role from the list and click **Next**.
    3. Click **+ Select members**.
    4. Search for and select **AI Exposure Connector** and then click **Select**.
    5. Click **Next** and then click **Review + assign** to finish. Repeat these steps for all additional roles.

6. Navigate to the AI Exposure console and enter the following values in step 1 of the wizard:
    - **Primary Domain Name**
    - **Service Principal ID**
7. Click **Next** and continue with step 2 of the wizard.

Next Steps

After your Azure organization is connected, subscriptions that belong to the organization appear on the **Accounts** page, under the Azure folder. From here, you can manage subscriptions and view connection status and enabled features.

The time required for Azure resource data to appear in AI Exposure varies based on the size and complexity of your environment.

To enable identity-related visibility, permissions analysis, and Just-in-Time access insights, configure a Microsoft Entra ID connection, if you didn't already.

Connect an Azure Subscription

Use this procedure to connect an individual subscription. Alternatively, you can connect your entire organization. Follow the wizard to choose which features to enable, and then add role assignments in Azure to grant the Tenable One AI Exposure application access to the subscriptions.

Prerequisites

Before you begin:

- Ensure you can access the Azure subscription you want to connect.
- Ensure you have permissions to create or use an application identity in Microsoft Entra ID for authentication to Azure APIs.
- (Public environments only) To verify tenant access, ensure you are either a member of the tenant organization or a guest user with the Global Administrator role. You can only be a guest user if you have integrated Microsoft Entra ID with the AI Exposure Console.

Note: Tenable recommends configuring your Microsoft Entra ID tenants to enable identity-related visibility and risk analysis.

Connect a Subscription

FedRAMP: If you use Tenable One AI Exposure in a FedRAMP environment, make sure to connect integrations only to FedRAMP authorized services and endpoints. You are responsible for confirming that each service you connect meets your FedRAMP requirements. Sending data to a service outside your authorization boundary can put your organization out of compliance with FedRAMP requirements.

To connect an Azure subscription:

1. In the AI Exposure Console, navigate to **Settings** > **Integrations** and click **+ Add Integration**.
2. In the Integrations Library, select **Azure Subscription**. The Azure Subscription wizard opens.
3. In the wizard:
    1. Enter the relevant subscription ID. You can find it in the Azure portal under **Subscriptions**.
    2. Select the relevant Azure Cloud environment: **Public** or **China**.
        - **Public** – The deployment script creates a service principal in your tenant tied to Tenable's multi-tenant app, which is used to pull data via the Microsoft Graph API.
        - **China** – You will need to manually create a dedicated app registration in Microsoft Entra ID, as instructed in the Application section of this wizard. The deployment script creates a service principal tied to the app registration, which is used to pull data via the Microsoft Graph API.
    3. Under **Microsoft Entra ID**, select whether to use an existing Entra ID integration. If an integration does not exist, you can click **+ Create**.
        - If selecting not **Do not use Microsoft Entra ID integration**, enter the tenant ID associated with the relevant Azure subscription to allow Tenable to identify the organization with the subscription.

4. Under **Access Verification**, click **Verify**. You are redirected to sign in to your Microsoft Entra ID tenant. This step ensures that the user creating the integration is a member of a target tenant or a guest user with the Global Administrator role, and is only required for public environments.
5. (Chinese environments only) Under **Application**, create a dedicated app registration in Microsoft Entra ID by following these instructions, making sure to copy and save the relevant values as instructed. This step is only required if you chose not to use an existing Entra ID integration above.
    - After creating the app registration, enter the application (client) ID and the client secret.
6. Under **Capabilities**, select the capabilities to enable. Your selection determines the required permissions and dynamically updates the deployment script. Tenable recommends enabling all capabilities to provide the most comprehensive security coverage. For more information, see Azure Permissions.
7. Under **Deployment**, select one of the following deployment options:
    - **PowerShell**. *Script-based deployment*. Copy the script that appears in the wizard and run it in Azure CLI or Azure Cloud Shell to grant AI Exposure the required permissions.
        - To assign roles, you must have the `Microsoft.Authorization/roleAssignments/*` permission on the root management group scope in Azure. This permission is granted by the `Owner` or `User Access Administrator` roles.
        - If you don't have this permission/role, but you have the `Global Administrator` role in Microsoft Entra ID, you can temporarily elevate your access to gain management permissions over all Azure subscriptions and management groups.
    - **Manual**. *Manually, via the Azure portal*. See Manually Deploy an Azure Subscription for step-by-step instructions on creating custom roles and assigning permissions.

8. Under **Post Deployment**, enter the primary domain name and the service principal ID.

   How to retrieve values - *PowerShell*: Copy/paste the values from the script output. - *Manual*: See Manually Deploy an Azure Subscription for how to retrieve these values. **Shared integration values** - These values must be identical across the organization and all its member subscriptions. - You must have permissions in AI Exposure to update all related subscription integrations to change these values, ensuring they remain identical across your environment. - When an organization is connected, these fields can only be updated at the organization level. Changes will automatically propagate to all member subscriptions.

9. When completed, click **Finish**.

Manually Deploy an Azure Subscription

Manually deploy your Azure organization via the Azure portal. This procedure is relevant if you selected **Manual** for the *Deployment* type when connecting your Azure subscription.

1. Log in to the Azure portal for the subscription that you want to connect.
2. (Only relevant if you chose **Do not use Microsoft Entra ID integration** above when you connected the organization.) Perform the following:
   - Obtain the **Service Principal ID**:
     1. Run the following command using the Azure CLI or Azure Shell: `az ad sp create --id 2608e51d-866a-43c9-99ab-3e44347ccb38 --query id`
     2. Copy and save the **Service Principal ID**. *You will need to enter this value in the AI Exposure Console* when connecting your Azure subscription.
   - Obtain the **Primary Domain Name**.
     1. Navigate to **Microsoft Entra ID**.
     2. Navigate to **Overview** > **Basic information** and locate the **Primary domain**. Copy and save the value. *You will need to enter this value in the AI Exposure Console* when connecting your Azure subscription.

3. Create a custom role called **Tenable Data Scanning** and add the following permissions to it:
    - `Microsoft.Storage/storageAccounts/privateEndpointConnections/write`
    - `Microsoft.Sql/servers/databases/write`
4. Assign roles to the AI Exposure Connector app by repeating the steps below for all roles related to the capabilities you want to use.
    1. Navigate to Access Control (IAM) and click on **Add > Add role assignment**.
    2. Search for and select a role from the list in the wizard and click **Next**.

        > **Note:** Access Administrator* (for JIT) role is in the *Privileged administrator roles* tab. The *User Access Administrator* (for JIT) role is in the *Privileged administrator roles* tab.

    3. Click **+ Select members**.able AI Exposure Connector** and then click **Select**.
    4. Search for and select **AI Exposure Connector** and then click **Select**.ll additional roles.
    5. Click **Next** and then click **Review + assign** to finish. Repeat these steps for all additional roles.
5. Navigate to the AI Exposure console and complete the Post Deployment section of the onboarding wizard.

Next Steps

- Azure resource data begins to appear in AI Exposure. The time required varies based on the size and complexity of your environment.
- You can update enabled features and application details later, subject to the following rules:
    - If the subscription is connected as part of an Azure organization, updates must be made at the organization level.
    - If only subscriptions are connected, updates apply to all related subscriptions and require permission to update all of them.
- If you connected Azure without Microsoft Entra ID, identity-related insights (such as permissions analysis and Just-in-Time access) are not available until Microsoft Entra ID is

connected. To enable identity-related visibility, permissions analysis, and Just-in-Time access insights, configure a Microsoft Entra ID connection.

Azure FAQ and Troubleshooting

> **Note:** Some questions are not relevant for the **Cloud Vulnerability Management** license.

This article contains:

- A list of frequently asked questions related to connecting Azure to Tenable One AI Exposure.
- Subscription Status and Troubleshooting information.

Azure Subscription and Organization FAQs

This section contains a list of frequently asked questions related to connecting Azure subscriptions/organizations.

Pair Organization with Microsoft Entra ID

> When I connect my organization to Tenable, should I pair it with Microsoft Entra ID?

Tenable recommends pairing your Microsoft Entra ID tenant with your organization. Doing so:

- Enables identity-related visibility, including users, permissions, and least-privilege analysis, providing a more complete risk assessment across your Microsoft cloud environment.
- Allows visibility into identities, permissions, and access relationships, enhancing security posture management beyond just resource visibility.
- Ensures comprehensive visibility across both cloud resources and identities, including all current and future subscriptions

Exclude a Folder or Subscription from Organization

> How can I exclude a specific folder or subscription from an organization that I have already connected?

1. In the Console, navigate to **Settings** > **Integrations**.
2. Click on the three dots menu next to the organization, and click **Edit**.
3. Click **Next** to navigate to the last step in the wizard (Scopes).
4. Select **Exclude specific folders and subscriptions** and then select the relevant folder or subscription.
5. Click **Finish**. It will be removed from the Console the next time Tenable syncs data in your environment.

Minimum Permissions for Microsoft Entra ID User

> What are the minimum roles/permissions that my Microsoft Entra ID user needs to authorize the AI Exposure app in Azure, when I add a Microsoft Entra ID tenant in Tenable?

Granting admin consent requires you to sign in to Azure as a user that is authorized to consent on behalf of the organization. For more information about the specific roles needed to do this, refer to Microsoft documentation.

Key Vault Reader Role Assignment

> Why does Tenable need to be granted the `Key Vault Reader` role assignment? Does this role grant Tenable access to key material?

The Key Vault Reader role only allows read access to metadata of key vaults and its certificates, keys, and secrets. It doesn't grant access to read sensitive values such as secret contents or key material. For more information, refer to the relevant Microsoft documentation.

Update the Integration Name for the Organization

You can modify the name of your Azure organization integration/s, reflecting how the integration is displayed in AI Exposure. This can be useful for better identification, especially if you have multiple organizations.

To update the name:

1. In the AI Exposure Console, navigate to **Settings** > **Integrations**.
2. Click the three dots menu next to the relevant integration, and then click **Edit**.
3. Navigate to step 2 in the wizard and update the **Organization Name** field.
4. Click **Next** to navigate to the last step in the wizard and then click **Update**.

Microsoft Entra ID FAQs

This section contains a list of frequently asked questions related to connecting Microsoft Entra ID.

Handling Unused PII

> How does AI Exposure handle PII that isn't directly used for product functionality? Is it stored in logs or databases?

AI Exposure only synchronizes the minimum set of user attributes necessary for product functionality from Microsoft Entra ID (and other identity providers).

Attributes not synchronized, such as `birthday` for Microsoft Entra ID, are never received or stored in any AI Exposure databases or logs. Therefore, no unused PII is retained.

For a detailed list of attributes synchronized by default from Microsoft Entra ID, refer to the official Microsoft Entra ID documentation. This information is subject to change based on updates from Microsoft.

Required User Permissions for Authorizing App

> What minimum roles/permissions are required for my Microsoft Entra ID user to authorize the AI Exposure app during integration?

To grant admin consent for the AI Exposure app in Azure, your user must be authorized to consent on behalf of the organization. For more information about the specific roles needed to do this, refer to Microsoft documentation.

Connecting Public vs. China Microsoft Entra ID Tenants

> Are there different connection procedures for public Microsoft Entra ID tenants versus China tenants?

Yes. Refer to the following instructions.

Just-in-Time (JIT) Access Support

> Does the Microsoft Entra ID integration support Just-in-Time (JIT) Access

Yes. See Onboard Microsoft Entra ID for JIT.

Subscription Status and Troubleshooting

AI Exposure displays a **Status** for each subscription, indicating, for example, whether Tenable can connect to the subscription, and helping you troubleshoot potential connection issues.

Status	Description
Microsoft Entra ID is not connected	The Microsoft Entra ID tenant is not connected. See Connect a Microsoft Entra ID Tenant for more information.
Connected	AI Exposure successfully connected to the subscription, and the subscription is up and running.
Deleting... this may take up to an hour	You deleted the subscription in AI Exposure, and the process hasn't completed yet.
Failed to connect	AI Exposure failed to connect to the subscription. This might happen for one of the following reasons: • The subscription was deleted in Azure, but not deleted from the AI

Status	Description
	Exposure Console. • The service principal is unauthorized
Missing permissions	One or more of the listed roles are missing, and need to be added to the subscription. See Azure Required Permissions for more information.
Subscription is not enabled	The subscription is Expired, Past Due, or Warned, in Azure. Refer to the relevant Azure documentation for more information about subscription states.
Subscription is pending deletion	The subscription is Deleted or Disabled in Azure. Refer to the relevant Azure documentation for more information about subscription states.

Google

GCP Overview

Connect a GCP environment in Tenable One AI Exposure to get full visibility and risk assessment for all cloud identities and resources associated with your organization/projects, including information about permissions, account usage, and security configurations. Tenable collects inventory and configuration data from GCP API.

After successful connection, Tenable displays a status for each project, indicating, for example, whether Tenable can connect to the project, and helping you troubleshoot potential issues.

For a list of frequently asked questions related to integration, see Google FAQ and Troubleshooting.

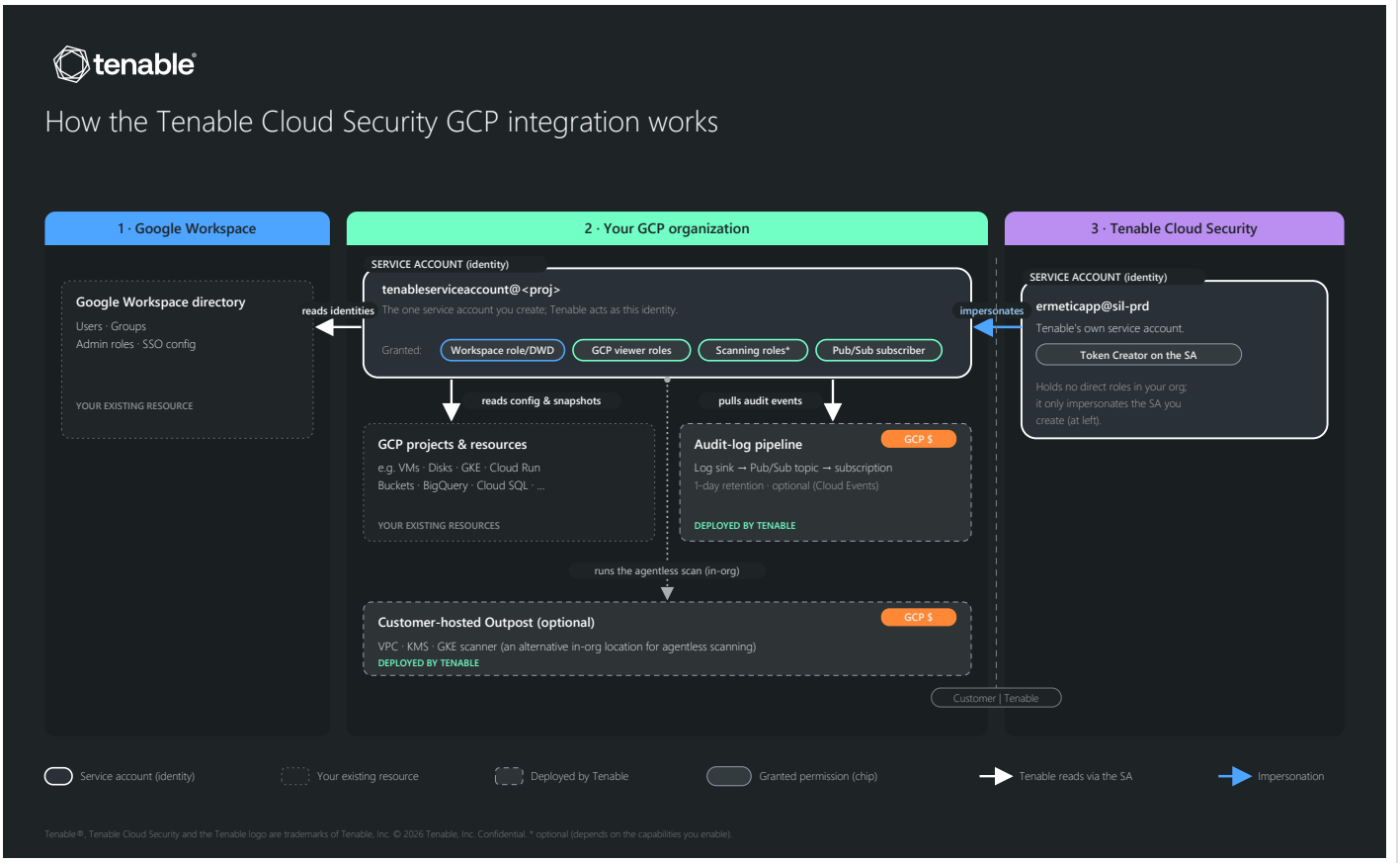
Perform the following steps to connect either:

- a single project.
- an entire organization

To view AI Exposure Activity Log data for your GCP resources, make sure to configure the audit log forwarding steps in the wizard. This can be done either on the organization level, or the individual project level. See Cloud Events Data.

It's important to fully understand the implications of Pub/Sub pricing before connecting accounts. Refer to Pub/Sub pricing for official, updated pricing information. Consider, for example, the following:

- **Message throughput costs** – Charges are based on the volume of data published and delivered, measured in GBs.
- **Data transfer costs** – Fees apply for data transferred across Google Cloud zones or regions.
- **Storage costs** – Charges are incurred for retaining messages, snapshots, or acknowledged messages.



Cloud Events Data

To view AI Exposure Cloud Events (activity log data) for your GCP resources, make sure to configure the audit log forwarding steps in the wizard. These steps require that you create a pub/sub topic, create a sink with the pub/sub topic as the destination, and then create a subscription to allow Tenable to receive messages published to the topic. This can be done either on the organization level, or the individual project level.

Add VPC Service Control Exceptions

If you use VPC Service Controls to restrict access to Google-managed services in the project/organization that you want to connect, you need to define exceptions to grant API access to Tenable IP addresses for your region. This ensures that the Tenable service account can access your projects, and that integration can proceed successfully.

For more information about creating service perimeters with VPC Service Controls, see the relevant Google Cloud documentation.

To add an exception:

> **Caution:** You need to add exceptions for all VPC perimeters associated with projects/organizations that you connect to AI Exposure.

1. Navigate to **VPC Service Controls** on the organization level.
2. Select the relevant access policy.
3. Click **EDIT PERIMETER** to edit the relevant VPC service perimeter.
4. In the **Ingress Policy**, update the **Identity** field (in the *FROM attributes of the API client* section) to include both the service account that you created for Tenable when you added a Google Workspace in AI Exposure AND the following Tenable service account:
    - `ermeticapp@sil-prd.iam.gserviceaccount.com`
5. In **Access Levels**, verify whether any access levels are configured by clicking on the **Choose Access Level** drop-down. *If so, make a note of the relevant access level/s that appear, as you need this information in the upcoming steps*.
6. Click **SAVE**.
7. Add Tenable IP addresses to any relevant access levels:
    - Navigate to **Access Context Manager** on the organization level, and locate the access level/s that you identified earlier.
    - **Edit** the relevant access level, and, in **IP subnetworks**, add the relevant Tenable IP addresses for your region.
    - Click **SAVE**.
    - Repeat this process for any other access levels.
8. (Workload Protection) Ensure the following:
    1. Allow all methods for `artifactregistry.googleapis.com` without any IP restrictions to cover tag listing and metadata calls used during discovery.

2. Add an egress rule that allows all operations for `compute.googleapis.com` for cross-project snapshot API read calls.
3. Add an ingress rule for `compute.snapshots.setIamPolicy`, which is the IAM binding step for the snapshot.
4. (Optional) Confirm the `sil-prd` account is in the relevant project.
5. Confirm both `ermeticapp@sil-prd.iam.gserviceaccount.com` and the delegated customer service account are in the relevant project.

Google Required Permissions

The following permissions are required to connect Google Workspace and GCP projects/organizations to Tenable One AI Exposure.

Google Workspace Permissions

You need to create a service account for Tenable. You can grant permissions to the service account in one of the following two ways when you Connect a Google Workspace:

- **Custom role** – Recommended for most organizations.
- **Domain-wide delegation** – Recommended for organizations that require Advanced IAM functionality.

Both methods support all core product functionality, including Just-In-Time (JIT) Access.

Required Permissions

Step	Permission	Description
1. **Create Service account**	`resourcemanager.projects.get`	Allows read access to project metadata, including project

Step	Permission	Description
		name, ID, and associated labels.
	`serviceusage.services.enable` `serviceusage.services.list`	Allows viewing and enabling services (APIs) within a Google Cloud project. This is required to activate specific APIs that AI Exposure depends on.
	`Service Account Token Creator`	Allows Tenable to generate access tokens to communicate with the API. For more information about why this permission is required, see Service Account Token Creator Role.
2a. **Custom role**	`Manage customer: Read customer` (all)	Allows read

Step	Permission	Description
(Recommended)		access to retrieve the primary domain name. This property is used for GCP permission evaluation.
	`Groups: Read`	Allows read access to groups.
	`Organization Units: Read`	Allows read access to organization units.
	`Users: Read`	Allows read access to users.
	(Optional) `Groups: Update`	Allows leveraging Just-In-Time access to temporarily add users to Google Workspace groups.

Step	Permission	Description

2b. **Domain-wide delegation (Advanced)**	OAuth scopes:
	`cloud-identity.groups.readonly`
	`admin.directory.customer.readonly`
	`admin.directory.domain.readonly`
	`admin.directory.group.readonly`
	`admin.directory.orgunit.readonly`
	`admin.directory.rolemanagement.readonly`
	`admin.directory.user.readonly`
	`admin.reports.audit.readonly`
	`cloud-identity.inboundsso.readonly`
		Allows read access to organization units, groups, users and advanced IAM features such as Admin roles and SSO profiles. For more information, see Added IAM Capabilities with Domain-Wide Delegation

GCP Project and Organization Permissions

Feature	GCP Roles	Notes
Monitoring (read-only)	• `App Engine Viewer` • `Artifact Registry Reader` • `BigQuery Metadata Viewer` • `Cloud Asset Viewer` • `Compute Network Viewer` • `Compute Viewer` • `Kubernetes Engine Viewer`	When connecting a GCP organization, these permissions must be granted at the organization level. Assign `Organization`

Feature	GCP Roles	Notes
	• `Organization Policy Viewer` • `Organization Viewer` • `Security Reviewer`	`Viewer` at the organization level, including for projects.
Data Protection	*Custom role* with the following permissions: • `bigquery.datasets.get` • `bigquery.datasets.getIamPolicy` • `bigquery.models.export` • `bigquery.models.getData` • `bigquery.models.getMetadata` • `bigquery.models.list` • `bigquery.routines.get` • `bigquery.routines.list` • `bigquery.tables.createSnapshot` • `bigquery.tables.export` • `bigquery.tables.get` • `bigquery.tables.getData` • `bigquery.tables.getIamPolicy` • `bigquery.tables.list` • `bigquery.tables.replicateData` • `cloudsql.backupRuns.create` • `cloudsql.backupRuns.delete` • `cloudsql.backupRuns.get` • `cloudsql.backupRuns.list` • `cloudsql.instances.get`	See Data Protection documentation for more information.

Feature	GCP Roles	Notes
	• `dataplex.projects.search` • `resourcemanager.projects.get` • `resourcemanager.projects.list` • `storage.folders.get` • `storage.folders.list` • `storage.managedFolders.get` • `storage.managedFolders.list` • `storage.objects.get` • `storage.objects.list`	
Workload Protection	*Custom role* with the following permissions: • `compute.disks.createSnapshot` • `compute.disks.use` • `compute.snapshots.create` • `compute.snapshots.delete` • `compute.snapshots.setIamPolicy` • `compute.snapshots.setLabels` • `compute.snapshots.useReadOnly`	Using this feature requires the Standard/Enterprise license. See Workload Protection documentation for more information.
Remediation (read-write)	• `BigQuery Data Owner` • `Security Admin` • `Service Account Admin`	
Just-In-Time Access (User Access Administrator)	`Security Admin`	

Feature	GCP Roles	Notes
Audit logs	`Pub/Sub Subscriber`	See the steps to configure audit logs for projects or organizations for specific instructions.

Org-Level Custom Role for Single-Project Connections

If you connect an individual GCP project without connecting its parent organization, AI Exposure still requires a basic set of permissions granted at the organization level, via a custom role with the following permissions:

- `cloudasset.assets.searchAllIamPolicies`
- `compute.firewallPolicies.list`
- `iam.roles.get`
- `iam.roles.list`
- `iam.workforcePools.list`
- `iam.workforcePoolProviderKeys.list`
- `iam.workforcePoolProviders.list`
- `recommender.iamPolicyInsights.list`
- `recommender.iamPolicyRecommendations.list`
- `resourcemanager.folders.getIamPolicy`
- `resourcemanager.folders.list`
- `resourcemanager.organizations.get`
- `resourcemanager.organizations.getIamPolicy`
- `resourcemanager.projects.list`

See Create a Custom Role with Org-Level Permissions for the procedure to create this role, and GCP FAQs for more information about why this is required.

Connect a Google Workspace

Connect your Google Workspace with Tenable One AI Exposure to reveal a complete inventory of relevant assets.

- This section does not relate to integrating your IdP for the purpose of enabling AI Exposure Console login via SSO. For more information about how to enable login via SSO for users who need access to the Console, see Single Sign-On.
- Tenable also identifies and displays information about external Google groups and users that aren't defined locally in Workspace.
- Even if you don't use Google Workspace, you should proceed with connecting *Cloud Identity* using the same procedure. Throughout the Console, the term *Google Workspace* is used interchangeably with *Cloud Identity*.

If you're using Tenable to monitor your GCP environment, it is recommended to connect your Google Workspace before you connect your projects/organization.

For answers to common questions that may arise about granting Tenable certain permissions during this integration, see Google FAQ and Troubleshooting.

Prerequisites

Before you begin:

- Grant sufficient permissions to the user who will create projects, create service accounts, and authorize the service accounts in the Google Cloud Console.
- Grant admin permissions to the user who will perform actions in the Google Workspace Admin Console.
- Create a dedicated project for each Google Workspace that will host the service account used by Tenable.

- Enable billing for the dedicated project in the Google Cloud Console. For instructions, see Google's documentation on enabling billing.
- Terraform-specific:
  - Ensure you have Terraform CLI v0.13+ installed.
  - Ensure `terraform init` can download and install Google Cloud provider v7.11+ without conflicting with your existing configurations.

Note: Dedicated projects:

- **Prevent API throttling** – GCP enforces API rate limits at the project level. Sharing a project with other service accounts increases the risk of hitting these limits and being blocked.
- **Isolate expenses** – A shared project obscures billing and usage data, making it harder to track the exact costs generated by a Tenable service account.

Add a Workspace

Follow the steps described here to add a Google Workspace to AI Exposure. This process consists of:

- Creating a service account for Tenable in your GCP Organization.
- Assigning permissions to the service account.

Note: If you use a single user for both consoles, make sure that user has all necessary permissions.

FedRAMP: If you use Tenable One AI Exposure in a FedRAMP environment, make sure to connect integrations only to FedRAMP authorized services and endpoints. You are responsible for confirming that each service you connect meets your FedRAMP requirements. Sending data to a service outside your authorization boundary can put your organization out of compliance with FedRAMP requirements.

To add a Google Workspace:

1. In the AI Exposure Console, navigate to **Settings > Integrations** and click **+ Add Integration**.
2. In the Integrations Library, click **Google Workspace**. The Google Workspace wizard opens.

3. In the wizard:
    1. Enter a name for the integration.
    2. For **Customer ID**, open the Google Admin console, navigate to **Account** > **Account settings**, and copy the **Customer ID**.
    3. Under **Deployment**, select one of the following deployment options to create a service account for Tenable in a dedicated project:
        - **Cloud Shell**. *Script-based deployment*. Copy the script that appears in the wizard and run it in a dedicated GCP project to grant AI Exposure the required permissions.
            1. In the Google Cloud Console, create a new project for Tenable.
            2. Activate the **Cloud Shell** within the newly created project.
            3. Copy the script displayed in the AI Exposure wizard and run it in your Cloud Shell.
            4. Wait until the script has completed successfully, and then copy the **Service Account Email** from the output.
        - **Terraform**. *Module-based deployment*. See Prerequisites before deploying.
            1. Enter the **Management Project ID**. This is the ID of the dedicated project hosting the service account for this integration.
            2. In the Google Cloud Console, navigate to the project you created.
            3. Go to **IAM & Admin** > **Labels**, click **+ Add label**, and add the key/value pair that appears in the AI Exposure wizard.
            4. Copy the module invocation displayed in the AI Exposure wizard, add it to your Terraform configuration, and then run `terraform apply`. The module creates the identity and grants Tenable the permissions to connect and scan the environment.
        - **Manual**. *Manually, via the Google Cloud Console*. See Manually Deploy a Google Workspace for step-by-step instructions.

> **Caution:** When you finish manual deployment, return to the wizard to complete Post Deployment.

4. Under **Post Deployment GCP Settings**, enter the service account email. Retrieve the email in one of the following ways, depending on the deployment method you chose in the previous step:
   - **Cloud Shell** – Wait until the script completes successfully, then copy/paste the service account email from the generated output.
   - **Terraform** – Retrieve the service account email (`tenable_service_account_mail`) from the Terraform output.
   - **Manual** – See Manually Deploy a Google Workspace.
5. Under **Post Deployment Google Workspace Settings**, grant Tenable permissions to the Google Workspace.
   1. Custom role: Supports all core functionality within AI Exposure. *This option is recommended for most organizations.*
   2. Domain-wide delegation: Designed for organizations that require advanced IAM functionality. For more information, see Added IAM Capabilities with Domain-Wide Delegation.

   For more information about why these permissions are needed, see Google Required Permissions.
4. Click **Finish**.

Grant Permissions via Custom Role (Recommended)

Grant permissions to the Google Workspace via a custom role.

This method supports all core functionality within AI Exposure, including Just-In-Time access. *This option is recommended for most organizations.*

1. In the Google Admin console, navigate to **Account** > **Admin roles** and then click **Create new role**.
2. Enter a **Name** and **Description**, and then click **CONTINUE**.

3. Under *Select Privileges* > *Admin API privileges*, select the privileges listed under **2a. Custom role (Recommended)** in Required Permissions.

   > **Note:** The optional *Groups* > *Update* privilege lets you leverage Just-In-Time access to temporarily add users to Google Workspace groups.

4. Click **CONTINUE** and then click **CREATE ROLE**.
5. In the *Admin roles* page of the newly created role, click **Assign service accounts**.
6. Enter the service account email that you created in step 2 of the AI Exposure wizard, click **ADD**, and then click **ASSIGN ROLE**.

Grant Permissions via Domain-Wide Delegation (Advanced)

Grant permissions to the Google Workspace via domain-wide delegation.

Designed for organizations that require advanced IAM functionality, and also supports Just-In-Time access. For more information, see Added IAM Capabilities with Domain-Wide Delegation.

1. In the Google Cloud console, navigate to the service account that you created in step 2 of the AI Exposure wizard, and in the **Details** tab, click to expand the **Advanced settings** section.
2. Copy the **Client ID** and click **View Google Workspace Admin Console**.
3. In the Admin console, navigate to **Security** > **Access and data control** > **API controls**.
4. Click on **MANAGE DOMAIN WIDE DELEGATION** and then click **Add new**.
5. Paste the **Client ID** that you copied earlier.
6. Copy and paste the following **OAuth scopes**:

```
https://www.googleapis.com/auth/cloud-identity.groups.readonly,
https://www.googleapis.com/auth/admin.directory.customer.readonly,
https://www.googleapis.com/auth/admin.directory.group.readonly,
https://www.googleapis.com/auth/admin.directory.orgunit.readonly,
https://www.googleapis.com/auth/admin.directory.rolemanagement.readonly,
https://www.googleapis.com/auth/admin.directory.user.readonly,
https://www.googleapis.com/auth/admin.reports.audit.readonly,
https://www.googleapis.com/auth/cloud-identity.inboundsso.readonly
```

7. (Optional) If you want to leverage Just-in-Time (JIT) access to temporarily add users to Google Workspace groups in this organization, add the following OAuth scope: `JIT OAuth scope`.
8. Click **AUTHORIZE**.
9. Enter the **User Email** of the relevant Google Admin console user in the AI Exposure wizard.
    - User must be assigned the *Super Admin* role
    - To assign or view users with this role, go to **Account** > **Admin roles**, hover over **Super Admin**, and click **Assign admin** or **View admins**.
    - Actual permissions granted to Tenable are limited to the OAuth scopes granted earlier.

Manually Deploy a Google Workspace

Manually deploy your Workspace via the Google Cloud Console. This procedure is relevant if you selected **Manual** for the *Deployment* type when adding your workspace.

1. In the Google Cloud Console, create a new project for Tenable, or navigate to an existing project (not recommended).
2. Within the newly created project, navigate to **IAM & Admin** > **Roles** and then click **+Create Role**.
3. Enter a **Title**, **Description**, and **ID**.
4. Click **+ Add Permissions**, and add the permissions listed under **Create Service Account** in Required Permissions.
5. Click **Create** to finish creating the role.
6. Click on the **Service Accounts** tab and then click **+ Create service account**.
7. Enter a **Service account name**, **ID**, and **description** and then click **Create and continue**.
8. Select the custom role you created and click **Continue**, and then **Done**.
9. Click on the newly created service account, go to the **Principals with access** tab, and click **+ Grant access**.

    Important: If you are unable to grant access, you may have an organization policy with a domain restriction constraint that prevents choosing Tenable as a principal in IAM policies. This

prevents Tenable from impersonating the created service account. If this is the case, follow the procedure described in Add Tenable as an Allowed Domain.

10. Insert **ermeticapp@sil-prd.iam.gserviceaccount.com** in the *New principals* field and choose the Service Account Token Creator role. Click **Save** to finish.
11. Copy and save the email of the service account you created. Visible under *IAM & Admin > Service Accounts*, in the **Email** field. You will need to enter this in the AI Exposure Console.
12. Go to **IAM & Admin** > **Labels**, click **+ Add label** and add the key/value pair that appears in the AI Exposure wizard.
13. Click **Save** to finish.
14. Navigate to **APIs & Services** > **Enabled APIs & services**, select **Service Usage API** and click **ENABLE**.
15. [AI Exposure Console] Return to the wizard and continue with **Post Deployment GCP Settings**. See Add a Workspace.

Add Tenable as an Allowed Domain

If you are unable to grant access to the created service account, you may have an organization policy with a domain restriction constraint that prevents choosing AI Exposure as a principal in IAM policies. This prevents Tenable from impersonating the created service account. If this is the case, follow the procedure described here.

To add Tenable as an allowed domain:

1. In the Google Cloud console, within the project where the service account was created, navigate to **IAM & Admin > Organization Policies**.

   Note: If you use Tenable for workload scanning *across all projects*, you must add Tenable as an allowed domain **at the top-level organization policy**.

2. In the Filter, search for and then select **Domain restricted sharing**, and then click on the policy to open it.
3. Click **MANAGE POLICY**.

4. In the Rules section, click **ADD A RULE**.
5. Under Policy values, choose **Custom**.
6. Under Policy type, choose **Allow**.
7. Under Custom values, enter the following value: `C00nd19ht`

Added IAM Capabilities with Domain-Wide Delegation

If you grant permissions to the service account via domain-wide delegation, the following additional IAM capabilities are supported.

> **Note:** To understand which permission-granting method is right for your organization, see Google Workspace Permissions. For more information about domain-wide delegation, see Domain-Wide Delegation (Advanced).

- **Admin roles** – Gain visibility into your Google Workspace admin roles. Admin roles define administrators' access and control over the organization's environment, including which settings, data, and administrative functions they can manage. With domain-wide delegation, you can see:
  - Which admin roles exist in your environment
  - Role assignments (providing insights into administrative access and privilege distribution.)
- **SSO Profile** – Improve the accuracy of MFA-related findings via visibility into your Workspace's SSO configuration. SSO profiles indicate whether multi-factor authentication (MFA) is enforced through third-party identity providers (IdPs).
  - **No MFA label behavior** – When an SSO profile is detected, AI Exposure assumes MFA is enforced at the third-party IdP level and does not assign the *No MFA* label to affected identities.
  - **Impact on finding severity** – Without this visibility, finding severity related to MFA enforcement is less granular, potentially affecting risk assessments.
- **Inactive users** – Reduce false positives in inactivity findings by distinguishing between truly inactive users and those active via API access. With domain-wide delegation:

- AI Exposure can detect **API-only activity**, even if a user hasn't logged into the UI.
- This ensures only genuinely inactive principals are flagged, improving the relevance and precision of inactivity-related findings.

Update the Integration Name

You can modify the name of your Google Workspace integration/s, reflecting how the integration is displayed in AI Exposure. This can be useful for better organization and identification, especially if you have multiple identity provider integrations.

To update the name:

1. In the AI Exposure Console, navigate to **Settings** > **Integrations** and click on **Google Workspace**.
2. Next to the relevant integration, click the three dots menu, and then **Edit**.
3. Navigate to step 1 in the wizard (Workspace Details) and update the **Name** field.
4. Click **Next** to progress to the last step, and then click **Update**.

Connect a GCP Organization

Connect your entire GCP organization to automatically onboard all current and future projects, without adding them individually.

Prerequisites

Before you begin:

- Grant sufficient permissions to the user who will create projects, create service accounts, authorize the service accounts, and enable logging in the Google Cloud Console.
- Define exceptions to allow Tenable network access if you use VPC Service Controls to restrict access to Google-managed services.

- Create a dedicated project for each Google Organization that will host the service account used by Tenable. If you already created a project when connecting a project to Tenable, use the same one.
- Enable billing for the dedicated project in the Google Cloud Console. For instructions, see Google's documentation on enabling billing.
- Terraform-specific:
  - Ensure you have Terraform CLI v0.13+ installed.
  - Ensure `terraform init` can download and install Google Cloud provider v7.11+ without conflicting with your existing configurations.

Note: Dedicated projects:

- **Prevent API throttling** – GCP enforces API rate limits at the project level. Sharing a project with other service accounts increases the risk of hitting these limits and being blocked.
- **Isolate expenses** – A shared project obscures billing and usage data, making it harder to track the exact costs generated by a Tenable service account.

Connect an Organization

FedRAMP: If you use Tenable One AI Exposure in a FedRAMP environment, make sure to connect integrations only to FedRAMP authorized services and endpoints. You are responsible for confirming that each service you connect meets your FedRAMP requirements. Sending data to a service outside your authorization boundary can put your organization out of compliance with FedRAMP requirements.

To connect a GCP organization:

1. In the Tenable One AI Exposure Console, navigate to **Settings** > **Integrations** and click **+ Add Integration**.
2. In the Integrations Library, click **GCP Organization**. The GCP Organization wizard opens.
3. In the **Configuration** step (step 1 of 2)::
   1. Enter a name for the integration.
   2. Enter the organization ID.

3. Under **Google Workspace**, select whether to use an existing Google Workspace integration. If an integration does not exist, you can click **+ Create**.

   > **Note:** Tenable recommends using your Google Workspace with your organization to enable identity-related visibility and complete risk assessment. Doing so:
   > - Enables identity-related visibility, including users, permissions, and least-privilege analysis, providing a more complete risk assessment across your GCP cloud environment.
   > - Allows visibility into identities, permissions, and access relationships, enhancing security posture management beyond just resource visibility.

4. Under **Capabilities**, select the capabilities to enable. Your selection determines the required permissions and dynamically updates the deployment script. Tenable recommends enabling all capabilities to provide the most comprehensive security coverage. For more information, see Google Required Permissions.

5. Under **Deployment**, select one of the following deployment options:

   - **Cloud Shell**. *Script-based deployment*.

     1. Enter the **Management Project ID**. This is the ID of the dedicated project hosting the service account for this integration.
     2. Copy the script displayed in the AI Exposure wizard, create a file with the script content, and then run it in your Cloud Shell to grant AI Exposure the required permissions.

   - **Terraform**. *Module-based deployment*. See Prerequisites before deploying.

     1. Enter the **Management Project ID**. This is the ID of the dedicated project hosting the service account for this integration.
     2. In the Google Cloud Console, navigate to the project you created.
     3. Go to **IAM & Admin** > **Labels**, click **+ Add label**, and add the key/value pair that appears in the AI Exposure wizard.
     4. Copy the module invocation displayed in the AI Exposure wizard, add it to your Terraform configuration, and then run `terraform apply`. The module

creates the identity and grants Tenable the permissions to connect and scan the environment.

- **Manual**. *Manually, via the Google Cloud Console*. See Manually Deploy a GCP Organization for step-by-step instructions.

  > **Caution:** When you finish manual deployment, return to the wizard to complete Post Deployment, and Step 2: Scopes and Hierarchy.

6. Under **Post Deployment**, enter the following values.

   > **Note:** Keep the following in mind about the integration values:
   > - **How to retrieve values**
   >   - *Cloud Shell*: Copy/paste the values from the script output.
   >   - *Terraform*. Retrieve the values from the Terraform output.
   >   - *Manual*: See Manually Deploy a GCP Organization for how to retrieve these values.
   > - **Shared integration values**
   >   - These values must be identical across the organization and all its member projects.
   >   - When an organization is connected, these fields can only be updated at the organization level. Changes will automatically propagate to all member projects.

   - **Service Account Email**
   - **Pub/Sub Subscription Name**

7. When finished, click **Next**.

4. In the **Scopes** step (step 2 of 2):

   1. (Optional) Select Automatically update compartments structure to mirror your compartment's structure as folders within Tenable, preserving the hierarchy and keeping the view synchronized. For more information, see Account Hierarchy and Folders.
   2. Under **Scopes**, choose which compartments to onboard:

- **Sync all current and future projects (recommended)**
- **Include specific folders and projects**
- **Exclude specific folders and projects**

> **Note:** If you include/exclude an entire folder, all current and future projects within the group are included/excluded. If you include/exclude specific projects in a folder, only the selected projects will be included/excluded.

5. Click **Finish**.

> **Note:** Due to access change propagation in GCP, it may take some time for permission changes to be applied in your cloud environment. If you see an error that the *service account permissions are missing or misconfigured* when you try to click Finish, please wait a few minutes and then try again.

Next steps:

After your organization is added successfully:

- You can see the organization on the **Integrations > GCP Organization** page.
- You can see projects that belong to the organization on the **Accounts > GCP** page. From here you can manage your projects and view project details to see, for example, which features are enabled and whether the required permissions were granted.

Data about project resources will start to appear in AI Exposure. The time it takes for all data to appear varies depending on the size of your cloud environment.

Manually Deploy a GCP Organization

> **Note:** When you finish manual deployment, return to the wizard to complete Post Deployment, and Step 2: Scopes and Hierarchy.

As an alternative to the script-based deployment, you can manually deploy your GCP organization via the Google Cloud Console. These procedures are relevant if you selected **Manual** for the deployment type when connecting your GCP organization.

1. Create a Service Account for Tenable
2. Authorize the Service Account at the Org Level
3. Configure Audit Logs

Create a Service Account for Tenable

Create a dedicated GCP project and service account that Tenable uses to access and monitor your organization.

1. In the Google Cloud Console, navigate to the project you created.
2. Go to **IAM & Admin** > **Roles** and then click **+ Create custom role**.
3. Enter a title, description, and ID.
4. Click **+ Add permissions**, and add the permissions listed under **Create Service Account** in Required Permissions.
5. Click **Create** to finish creating the role.
6. Go to **IAM & Admin > Service Accounts** and then click **+ Create service account**.
7. Enter a **Service account name**, **ID**, and **description**.
8. Copy and save the service account email that is generated. You will need to enter this value in the Post Deployment section of the wizard when connecting your organization to AI Exposure.
9. Click **Create and continue**.
10. Select the custom role you created, and then click **Continue** and **Done**.
11. Select the newly created service account, click the **Principals with access** tab, and then **Grant access**.

    > **Important:** If you are unable to grant access, you may have an organization policy with a domain restriction constraint that prevents choosing Tenable as a principal in IAM policies. This prevents Tenable from impersonating the created service account. If this is the case, follow the procedure described in Add Tenable as an Allowed Domain.

12. In the Add principals section, enter **ermeticapp@sil-prd.iam.gserviceaccount.com** in the New principals field.

13. In the Assign roles section, select the **Service Account Token Creator** role and then click **Save** to finish.
14. Go to **IAM & Admin** > **Labels**, click **+ Add label**, and add the key/value pair that appears in the AI Exposure wizard:
    - **Key**: `ermetic-external-id`
    - **Value** – Appears in the Deployment section of the AI Exposure wizard
15. Click **Save** to finish creating the service account.

Authorize the Service Account at the Org Level

Grant the service account the permissions Tenable requires to scan and monitor your organization.

1. In the Google Cloud Console, select the organization you want to connect to Tenable using the project picker at the top left of the screen.
2. Navigate to **IAM & Admin > IAM** and then click **Grant access**.
3. In the Add principals section, enter the service account email you saved earlier in the New principals field.
4. In the Assign roles section, select relevant roles according to the desired capabilities.
5. Click **Save** to finish.

Configure Audit Logs

Set up a Pub/Sub topic, subscription, and log sink to stream GCP audit logs to Tenable.

> **Caution:** While Pub/Sub topics and subscriptions are created at the project level, log sinks must be created at the organization level.

1. In the Google Cloud Console, select the relevant project with the project picker and create a Pub/Sub topic by following these steps:
    1. Navigate to **Pub/Sub > Topics** and then click **+ Create topic**.
    2. In the Topic ID field, enter `tenable-audit-logs`.
    3. Clear **Add a default subscription**.

4. Select **Enable message retention** and set the duration to at least 1 day.
5. Click **Create**.

2. Create a Pub/Sub subscription by following these steps:
    1. Navigate to **Pub/Sub > Subscriptions** and then click **+ Create subscription**.
    2. In the Subscription ID field, enter `tenable-audit-logs-sub`.
    3. Select the topic you created earlier.
    4. In the Delivery type section, select **Pull**.
    5. In the Message retention duration section, set the duration to at least 1 day.
    6. In the Retry policy section, select **Retry after exponential backoff delay** and keep the default values.
    7. In the Expiration period section, select **Never expire**.
    8. Click **Create**.
    9. In the Permissions tab of the newly created subscription, click **Add principal**.
    10. In the Add principals section, enter the service account email you saved earlier in the New principals field.
    11. In the Assign roles section, select the **Pub/Sub Subscriber** role and then click **Save** to finish.
    12. Copy and save the Pub/Sub subscription name. You will need to enter this value in the Post Deployment section of the wizard when connecting your organization to AI Exposure.
3. Create a log sink at the organization level by following these steps:
    1. Select the relevant organization with the project picker and navigate to **Logging > Configure > Log router**.
    2. Click **Create sink**.
    3. In the Sink name field, enter `tenable-audit-logs` and then click **Next**.
    4. For the sink service, select **Cloud Pub/Sub topic** and then **Use a Cloud Pub/Sub topic in a project**.

5. In the Sink destination field, replace `[PROJECT_ID]` and `[TOPIC_ID]` with the relevant IDs and click **Next**.
6. Select Include logs ingested by this organization and all child resources, and then paste the following in the inclusion filter:

```
LOG_ID(cloudaudit.googleapis.com/activity) OR
LOG_ID(cloudaudit.googleapis.com/data_access) OR
LOG_ID(cloudaudit.googleapis.com/policy)
```

7. Click **Next**.
8. Click **+ Add exclusion**.
9. In the Exclusion filter name field, enter `exclude-k8s-internal` and then paste the following in the exclusion filter:

```
protoPayload.authenticationInfo.principalEmail-:* OR
protoPayload.authenticationInfo.principalEmail=~"^system:" OR
protoPayload.authenticationInfo.principalEmail=~"@container-engine-
robot.iam.gserviceaccount.com$" OR
protoPayload.authenticationInfo.principalEmail=~"@security-center-
api.iam.gserviceaccount.com$"
```

10. Click **Create sink**.

> **Important:** Even if you are a GCP Organization Admin or Super Admin, Google Cloud segregates logging permissions by default. If you receive the error **Permission `logging.sinks.create` denied on resource** when trying to create the sink, you must explicitly grant your user account the Logging Admin or Logs Configuration Writer role at the organization level.

4. Assign the **Pub/Sub Publisher** role to the service account at the organization level.
    1. Go to **IAM & Admin > IAM**.
    2. Find the service account and click **Edit principal**.
    3. Click **+ Add another role**.
    4. Select **Pub/Sub Publisher**.
    5. Click **Save**.

Connect a GCP Project

Connect an individual GCP project to Tenable to monitor its cloud resources and security posture. To connect all projects in your organization at once, see Connect a GCP Organization.

Prerequisites

Before you begin:

- Grant sufficient permissions to the user who will create projects, create service accounts, authorize the service accounts, and enable logging in the Google Cloud Console.
- Define exceptions to allow Tenable network access if you use VPC Service Controls to restrict access to Google-managed services.
- Verify that your organization does not have a domain restriction policy that would block Tenable as a principal in IAM policies. If it does, Add Tenable as an Allowed Domain.
- Create a dedicated project for each Google Organization (including all its projects) that will host the service account used by Tenable.
- Enable billing for the dedicated project in the Google Cloud Console. For instructions, see Google's documentation on enabling billing{target=_blank}.

Note: Dedicated projects:

- **Prevent API throttling** – GCP enforces API rate limits at the project level. Sharing a project with other service accounts increases the risk of hitting these limits and being blocked.
- **Isolate expenses** – A shared project obscures billing and usage data, making it harder to track the exact costs generated by a Tenable service account.

Connect a Project

Note: Depending on your setup, shared fields are managed differently:

- **If a parent organization integration exists in Tenable** – Some sections contain fields managed at the organization level. To modify these fields, edit the organization integration.

- **If no parent organization integration exists in Tenable** – Some sections contain fields shared across all project integrations in the organization. These fields can only be modified when editing the integration.

FedRAMP: If you use Tenable One AI Exposure in a FedRAMP environment, make sure to connect integrations only to FedRAMP authorized services and endpoints. You are responsible for confirming that each service you connect meets your FedRAMP requirements. Sending data to a service outside your authorization boundary can put your organization out of compliance with FedRAMP requirements.

To connect a GCP project:

1. In the Tenable One AI Exposure Console, navigate to **Settings** > **Integrations** and click **+ Add Integration**.
2. In the Integrations Library, click **GCP Project**. The GCP Project wizard opens.
3. In the wizard:
    1. Enter the project ID of the GCP project you want to connect.
    2. Enter the organization ID. AI Exposure does not currently support projects that are not part of an organization.
    3. Under **Google Workspace**, select whether to use an existing Google Workspace integration. If an integration does not exist, you can click **+ Create**.

        Note: Tenable recommends using your Google Workspace with your organization to enable identity-related visibility and complete risk assessment. Doing so:
        - Enables identity-related visibility, including users, permissions, and least-privilege analysis, providing a more complete risk assessment across your GCP cloud environment.
        - Allows visibility into identities, permissions, and access relationships, enhancing security posture management beyond just resource visibility.
    4. Under **Capabilities**, select the capabilities to enable. Your selection determines the required permissions and dynamically updates the deployment script. Tenable recommends enabling all capabilities to provide the most comprehensive security coverage. For more information, see Google Required Permissions.

5. Under **Deployment**, select one of the following deployment options:
    - **Cloud Shell**. *Script-based deployment*.
        1. Enter the **Management Project ID**. This is the ID of the dedicated project hosting the service account for this integration.
        2. Copy the script displayed in the AI Exposure wizard, create a file with the script content, and then run it in your Cloud Shell to grant AI Exposure the required permissions.
    - **Manual**. *Manually, via the Google Cloud Console*. See Manually Deploy a GCP Project for step-by-step instructions.

      > **Caution:** When you finish manual deployment, return to the wizard to complete Post Deployment.

6. Under **Post Deployment**, enter the following values.

    > **Note:** Keep the following in mind about the integration values:
    > - **How to retrieve values**
    >   - *Cloud Shell*: Copy/paste the values from the script output.
    >   - *Manual*: See Manually Deploy a GCP Project for how to retrieve these values.
    > - **Shared integration values**
    >   - These values must be identical across all projects in the same organization.
    >   - If a parent organization integration exists, these fields are managed at the organization level. Changes propagate automatically to all member projects.

    - **Service Account Email**
    - **Pub/Sub Subscription Name**

4. Click **Finish**.

> **Note:** Due to access change propagation{target=_blank} in GCP, it may take some time for permission changes to be applied in your cloud environment. If you see an error that your organization doesn't exist when you try to click Finish, wait a few minutes and then try again.

Next steps:

After your project is added successfully:

- You can see the project on the **Accounts > GCP** page. From here you can manage your project and view project details to see, for example, which features are enabled and whether the required permissions were granted.

Data about your project resources will start to appear in AI Exposure. The time it takes for all data to appear varies depending on the size of your cloud environment.

Manually Deploy a GCP Project

> **Note:** When you finish manual deployment, return to the wizard to complete Post Deployment.

As an alternative to the script-based deployment, you can manually deploy your GCP project via the Google Cloud Console. These procedures are relevant if you selected **Manual** for the deployment type when connecting your GCP project.

1. Create a Service Account for Tenable
2. Authorize the Service Account at the Org Level
3. Authorize the Service Account at the Project Level
4. Configure Audit Logs
5. Create a Custom Role with Org-Level Permissions

Create a Service Account for Tenable

Create a dedicated GCP project and service account that Tenable uses to access and monitor your project.

1. In the Google Cloud Console{target=_blank}, navigate to the project you created.
2. Go to **IAM & Admin** > **Roles** and then click **+ Create custom role**.
3. Enter a title, description, and ID.
4. Click **+ Add permissions**, and add the permissions listed under **Create Service Account** in Required Permissions.
5. Click **Create** to finish creating the role.

6. Go to **IAM & Admin > Service Accounts** and then click **+ Create service account**.
7. Enter a **Service account name**, **ID**, and **description**.
8. Copy and save the service account email that is generated. You will need to enter this value in the Post Deployment section of the wizard when connecting your organization to AI Exposure.
9. Click **Create and continue**.
10. Select the custom role you created, and then click **Continue** and **Done**.
11. Select the newly created service account, click the **Principals with access** tab, and then **Grant access**.

    > **Important:** If you are unable to grant access, you may have an organization policy with a domain restriction constraint that prevents choosing Tenable as a principal in IAM policies. This prevents Tenable from impersonating the created service account. If this is the case, follow the procedure described in Add Tenable as an Allowed Domain.

12. In the Add principals section, enter **ermeticapp@sil-prd.iam.gserviceaccount.com** in the New principals field.
13. In the Assign roles section, select the **Service Account Token Creator** role and then click **Save** to finish.
14. Go to **IAM & Admin** > **Labels**, click **+ Add label**, and add the key/value pair that appears in the AI Exposure wizard:
    - **Label key**: `ermetic-external-id`
    - **Value** – Appears in the Deployment section of the AI Exposure wizard
15. Click **Save** to finish creating the service account.

Authorize the Service Account at the Org Level

Grant the service account the organization-level permissions Tenable requires to access and monitor your GCP environment. For step-by-step guidance on resolving GCP role and permission errors, see Resolve Cloud Onboarding Permission and Role Errors (AWS, Azure, GCP).

Role bindings in this procedure are granted at the organization level, following Tenable's best-practice recommendations. If you are not planning to connect your entire organization (for example,

as part of a trial), Tenable supports granting these role bindings at the project level instead. In that case, you must still grant a basic set of permissions at the organization level via a custom role, and then contact Technical Support for assistance completing the integration. For more information, see Grant Organization-Level Permissions.

1. In the Google Cloud Console{target=_blank}, select the organization you want to connect to Tenable using the project picker at the top left of the screen.
2. Navigate to **IAM & Admin > IAM** and then click **Grant access**.
3. In the Add principals section, enter the service account email you saved earlier in the New principals field.
4. In the Assign roles section, add the following roles:
    - `Cloud Asset Viewer`
    - `Security Reviewer`
    - `Organization Policy Viewer`
    - `Organization Viewer`
5. Click **Save** to finish.

Authorize the Service Account at the Project Level

Grant the service account the project-level permissions Tenable requires to scan and monitor your project.

1. In the Google Cloud Console{target=_blank}, select the relevant project using the project picker at the top left of the screen.
2. Navigate to **IAM & Admin > IAM** and then click **Grant access**.
3. In the Add principals section, enter the service account email you saved earlier in the New principals field.
4. In the Assign roles section, select relevant roles according to the desired capabilities.
5. Click **Save** to finish.



> **Note:** If you enabled Workload Protection in the Capabilities section, there is an additional step to grant Workload Protection permissions. See the relevant Workload Protection documentation for more information.

Configure Audit Logs

Set up a Pub/Sub topic, log sink, and subscription to stream GCP audit logs to Tenable.

1. In the Google Cloud Console{target=_blank}, select the relevant project with the project picker and create a Pub/Sub topic by following these steps:
    1. Navigate to **Pub/Sub > Topics** and then click **+ Create topic**.
    2. In the Topic ID field, enter `tenable-audit-logs`.
    3. Clear **Add a default subscription**.
    4. Select **Enable message retention** and set the duration to at least 1 day.
    5. Click **Create**.
2. Create a Pub/Sub subscription by following these steps:
    1. Navigate to **Pub/Sub > Subscriptions** and then click **+ Create subscription**.
    2. In the Subscription ID field, enter `tenable-audit-logs-sub`.
    3. Select the topic you created earlier.
    4. In the Delivery type section, select **Pull**.
    5. In the Message retention duration section, set the duration to at least 1 day.
    6. In the Retry policy section, select **Retry after exponential backoff delay** and keep the default values.
    7. In the Expiration period section, select **Never expire**.
    8. Click **Create**.
    9. In the Permissions tab of the newly created subscription, click **Add principal**.
    10. In the Add principals section, enter the service account email you saved earlier in the New principals field.

11. In the Assign roles section, select the **Pub/Sub Subscriber** role and then click **Save** to finish.
12. Copy and save the Pub/Sub subscription name. You will need to enter this value in the Post Deployment section of the wizard when connecting your project to AI Exposure.

3. Create a log sink by following these steps:
    1. Navigate to **Logging > Configure > Log router**.
    2. Click **Create sink**.
    3. In the Sink name field, enter `tenable-audit-logs` and then click **Next**.
    4. For the sink service, select **Cloud Pub/Sub topic** and the relevant topic and then click **Next**.
    5. Paste the following in the inclusion filter:

```
LOG_ID(cloudaudit.googleapis.com/activity) OR
LOG_ID(cloudaudit.googleapis.com/data_access) OR
LOG_ID(cloudaudit.googleapis.com/policy)
```

    6. Click **Next**.
    7. Click **+ Add exclusion**.
    8. In the Exclusion filter name field, enter `exclude-k8s-internal` and then paste the following in the exclusion filter:

```
protoPayload.authenticationInfo.principalEmail-:* OR
protoPayload.authenticationInfo.principalEmail=~"^system:" OR
protoPayload.authenticationInfo.principalEmail=~"@container-engine-
robot.iam.gserviceaccount.com$" OR
protoPayload.authenticationInfo.principalEmail=~"@security-center-
api.iam.gserviceaccount.com$"
```

    9. Click **Create sink**.

Create a Custom Role with Org-Level Permissions

In the procedure outlined above, role bindings are granted at the organization level, following AI Exposure's best practices. However, if you are not planning to connect your entire organization at any point (e.g., as part of a trial), AI Exposure supports granting these role bindings at the project level instead. If you decide to grant role bindings at the project level, AI Exposure still requires that you grant a basic set of permissions at the organization level.

To create a custom role:

1. In the Google Cloud Console{target=_blank}, select the relevant organization using the project picker at the top left of the screen.
2. Navigate to **IAM & Admin** > **Roles** and then click **+ Create custom role**.
3. Enter a title, description, and ID.
4. Click **+ Add permissions**, and add the permissions listed in Org-Level Custom Role for Single-Project Connections.
5. Click **Create** to finish creating the role.
6. Add the custom role to the Tenable service account, on the organization level.

For more information about creating custom roles, refer to the relevant Google Cloud documentation. For more information about why AI Exposure requires organization-level permissions when connecting an individual project, see Grant Organization-Level Permissions.

Google FAQ and Troubleshooting

This article contains:

- A list of frequently asked questions related to onboarding GCP and Google Workspace to Tenable One AI Exposure
- GCP and Google Workspace status and troubleshooting information

GCP FAQs

This section contains a list of frequently asked questions related to onboarding GCP projects/organizations.

Exclude a Folder or Project from an Organization

> How can I exclude a specific folder or project from an organization that I already onboarded?

1. In the Console, navigate to **Settings** > **Integrations**.
2. Click on the three dots menu next to the organization, and click **Edit**.
3. Click **Next** to navigate to the last step in the wizard (Scopes).
4. Select **Exclude specific folders and projects** and then select the relevant folder or project.
5. Click **Finish**. It will be removed from the Console the next time Tenable syncs data in your environment.

Grant Organization-Level Permissions

> When I onboard an individual project, why do I need to grant organization-level permissions to the Tenable service account?

In order to see all relevant role bindings, Tenable needs permissions to be granted on the parent-level scope (organization). Without this ability, Tenable cannot provide critical security information for GCP resources, such as effective permissions. Even though role bindings are granted on the level of the organization, Tenable cannot access any other organization-level data unless the organization itself, or specific projects within it, are onboarded to Tenable.

Project Is Pending Deletion

> Why does a project that I deleted in GCP have a status of Project is pending deletion in Tenable for so long before it's actually deleted?

After you delete a project in GCP, it takes 30 days until the project is fully deleted. After this 30 day period, Tenable will offboard the project automatically from the system. Since Google Cloud allows you to revert the deletion during this time period, Tenable doesn't delete the data from the system until after 30 days, allowing you to restore the project in GCP if you wish. For more information, refer to the relevant Google documentation{target=_blank}.

User in Domain Considered External

> Why do I see a user that is part of my organization's domain in the Users (external) resource type category in the Tenable inventory? Why would such a user be considered external (not defined locally in Workspace)?

It's possible that some members of your organization independently created Google accounts using the domain of your organization. Such accounts are considered unmanaged user accounts by Google, and are categorized by Tenable as external. Refer to Google documentation{target=_blank} for more information.

Update the Integration Name for the Organization

You can modify the name of your GCP organization integration/s, reflecting how the integration is displayed in AI Exposure. This can be useful for better identification, especially if you have multiple organizations.

To update the name:

1. In the AI Exposure Console, navigate to **Settings** > **Integrations**.
2. Next to the relevant integration, click the three dots menu, and then **Edit**.
3. Navigate to step 2 in the wizard and update the **Organization Name** field.
4. Click **Next** to navigate to the last step in the wizard and then click **Update**.

Terraform Deployment

> Is GCP project onboarding via Terraform supported?

Terraform is only supported for GCP organizations.

Google Workspace FAQs

This section contains a list of frequently asked questions related to onboarding Google Workspace.

Service Account Token Creator Role

> When I add a Google Workspace, why does the Service Account Token Creator role need to be granted to the principal (ermeticapp@sil-prd.iam.gserviceaccount.com) that has access to the service account that grants Tenable access to my environment?

Although the name of this role might be misleading, it effectively allows Tenable to impersonate {target=_blank} (or "assume") the service account to interact with your environment via queries.

This is the safest method Tenable has found to connect to your GCP environment as a third party.

The alternative, which is sometimes used by other vendors, is to create user-managed access keys. This requires manual rotation, and can be compromised. The benefit of using impersonation here is that it reduces your risk exposure by not having static credentials associated with Tenable's service account. See Service Account Impersonation vs. Service Account Key.

Service Account Impersonation vs. Service Account Key

> Why does Tenable use service account impersonation and not a service account key?

According to GCP documentation{target=_blank}, service account impersonation is more secure than using a service account key, because impersonation requires a prior authenticated identity, and the credentials that are created do not persist. In comparison, authenticating with a service account key requires no prior authentication, and the persistent key is a high risk credential if exposed.

Super Administrator User (Advanced)

Note: Only relevant if you grant permissions via domain-wide delegation (advanced). AI Exposure recommends granting permissions via custom role for most organizations.

> When I add a Google Workspace, why does Tenable require the email address of a super administrator user? How does Tenable limit risk associated with such wide access? And why does Tenable need an email address at all?

Tenable needs to access certain Google APIs in your environment that require the super administrator user. These are needed for identity and other general cloud security capabilities. Here is a partial list of APIs:

- https://developers.google.com/admin-sdk/reference-overview
- https://cloud.google.com/identity/docs/apis

However, the actual permissions granted to Tenable are restricted to the OAuth scopes granted when you add your workspace. These permissions are all read-only. So, although Tenable needs super administrator permissions to access the required APIs, in practice, only read-only permissions are actually granted, thus limiting risk.

Tenable needs an email address, because the only way to query objects in Google Workspace is by using domain-wide delegation and user impersonation, which requires a user email address. For more information about how service accounts should access Google Workspace, refer to Google documentation{target=_blank}. Mailbox is not required for this user.

Domain-Wide Delegation (Advanced)

> **Note:** Only relevant if you grant permissions via domain-wide delegation (advanced). AI Exposure recommends granting permissions via custom role for most organizations.

> What is domain-wide delegation, and why do I need to use it to grant Tenable access when I add a Google Workspace?

Domain-wide delegation is a Google Workspace mechanism used to grant applications with domain-wide access to relevant user data. This delegation of authority is done using service accounts with OAuth 2.0. The access granted via this delegation is what allows Tenable to gather and provide information fundamental to understanding your GCP assets, since Google Workspace is inherently connected to GCP.

Without this access, Tenable would be unable to:

- Map Google Workspace users to the GCP resources they use.
- Map Google Workspace users to groups, since GCP permissions can be granted to groups.
- Build user/group permission graphs
- Identify users with strong Google Workspace permissions who can therefore escalate their privileges in GCP (e.g., Super Administrators).

Domain-wide delegation lets Tenable impersonate any Google Workspace user, including administrators. Despite the fact that, technically speaking, it might appear as if Tenable has super administrator permissions, this is not actually the case in practice: Tenable does not have any administrator permissions within Google Workspace. The actual permissions granted to Tenable are restricted to the specific OAuth scopes defined during the configuration of domain-wide delegation: These permissions only grant Tenable read access to Google Workspace.

Important: You must grant Tenable this access in the form of a super administrator user, and not via a custom role. There are some permissions that are only available to super admins, and unavailable when creating custom roles. For example, the following oauth scopes:
https://www.googleapis.com/auth/admin.directory.rolemanagement.readonly
https://www.googleapis.com/auth/admin.reports.audit.readonly

For more information refer to the relevant Google Workspace documentation:
https://developers.google.com/admin-sdk/directory/v1/guides/delegation

Quota Administrator Role (Legacy)

Note: This section is only relevant if you onboarded your Google Workspace before April 27, 2025.

When I add a Google Workspace, why does the Quota Administrator role need to be added to the service account that grants Tenable access to my environment?

This role contains permissions to manage API access for the Tenable service account, which is needed by Tenable to:

- Query some of the services that you're currently using in your environment.
- Automatically support new GCP services as they are released.

Although the name of this role might be misleading, it effectively allows Tenable to enable APIs needed to collect configuration data from your GCP environment. Without this ability, Tenable wouldn't be able to perform the functions mentioned above.

Since quotas are managed in GCP{target=_blank} per project, and Tenable's service account belongs to a single project, the permissions contained in this role are limited in scope. Unless you

explicitly enable API access for a service in a different project, Tenable will not have access to it. Even though Tenable's service account can query new services from the dedicated project that you added during the onboarding process, it cannot alter quotas in your environment.

AI Exposure currently maps all services and permissions in your GCP environment programmatically, meaning that as soon as a new GCP service is released, you can view it in Tenable, along with its underlying permissions.

Project Status and Troubleshooting

AI Exposure displays a **Status** for each project on the **Accounts > GCP** page, indicating whether Tenable can connect to the project, and helping you troubleshoot potential onboarding issues. For step-by-step guidance on resolving GCP role and permission errors, see Resolve Cloud Onboarding Permission and Role Errors (AWS, Azure, GCP).

Status	Description
Connected	Tenable successfully connected to the project, and the project is up and running.
Deleting... this may take up to an hour	You deleted the project in Tenable, and the process hasn't completed yet.
Failed to connect	Tenable failed to connect to the project. This might happen because the project was deleted in GCP, but not deleted from the AI Exposure Console.
Google workspace is not connected	The Google workspace is not connected. See Connect a Google Workspace for more information.
Missing permissions	One or more of the listed roles are missing, and need to be added to the Tenable service account.

Status	Description
Project is deleted	You deleted the project in Tenable. The project will be removed the next time data is synced in Tenable.
Project is pending deletion	After you delete a project in GCP, it takes 30 days until the project is fully deleted. After this 30-day period, Tenable will offboard the project automatically from the system. Since Google Cloud allows you to revert the deletion during this time period, Tenable doesn't delete the data from the system until after 30 days, allowing you to restore the project in GCP if you wish. For more information, refer to the relevant Google documentation.
Project is suspended	The project is suspended in GCP. The project will remain in this state until changed in GCP.
Some features are disabled	Billing is disabled in GCP for the project where you created the Tenable service account. This causes limitations on queries to this account. Some AI Exposure features, such as findings on inactive service accounts and Kubernetes visibility and security, will be disabled until a billing account is connected. Refer to the relevant Google Cloud documentation for more information about project billing.
Subscription is not configured	The Pub/Sub subscription used to collect audit logs (activity logs) from the GCP project is not configured. As a result, audit logs are not being sent to AI Exposure. See Connect a GCP Organization.

Workspace Status and Troubleshooting

AI Exposure displays a **Status** for each Workspace on the **Integrations > Google Workspace** page, indicating whether Tenable can connect to the Workspace and helping you troubleshoot potential onboarding issues.

Status	Description
Service Usage API is not enabled	Enable at the project level where the service account was created.
Missing permissions	• Ensure the Tenable service account has the required permissions. • Ensure the AI Exposure principal was granted the **Service Account Token Creator** role.
Missing label	Ensure the label exists and has the relevant key/value pair.
Missing OAuth scopes	Ensure all required OAuth scopes are added via domain-wide delegation.

Ticketing and ITSM

Jira

Integrate your Jira projects with Tenable One AI Exposure to support the creation of issues related to specific findings in Tenable. Tenable supports integration with both Jira Software (on premises, version 8.5.3 and above) and Jira Software Cloud.

To integrate your projects with Tenable, you need to:

1. Add a Jira Instance - Connect a Jira instance to Tenable using OAuth, a password or API token, or a personal access token. Must be an admin user.
2. Add a Jira Space - Integrate one or more Jira projects with Tenable by granting the dedicated Tenable user permission to the projects.

What to do next:

- To start creating issues for findings, you need to also configure automation rules or manually trigger an action after you integrate a tool. Successfully completing all integration steps does not trigger the sending of any data on its own.

Before You Begin

Adding a Jira instance to AI Exposure requires a dedicated Jira identity and one of three authentication methods:

- OAuth 2.0
- A password or API token
- A personal access token (PAT)

Tenable recommends OAuth. Although you can use an existing Jira user, Tenable recommends that you create a dedicated user or service account to simplify audit-trail activities. If needed at a later date, you can remove the Jira identity to terminate the integration.

Complete the setup for your chosen authentication method in Jira before you start the wizard.

> **FedRAMP:** If you use Tenable One AI Exposure in a FedRAMP environment, make sure to connect integrations only to FedRAMP authorized services and endpoints. You are responsible for confirming that each service you connect meets your FedRAMP requirements. Sending data to a service outside your authorization boundary can put your organization out of compliance with FedRAMP requirements.

Set Up an OAuth 2.0 Credential

Create an OAuth 2.0 credential for a Jira service account. The integration runs as that service account and inherits the scopes you grant the credential. If you do not already have a service account, create one first. For more information, see the Atlassian documentation.

To create an OAuth 2.0 credential:

1. In Atlassian Administration, select your organization (if you have more than one).
2. Navigate to **Directory** > **Service accounts**.

3. Select the service account to create a credential for.
4. Click **Create credentials**.
5. Select **OAuth 2.0**, and then click **Next**.
6. Select the following scopes to determine what the credential can do in Jira:
    - `write:jira-work`
    - `read:jira-work`
    - `read:jira-user`
    - `read:priority:jira`
7. Click **Next**.
8. Review the OAuth information, and then click **Create**.
9. Copy the **Client ID** and **Client secret**.

> **Important:** You cannot recover the Client ID and Client secret after you create the credential. Tenable recommends that you save them in a password manager.

Set Up a Jira User

For **password or API token** or **personal access token** authentication, create a dedicated Jira user with:

- **Product access** to the Jira product that your project belongs to (for example, Jira Software). To identify the product, in the Jira console (not the Admin page), navigate to **Projects** > **View all projects**, and then use the dropdown filter.
- The following project permissions, granted via the permission scheme for the user's project:
    - Assign issues
    - Browse projects
    - Create attachments
    - Create issues
    - Edit issues

Then create the credential for your method:

- (Password or API token) Create an API token. Create an API token for the Jira user. For the steps to create an API token, see the Atlassian documentation.
- (Personal access token) Create a personal access token. Create a personal access token (PAT) for the Jira user. For the steps to create a personal access token, see the Atlassian documentation.

Add a Jira Instance

After you complete the prerequisites, add the Jira instance from the AI Exposure Console.

To add a Jira instance:

1. In the AI Exposure Console, navigate to **Settings** > **Integrations**.
2. (Optional) Select an account scope in the Organization dropdown.
3. Click **Add Integration**.
4. In the Integrations Library, click **Jira**. The Jira wizard opens.
5. Activate the Jira instance:
    1. Enter your Jira **Instance URL**.

        > **Note:** You can find your Jira URL in the Atlassian Administration console, in the account profile area, on the **Products** page.

    2. Under **Authentication**, do one of the following:
        - To use OAuth, select **OAuth (recommended)**, and then enter the **Client ID** and **Client secret** from the OAuth 2.0 credential you created in Jira.
        - To use a password or API token, select **Password or API token**, and then enter the **User name** (email address) and the **User password or API token** of the Jira user you created.
        - To use a personal access token, select **Personal access token (PAT)**, and then enter the token you created.
    3. Click **Finish**.

After your instance is added successfully, it appears in the AI Exposure Console, in the table in Settings > Integrations > Jira.

Add a Jira Space

Before you can add a Jira space, you must first Add a Jira Instance.

To add a Jira space:

> **Note:** During the wizard, you navigate back and forth between the AI Exposure Console and your Jira Software instance.

1. In the AI Exposure Console, navigate to **Settings** > **Integrations** and find the relevant Jira instance you created.
2. Click the three dots next to an instance name, and then click **Add Space**. The Add Jira Space wizard opens.
3. **Configure the space** (Step 1 in wizard). Grant the Tenable service account or user you created when you added a Jira instance permission to the Jira project, and then enter the space's key:
    1. In your Jira Software instance, navigate to the **Projects** page and select the project you want to add.
    2. Find the project, and then navigate to **Project settings** in one of the following ways:
        - Click the three dots next to the project, and then click **Project settings**.
        - Click the project, and then navigate to **Project settings**.
    3. Navigate to **People**, and then click **Add people**.
    4. Enter the email address of the service account or user you created when you added a Jira instance, select a **Role**, and then click **Add**.
    5. In the AI Exposure Console, enter the **Space Key**. You can find the project key in your Jira Software instance on the Projects page.
    6. Click **Next**.

4. **Sync Work Item Priorities** to align the severity of findings in Tenable with the corresponding priority in Jira (Step 2 in wizard). Jira tickets created via Tenable are assigned the chosen priority. When finished, click **Next**.
    - **Do not sync**
    - **Sync using custom mapping** – For each **Finding Severity** in Tenable, assign a **Jira Issue Priority**.
5. **Sync Work Item Statuses** to align the statuses of findings in Tenable with the corresponding status in Jira (Step 3 in wizard). Jira tickets created via Tenable are assigned the chosen status. When finished, click **Next**.

    > **Note:** This feature requires additional permissions and configuration in Jira. See Allow Jira Issue Transitions for more information.

    - **Do not sync**
    - **Sync issues using custom mapping**.
        1. For each **Issue Type** in Tenable, choose whether to **sync using custom mapping**.
        2. For each **Finding Status** in Tenable, assign a **Jira Issue Status**.
6. Click **Finish**.

After your space is added successfully, it appears in the table in Settings > Integrations > Jira.

> **Important:** To start creating issues for findings, you need to configure automation rules or manually trigger an action after you integrate with Jira. Successfully completing all integration steps does not trigger the sending of any data on its own.

Allow Jira Issue Transitions

To transition Jira issues between statuses, you need to verify that it is allowed in the project *workflow*. A workflow is a set of statuses and transitions that an issue moves through during its lifecycle, and typically represents a process within your organization. If the transition is not allowed in your workflows, you need to configure additional transitions that allow Tenable to move issues.

Example:

Your workflow might dictate that an issue with a status of *To Do* cannot transition to *Done* without

first moving to *In Progress*. However, this means that when an *Open* finding becomes *Closed* in AI Exposure, your workflow would not allow the status transition, because it was not moved to *In Progress* first. To allow AI Exposure to bypass such transition limitations, you need to configure additional transitions in Jira.

Finding Status	Jira Status
Open	To Do
-	In Progress
Closed	Done

Note: Before you configure additional Jira transitions, first define a custom mapping between Tenable finding statuses and Jira issue statuses in Add a Jira Space.

To configure Jira transitions for Tenable:

1. **Add a project role:**
    1. In the relevant project, navigate to **Settings** > **System**.
    2. Under SECURITY, click **Project roles**. The Project Role Browser displays, which contains a list of all the project roles in your Jira site.
    3. Under *Add Project Role* at the bottom of the page, enter a meaningful name and description. For example:
        - *Name*: **AI Exposure Project Role**
        - *Description*: **Used in the project's workflow to set transition permissions**.
    4. Click **Add Project Role**.
2. **Assign a user or group to the project role:**
    1. Navigate back to the same project, click **Back to project**, and then click **Project settings**.
    2. Click **People**.
    3. Click **Add people** in the top right corner.

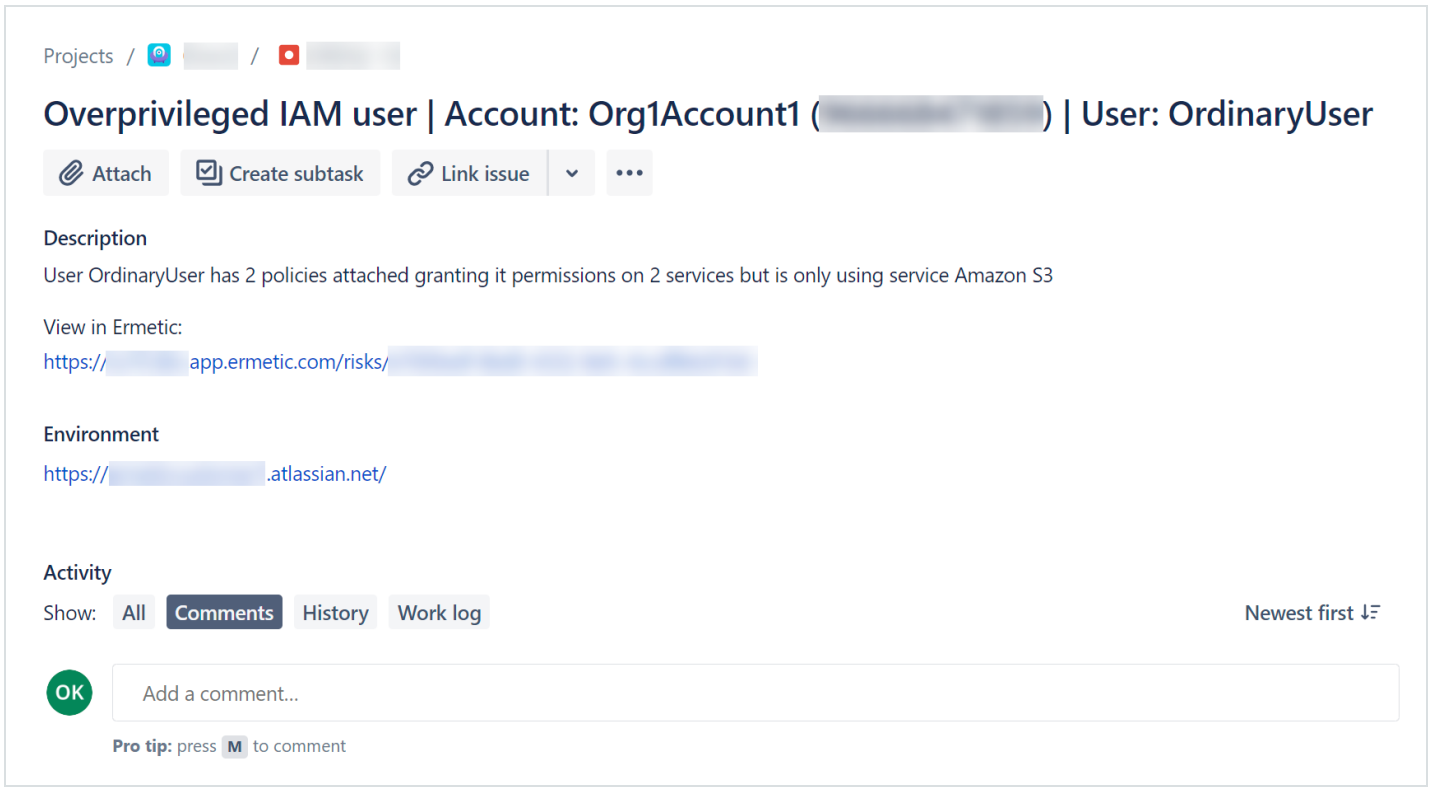
4. Select the **name** of the user that you created when you added your Jira instance in AI Exposure.

   > **Note:** Select the *user name* and not the *email address* of the relevant user.

5. Select the **Role** that you created earlier (*AI Exposure Project Role*).
6. Click **Add 1 person**.

3. **Add a workflow transition:**
   1. Click **Back to project**, and then click **Project settings**.
   2. Click **Workflows**.
   3. Select the relevant workflow, and then click **Edit**.
   4. In the **Diagram** view, click **Add transition**.
   5. In the dialog, complete the following fields:
      - *From status*: **Any status**
      - *To status*: **Done**
      - *Name*: **Any to Done**
   6. Click **Add**.
   7. In the diagram, next to the DONE status, click **All**.
   8. Click **Conditions**.
   9. At the bottom of the page that opens, click **Add condition**.
   10. Select the **User is in Project Role** option, and then click **Add**.
   11. Select the **Project Role** you created in the previous step, and then click **Add**.
   12. Repeat the above steps to add another transition from *Any Status* to *To Do*.
   13. When ready, click **Publish Draft** at the top of the Workflows page.

Sample Jira Issue



ServiceNow

Integrate your ServiceNow instance with Tenable One AI Exposure to support the creation of incidents related to specific findings in Tenable.

What to do next:

- To start creating issues/incidents for findings, you need to also configure automation rules or manually trigger an action after you integrate a tool. Successfully completing all integration steps does not trigger the sending of any data on its own.

Before You Begin

You can authenticate the integration with OAuth 2.0 or basic authentication. Tenable recommends OAuth. Both methods require a dedicated ServiceNow user. OAuth requires one additional step: registering an OAuth application that runs as that user.

Tenable recommends a dedicated user to simplify audit-trail activities. If you no longer need the integration, you can remove the user to terminate it.

Complete the following in your ServiceNow instance before you start the wizard:

- **Create a ServiceNow user** – Required for both authentication methods. Create a dedicated user and select the **Web service access only** option. Tenable recommends a **Global** user so that all data is visible. Grant roles according to the authentication method you use:
  1. For basic authentication, grant the `itil` role.
  2. For OAuth, grant the `itil`, `sn_incident_read`, and `sn_incident_write` roles.

  > **Note:** Tenable recommends a **Global** user so that all data is visible. The user must be able to create and update incidents and view users and groups.

- (OAuth only) Register an OAuth application. To authenticate with OAuth, register an OAuth application in ServiceNow that uses the Client Credentials grant. The application runs as the user you created above and inherits only that user's permissions:
  1. In your ServiceNow instance, navigate to **System OAuth** > **Inbound Integrations**.
  2. Click **New Integration**, and then select **OAuth - Client credentials grant**.
  3. For **OAuth Application User**, select the dedicated user you created.
  4. Set the **Auth scope** to **Restricted** so that the application inherits only the permissions of that user.
  5. For **Limit authorization to the following APIs**, choose **Attachment API** and **Table API**
  6. Copy the generated **Client ID** and **Client secret**.

  > **Note:** The minimum access token lifespan is 5 minutes (300 seconds).

Add an Instance

After you complete the prerequisites, add the ServiceNow instance from the AI Exposure Console.

> **FedRAMP:** If you use Tenable One AI Exposure in a FedRAMP environment, make sure to connect integrations only to FedRAMP authorized services and endpoints. You are responsible for confirming

that each service you connect meets your FedRAMP requirements. Sending data to a service outside your authorization boundary can put your organization out of compliance with FedRAMP requirements.

To add a new instance:

1. In the AI Exposure Console, navigate to **Settings** > **Integrations**.
2. (Optional) In the Organization dropdown, select an account scope.
3. Click **Add Integration**.
4. In the Integrations Library, click **ServiceNow**. The ServiceNow wizard opens.
5. Activate the instance (Step 1 in wizard):
    1. Enter an **Instance Name** for the instance in Tenable.
    2. Enter the **Instance URL** of your ServiceNow instance.
    3. Under **Authentication**, do one of the following:
        - To use OAuth, select **OAuth**, and then enter the **Client ID** and **Client secret** from the OAuth application you registered in ServiceNow.
        - To use basic authentication, select **Basic**, and then enter the **User name** (ID) and **Password** of the ServiceNow user you created.

        See Before You Begin for more information.
    4. Click **Next**.
6. **Sync Incident Priorities** to align the severity of findings in Tenable with the corresponding impact/urgency of incidents in ServiceNow (Step 2 in wizard). ServiceNow incidents created via Tenable are assigned the chosen priority. When finished, click **Next**.
    - **Do not sync**
    - **Sync using custom mapping** – For each **Finding Severity** in Tenable, assign a **ServiceNow Incident Impact** and a **ServiceNow Incident Urgency**.
7. **Sync Incident States** to align the statuses of findings in Tenable with the corresponding state in ServiceNow (Step 3 in wizard). ServiceNow incidents created via Tenable are assigned the chosen state. When finished, click **Next**.

> **Note:** This feature requires additional permissions and configuration in ServiceNow. See Sync Incident States with Finding Statuses for more information.

- **Do not sync**
- **Sync using custom mapping**.
  - For each **Finding Status** in Tenable, assign a **ServiceNow Incident State**.
  - Choose whether to **Create** a **new incident when** a **finding is reopened**.

> **Important:** The *Closed* and *Canceled* states in ServiceNow are considered final and cannot be reverted to an active state. Once an incident reaches one of these states, it is effectively retired from the incident lifecycle. As a result, if you map a finding status to one of these states, you cannot choose to create a new incident when a finding is reopened. To ensure findings can be reopened and tracked, consider mapping findings to a non-final ServiceNow state.

8. **Assignment Groups**: Exclude to stop AI Exposure from assigning incidents to specific ServiceNow assignment groups (Step 4 in wizard). AI Exposure disables excluded groups wherever you or the system can select an assignment group.
   - **Allow all** – No groups are excluded. This is the default.
   - Select the groups to exclude.

> **Note:** Automation rules that already use an excluded group keep running as before. After you remove an excluded group from a rule, you cannot select it again.

After your instance is added successfully, it appears in the table in Settings > Integrations > ServiceNow.

> **Important:** To start creating issues/incidents for findings, you need to also configure automation rules or manually trigger an action after you integrate a tool. Successfully completing all integration steps does not trigger the sending of any data on its own.

Sync Incident States with Finding Statuses

You can sync ServiceNow incident states with AI Exposure finding statuses by granting Tenable an extra level of permissions. This is done by importing a custom update set created by Tenable.

To sync incident states with findings statuses:

1. In your ServiceNow instance, navigate to **Retrieved Update Sets** (under System Update Sets).
2. Under Related Links, click **Import Update Set from XML**.
3. Choose and **Upload** the following XML file:

   ServiceNowSyncIncidentStates.xml
4. Click to open the newly created **Tenable Role Update Set - Incident States**.
5. Click **Preview Update Set**. The Update Set Preview dialog displays. When finished, click **Close**.
6. Verify that no conflicts (Collisions) exist.
7. Review the changes (Customer Updates), and then click **Commit Update Set**. The Update Set Commit dialog displays. When finished, click **Close**. The State of the update set should now be *Committed*.
8. Navigate to **Users and Groups > Users**.
9. Find and click on the **User ID** of the Tenable user you created when you added a ServiceNow instance.
10. Navigate to the **Roles** section at the bottom of the page and then click **Edit...**.
11. Add the Tenable role to the Roles List:
    - From the left-hand *Collection* area, search for and select **tenable_state_readonly_role**.
    - Click on the Add button (>) to move the role to the **Roles List** on the right side.

    Important: Make sure the **itil** role is also in the Roles List on the right side. This role was granted when you added a ServiceNow instance, and is needed for the integration to work.
12. Click **Save**.

Use Additional Fields in Incidents

By default, Tenable supports customizing a basic set of relevant fields when creating ServiceNow incidents via AI Exposure actions. These include the *Assignee*, *Assignment group*, *Category*, *Impact*, *Urgency*, *Summary*, and *Description* fields.

- You can customize additional fields by granting Tenable an extra level of permissions beyond those granted when you integrated with ServiceNow. This is done by importing a custom update set created by Tenable.
- See Supported Fields to understand which additional fields you can use.

To use additional fields in incidents:

1. In your ServiceNow instance, navigate to **Retrieved Update Sets** (under System Update Sets).
2. Under Related Links, click **Import Update Set from XML**.
3. Choose and **Upload** the following XML file:

   ServiceNowAdditionalFields.xml
4. Click to open the newly created **Tenable Role Update Set - Additional Fields**.
5. Click **Preview Update Set**. The Update Set Preview dialog displays. When finished, click **Close**.
6. Verify that no conflicts (Collisions) exist.
7. Review the changes (Customer Updates), and then click **Commit Update Set**. The Update Set Commit dialog displays. When finished, click **Close**. The State of the update set should now be *Committed*.
8. Navigate to **Users and Groups > Users**.
9. Find and click on the **User ID** of the Tenable user you created when you added a ServiceNow instance.
10. Navigate to the **Roles** section at the bottom of the page and then click **Edit...**.
11. Add the Tenable role to the Roles List:

- From the left-hand *Collection* area, search for and select **tenable_fields_readonly_role**.
- Click on the Add button (>) to move the role to the **Roles List** on the right side.

Important: Make sure the **itil** role is also in the Roles List on the right side. This role was granted when you added a ServiceNow instance, and is needed for the integration to work.

12. Click **Save**.

Supported Fields

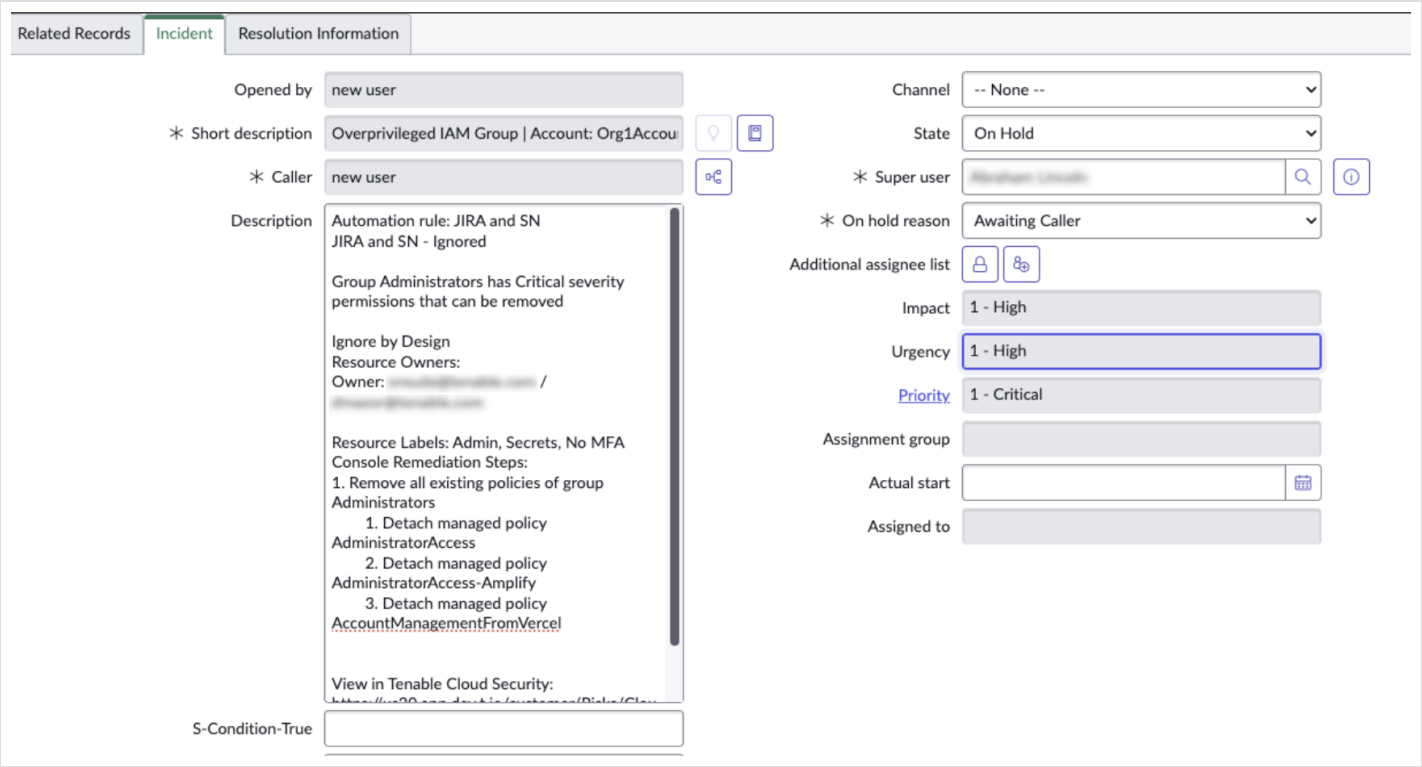
Tenable only supports customizing fields that meet **all** of the following criteria:

- Field is *not dependent* on the value of another field.
- Field is *visible* (not hidden by UI Policy that applies unconditionally).
- Field is *writable*. A field is excluded if it is marked *read-only* in the Dictionary, a Dictionary Override, or by a UI Policy that applies unconditionally.
- Field type is *supported* (string, choice, integer, reference).
- Fields restricted by a UI Policy with conditions remain fully available (visible, optional, writable). Since Tenable can detect that conditions exist but cannot evaluate them, these fields are flagged with a "(UI-Policy)" label and tooltip.

The following fields are *never shown:*

- `number` (auto-generated by ServiceNow)
- `state` (managed separately)

Sample ServiceNow Incident



SIEM

Datadog

Integrate with Datadog to send Tenable One AI Exposure findings to your Datadog organization/s.

What to do next:

- To start sending data for findings, you need to also configure automation rules or manually trigger an action after you add the integration. Successfully completing all integration steps doesn't trigger the sending of any data on its own.

Add a Datadog Organization

> **FedRAMP:** If you use Tenable One AI Exposure in a FedRAMP environment, make sure to connect integrations only to FedRAMP authorized services and endpoints. You are responsible for confirming that each service you connect meets your FedRAMP requirements. Sending data to a service outside

your authorization boundary can put your organization out of compliance with FedRAMP requirements.

To add a Datadog organization:

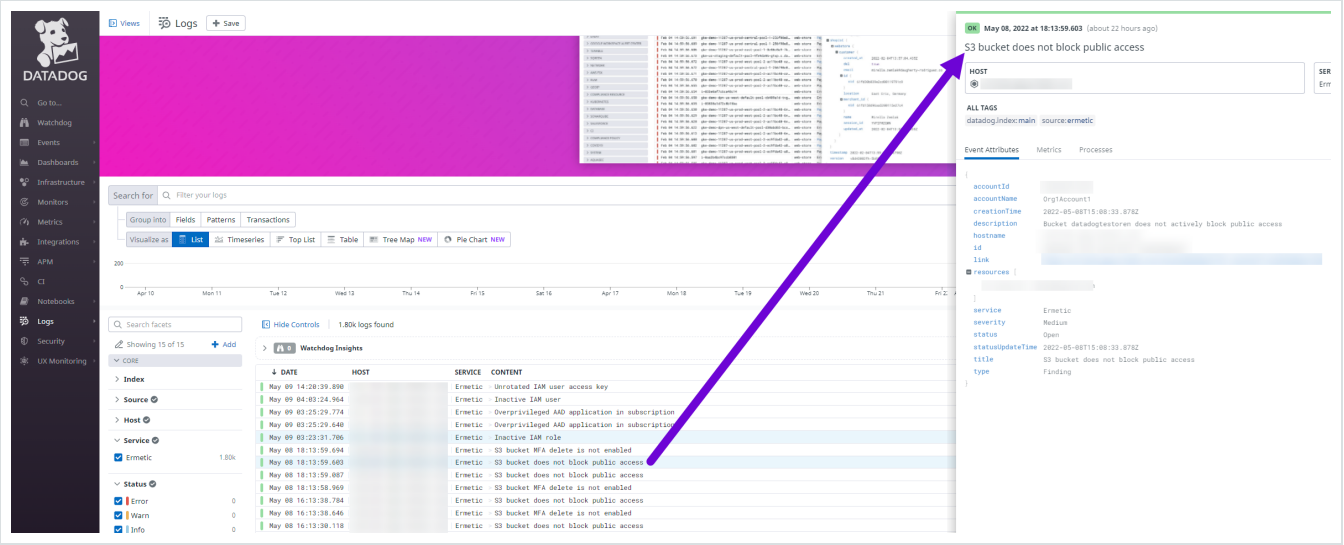
1. In the AI Exposure Console, navigate to **Settings > Integrations**.
2. (Options) Select a scope in the Organization dropdown.
3. Click **Add Integration**.
4. In the Integrations Library, click **Datadog**. The Datadog wizard opens.
5. Enter the **Organization Name** of your Datadog organization.
6. Select your Datadog **Site** from the dropdown. You can identify which site you're on by matching your Datadog website URL to the site URL listed in the Datadog documentation.
7. Enter a Datadog **API Key**. To add a new API key in the Datadog user interface:
    1. Log in to the Datadog user interface, navigate to Organization settings (next to your user name), and then click the **API keys** tab.
    2. Click the **New Key** button.
    3. Enter a name for your key or token.
    4. Click **Create API key**.
8. Click **SAVE**.

Important: To start sending notifications for findings, you need to configure automation rules after you integrate with Datadog. Successfully completing all integration steps doesn't trigger the sending of any data on its own.

View Tenable Findings in Datadog

To view findings in Datadog:

1. Log into your Datadog organization.
2. Navigate to **Logs** and search for logs with Ermetic listed as the Service.



Sample JSON

JSON

```
{
    "id": "***",
    "content": {
        "timestamp": "2022-05-08T12:31:25.909Z",
        "tags": [
            "source:ermetic"
        ],
        "host": "***",
        "service": "Ermetic",
        "attributes": {
            "status": "Open",
            "hostname": "***",
            "description": "***",
            "service": "Ermetic",
            "labels": [
                "Admin"
            ],
            "creationTime": "2022-05-08T12:15:16.164Z",
            "accountName": "Org1Subscription1",
            "link": "***",
            "statusUpdateTime": "2022-05-08T12:15:16.164Z",
            "accountId": "***",
            "type": "Finding",
```

```
            "id": "***",
            "resource": [
                "azure-cli-2021-01-19-07-49-00"
            ],
            "severity": "Critical",
            "policyName": "Inactive AAD application in subscription",
            "ticketLinks": [
                "https://tenablecustomer1.atlassian.net/browse/DAV-24140",
                "https://tenablecustomer1.atlassian.net/browse/DAV-24144",
                "https://tenablecustomer1.atlassian.net/browse/DAV-24148",
                "https://tenablecustomer1.atlassian.net/browse/DAV-24152"
            ],
            "comments": [
                {
                    "message": "created a ServiceNow incident for this threat story",
                    "time": "2026-07-29T09:00:13.124307Z",
                    "userName": "Tenable"
                },
                {
                    "message": "created a Jira ticket for this threat story",
                    "time": "2026-07-29T09:00:05.609867Z",
                    "userName": "Tenable"
                }
            ]
        }
    }
}
```


QRadar

Integrate with IBM QRadar (version 7.3.2 and above) to send Tenable One AI Exposure findings to your QRadar server/s.

What to do next:

- To start sending data for findings, you need to also configure automation rules or manually trigger an action after you add the integration. Successfully completing all integration steps doesn't trigger the sending of any data on its own.

Add a QRadar Server

This integration supports both *internet-facing* and *network-isolated* servers. See Connect Network-Isolated Servers for more information about working with network-isolated servers.

Note: The Tenable QRadar extension XML used to integrate with QRadar is static. This means that, as new versions of AI Exposure are released, any new finding types released by Tenable will be displayed in QRadar as unknown events. To ensure that such events are displayed properly, you will need to re-upload the Tenable extension in the QRadar Console.

FedRAMP: If you use Tenable One AI Exposure in a FedRAMP environment, make sure to connect integrations only to FedRAMP authorized services and endpoints. You are responsible for confirming that each service you connect meets your FedRAMP requirements. Sending data to a service outside your authorization boundary can put your organization out of compliance with FedRAMP requirements.

To add a QRadar server:

Note: Be aware that during the wizard you will need to navigate back and forth between the AI Exposure Console and the IBM QRadar Console. Most steps in this task are performed in the IBM QRadar Console, unless indicated otherwise.

1. In the AI Exposure Console, navigate to **Settings > Integrations**.
2. (Options) Select a scope in the Organization dropdown.
3. Click **Add Integration**.
4. In the Integrations Library click **QRadar**. The QRadar wizard opens.
5. Add the Tenable extension in QRadar (Step 1 in wizard):
    1. Download the Tenable QRadar extension using the link in the wizard.
    2. In the IBM QRadar Console, navigate to the **Admin** page, and then click on **Extensions Management**.
    3. Click **Add**, and then browse to the location where you saved the Tenable QRadar extension.
    4. Click **Add**.

6. Add the Tenable Log Source (Step 2 in wizard):
    1. From the QRadar **Admin** page, click on **Log Sources** (in the Data Sources > Events section). A new window is displayed, requiring you to use the QRadar Log Source Management app.
    2. Click **Launch**.
    3. From the IBM QRadar Log Source Management page, click **Log Sources**.
    4. Click **+ New Log Source**. A page asking you how many log sources you will be adding is displayed.
    5. Click **Single Log Source**.
    6. Search for and select **Ermetic** as the log source, and then click **Step 2: Select Protocol Type**.
    7. Select **TLS Syslog** and then click **Step 3: Configure Log Source Parameters**.
7. Add the Tenable Log Source (Step 3 in wizard), by configuring the Log Source parameters, as follows:
    1. Enter Ermetic as the **Name** for the log source.
    2. For the **Extension**, select **ErmeticCustom_ext**.
    3. Clear the **Coalescing Events** radio button.
    4. Click **Step 4: Configure Protocol Parameters**.
    5. Enter **Ermetic** as the **Log Source Identifier**.
    6. (Optional) Change the TLS Listen Port or Certificate Type, if needed.
    7. Enter **30000** as the **Max Payload Length**.
    8. Click **Step 5: Test Protocol Parameters**.
    9. (Optional) Click **Start Test** to test the protocol parameters.
8. Enter the following QRadar server parameters in AI Exposure (Step 4 in wizard):
    - **Display name** – A display name for the QRadar integration in AI Exposure.
    - Select how Tenable connects to your server. If your server is network-isolated, use a *Tenable Endpoint Connector* to establish connection.

- **Endpoint (internet-facing)**:
  - Enter the **hostname or IP address** of the IBM QRadar Console, without the `https://` protocol prefix.
  - Enter the **QRadar TLS port**. By default 6514, unless changed.
- **Endpoint Connector (network-isolated)** – Select the relevant connector from the dropdown. If this option is disabled, it means you haven't yet added a connector. See Connect Network-Isolated Servers for information about how to add one.

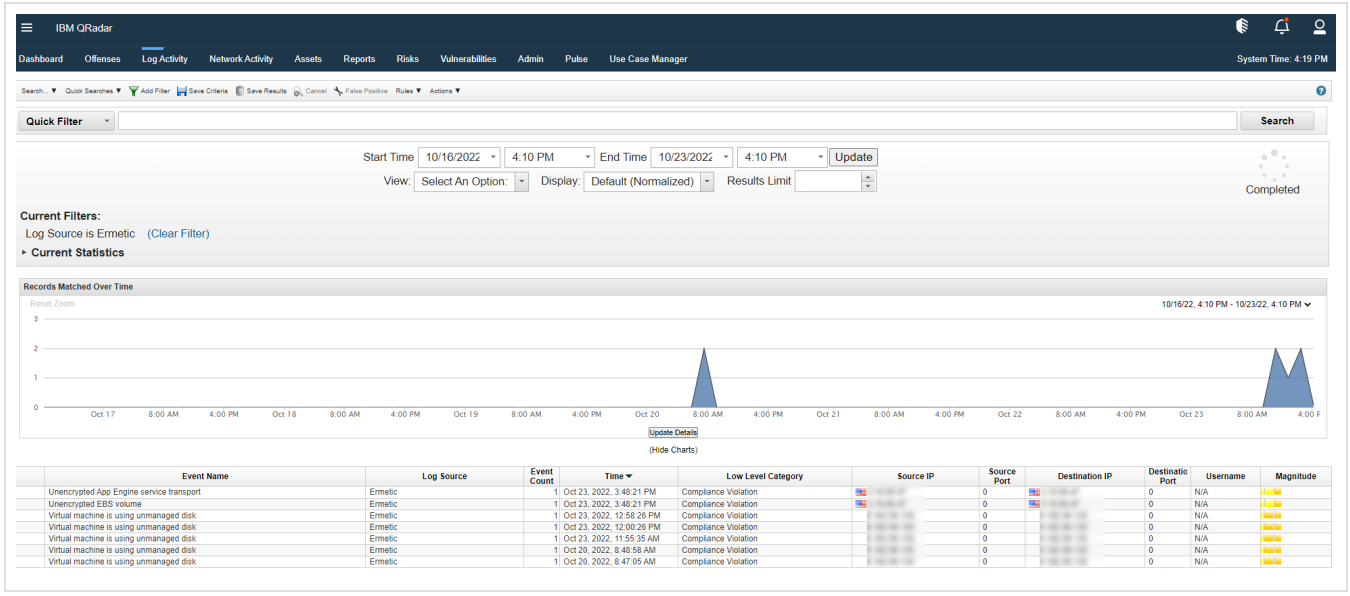
- Check **Accept any server SSL certificates** if SSL is enabled for the server.

9. Click **Finish**.

Important: To start sending notifications for findings, you need to configure automation rules after you integrate with QRadar. Successfully completing all integration steps doesn't trigger the sending of any data on its own.

View Tenable Findings in QRadar

1. In the IBM QRadar Console, navigate to the **Log Activity** page.
2. Click **Add Filter** and define the filter as follows:
   - Parameter: **Log Source [Indexed]**
   - Operator: **Equals**
   - Log Source Filter: **Ermetic**
3. Click **Add Filter**.



4. Double-click on an event to view a detailed view of the event.

Event Information

Event Name	Virtual machine is using unmanaged disk						
Low Level Category	Compliance Violation						
Event Description							
Magnitude	(3)	Relevance	1	Severity	4	Credibility	5
Username	N/A						
Start Time	Oct 23, 2022, 12:58:26 PM	Storage Time	Oct 23, 2022, 12:58:26 PM	Log Source Time	Oct 23, 2022, 12:58:07 PM		
Finding Account ID (custom)							
Finding Account Name (custom)	Org1Subscription2						
Finding Creation Time (custom)	Aug 25, 2022, 12:07:19 PM						
Finding Description (custom)	Virtual machine YochayTestManagedDiskVM is using 2 unmanaged disks						
Finding ID (custom)							
Finding Link (custom)							
Finding Status (custom)	Open						
Finding Status Update Time (custom)	Nov 29, 2022, 8:50:23 AM						
Finding Title (custom)	Virtual machine is using unmanaged disk						
Domain	Default Domain						

Source and Destination Information

Source IP		Destination IP	
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	0	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Payload Information

utf | hex | base64

Wrap Text

<12>1 2022-10-23T12:58:07.970882+00:00 Ermetic Ermetic - - - { "accountId": "[redacted]", "accountName": "Org1Subscription2", "creationTi

Sample JSON

JSON


```
{
  "accountId": "*****project",
  "accountName": "*****Project",
  "creationTime": "2022-10-23T10:31:54.446Z",
  "description": "App Engine Service default has 1 version not enforcing HTTPS connections",
  "id": "********-****-****-****-************",
  "link": "https://****.***.app.ermetic.com/customer/risks/ca6978eb-****-****-****-68241bedc38f",
  "labels": [
  ],
  "resource": [
    "apps/*****project/services/default"
```

```
  ],
  "severity": "Medium",
  "status": "Open",
  "statusUpdateTime": "2022-10-23T18:50:23.321Z",
  "policyName": "Unencrypted App Engine service transport",
  "type": "Finding",
  "ticketLinks": [
    "https://tenableccustomer1.atlassian.net/browse/DAV-24140",
    "https://tenablecustomer1.atlassian.net/browse/DAV-24144",
    "https://tenablecustomer1.atlassian.net/browse/DAV-24148",
    "https://tenablecustomer1.atlassian.net/browse/DAV-24152"
  ],
  "comments": [
    {
      "message": "created a ServiceNow incident for this threat story",
      "time": "2026-07-29T09:00:13.124307Z",
      "userName": "Tenable"
    },
    {
      "message": "created a Jira ticket for this threat story",
      "time": "2026-07-29T09:00:05.609867Z",
      "userName": "Tenable"
    }
  ]
}
```


Splunk

Integrate with Splunk Enterprise or Splunk Cloud Platform to send Tenable One AI Exposure findings to your Splunk instance.

What to do next:

- To start sending data for findings, you need to also configure automation rules or manually trigger an action after you add the integration. Successfully completing all integration steps doesn't trigger the sending of any data on its own.

Add a Splunk Instance

To enable notifications in Splunk, you first need to create an HTTP Event Collector (HEC) and an HEC token. These are used to allow Splunk to receive findings sent by Tenable.

FedRAMP: If you use Tenable One AI Exposure in a FedRAMP environment, make sure to connect integrations only to FedRAMP authorized services and endpoints. You are responsible for confirming that each service you connect meets your FedRAMP requirements. Sending data to a service outside your authorization boundary can put your organization out of compliance with FedRAMP requirements.

To integrate with Splunk:

1. In Splunk, enable HEC and configure an HEC token. Refer to Splunk documentation for instructions on how to do this for either Splunk Enterprise or Splunk Cloud Platform. As you perform these steps, record the following information:
    - Whether SSL is enabled for the HEC.
    - The HTTP port number used by the HEC.
    - The value of the token you configure.

    Note: On Splunk Cloud Platform, HEC is enabled by default, and the SSL/HTTP port number settings are automatically set and cannot be changed: SSL is enabled, and the port is 8088. On Splunk Enterprise, you must actively enable HEC, and the SSL/HTTP port number settings are configurable.
2. In the AI Exposure Console, navigate to **Settings > Integrations**.
3. (Options) Select a scope in the Organization dropdown.
4. Click **Add Integration**.
5. In the Integrations Library, click **Splunk** and then click **Next** to proceed to Step 2 (Provide Splunk HTTP Event Collector Info).
6. Enter a **Display name** for the Splunk integration in AI Exposure.
7. Enter the **Event Collector URL**. This is the Splunk platform instance address, together with the HTTP port number used by HEC. For example, https://splunkcloud.com:8088
8. Check **Accept any server SSL certificates** if SSL is enabled for the HEC.
9. Enter the HEC **token** value that you configured in Splunk.
10. Click **Finish**.

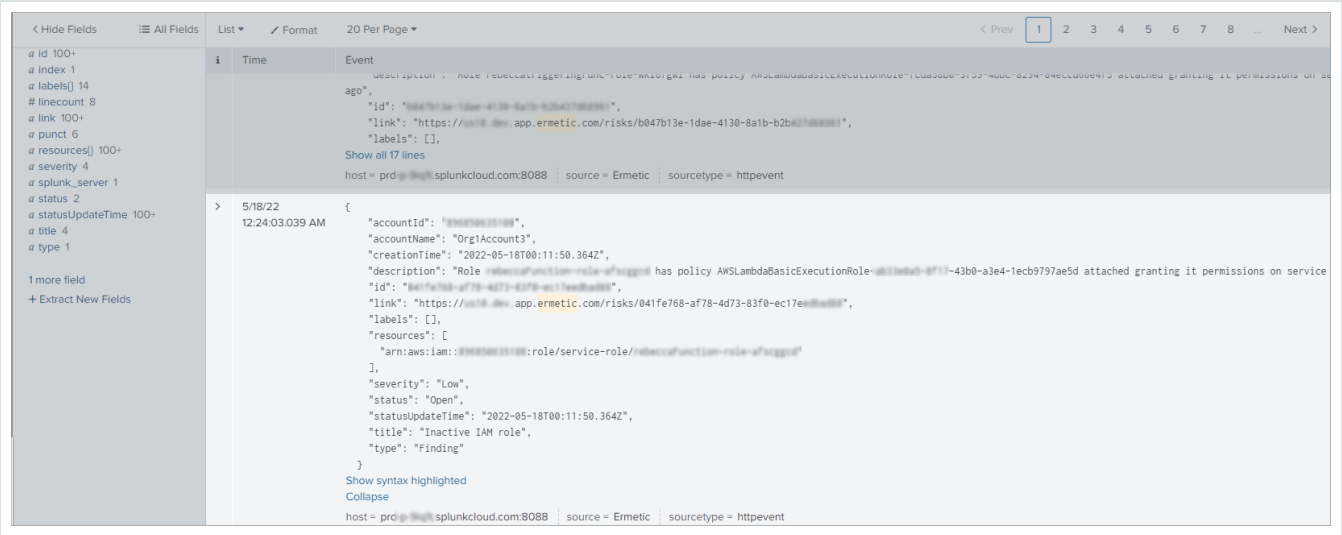
After your integration is added successfully, click **Done** to return to the **Integrations** page, where you will see your newly added integration.

Important: To start sending notifications for findings, you need to configure automation rules after you integrate with Splunk. Successfully completing all integration steps doesn't trigger the sending of any data on its own.

View Tenable Findings in Splunk

To view findings in Splunk:

1. Log into your Splunk Cloud or Enterprise instance.
2. Search for events using a relevant search term for AI Exposure findings.



Sample JSON

JSON


```
{
  "preview": false,
  "lastrow": true,
  "result": {
    "_raw": "{\n    \"accountId\": \"***\",\n    \"accountName\": \"***\",\n    \"creationTime\": \"2022-
05-18T00:11:50.364Z\",\n    \"description\": \"Role Function-role-afscggcd has policy
AWSLambdaBasicExecutionRole-********************************* attached granting it permissions on
service Amazon CloudWatch Logs, but it has not used it and was last active one month ago\",\n    \"id\":
```

```
\"**********\",\n    \"link\":
\"https://****.***.app.ermetic.com/risks/**********\",\n    \"labels\": [],\n
\"resources\": [\n      \"arn:aws:iam::"
    ***********
    ",:role/service-role/Function-role-afscggcd\"\n    ],\n    \"severity\": \"Low\",\n    \"status\":
\"Open\",\n    \"statusUpdateTime\": \"2022-05-18T00:11:50.364Z\",\n    \"title\": \"Inactive IAM
role\",\n    \"type\": \"Finding\"\n  }",
    "_time": "2022-05-18T00:24:03.039+0000",
    "accountId": "***********",
    "accountName": "Org1Account3",
    "creationTime": "2022-05-18T00:11:50.364Z",
    "description": "Role rebeccaFunction-role-afscggcd has policy AWSLambdaBasicExecutionRole-
********** attached granting it permissions on service Amazon CloudWatch Logs,
but it has not used it and was last active one month ago",
    "host": "********.splunkcloud.com:8088",
    "id": "**********",
    "index": "main",
    "linecount": "17",
    "link": "https://******.app.ermetic.com/risks/**********",
    "punct": "{____\"\":_\"\",____\"\":_\"\",____\"\":_\"--::.\",____\"\":_\"_-",
    "resource{}": "arn:aws:iam::***********:role/service-role/Function-role-afscggcd",
    "severity": "Low",
    "source": "Ermetic",
    "sourcetype": "httpevent",
    "splunk_server": "si-i-**********.*****.splunkcloud.com",
    "status": "Open",
    "statusUpdateTime": "2022-05-18T00:11:50.364Z",
    "policyName": "Inactive IAM role",
    "type": "Finding",
    "ticketLinks": [
      "https://tenablecustomer1.atlassian.net/browse/DAV-24140",
      "https://tenablecustomer1.atlassian.net/browse/DAV-24144",
      "https://tenablecustomer1.atlassian.net/browse/DAV-24148",
      "https://tenablecustomer1.atlassian.net/browse/DAV-24152"
    ],
    "comments": [
      {
        "message": "created a ServiceNow incident for this threat story",
        "time": "2026-07-29T09:00:13.124307Z",
        "userName": "Tenable"
      },
      {
        "message": "created a Jira ticket for this threat story",
        "time": "2026-07-29T09:00:05.609867Z",
        "userName": "Tenable"
      }
    ]
```

```
    }
  }
```

SQS Queue

Integrate with SQS to send Tenable One AI Exposure findings to your SQS queue.

What to do next:

- To start sending data for findings, you need to also configure automation rules or manually trigger an action after you add the integration. Successfully completing all integration steps doesn't trigger the sending of any data on its own.

Add an SQS Queue

> **FedRAMP:** If you use Tenable One AI Exposure in a FedRAMP environment, make sure to connect integrations only to FedRAMP authorized services and endpoints. You are responsible for confirming that each service you connect meets your FedRAMP requirements. Sending data to a service outside your authorization boundary can put your organization out of compliance with FedRAMP requirements.

To add an SQS queue:

1. In the AI Exposure Console, navigate to **Settings > Integrations**.
2. (Options) Select a scope in the Organization dropdown.
3. Click **Add Integration**.
4. In the Integrations Library, click **SQS**. The SQS wizard opens.
5. Enter a **Name** for the integration to be displayed in AI Exposure.
6. Enter the **URL** of the queue. The URL is available in the AWS Console, in the **Details** section of the queue. Valid format - https://sqs.{`region`}.amazonaws.com/{`account id`}/{`queue name`}
7. **Grant Tenable permissions**. Tenable uses an IAM role to push messages to your SQS queue. Use the same role used to onboard your AWS environment to Tenable (default), or create a

custom role (for example, if your queue is in an account that hasn't been onboarded).

- **Use default IAM role**:
    1. In the AWS Management Console, navigate to **IAM > Roles**.
    2. Search for and click on the role you created for AI Exposure when you onboarded your AWS environment.
    3. To edit the policy, under *Permissions > Permissions policies*, click on the monitoring (read-only) policy name that you created during onboarding.
    4. In the JSON editor, add the following permission:

       `"SQS:SendMessage"`
    5. Click **Next**.
    6. Review the changes and then click **Save changes**.
    7. (**If your queue is encrypted with KMS**):
        1. In the AWS Management Console, navigate to **KMS > Customer managed keys**.
        2. Click on the relevant key, and in the *Key policy* section click **Edit**.
        3. In the JSON editor, add the following additional statement to the policy and then click **Save changes**:

```JSON
{
   "Sid": "Allow Read Access to Key",
   "Effect": "Allow",
   "Principal": {
       "AWS": "<IAM Role ARN>"
   },
   "Action": [
    "kms:GenerateDataKey",
    "kms:Decrypt"
   ],
   "Resource": "*"
}
```

- **Use custom IAM role**:
    1. In the AWS Management Console, navigate to **IAM > Roles** and click **Create role**.
    2. For the trusted entity type, select **AWS account**.
    3. For the AWS account, select **Another AWS account** and then enter one of the following numbers as the Account ID, depending on your AWS environment type:
        - Public Cloud: **081802104111**
        - US Gov Cloud: **757023926892**

        > **Note:** This is Tenable's account ID. The ID must be exactly twelve-digits; make sure not to include any extra spaces.

    4. Under Options, check **Require external ID**.
    5. Enter the Role **External ID** provided in the Add SQS Queue wizard (Tenable Console).

        > **Note:** The Role External ID is a unique identifier that AI Exposure assigns to your customer account. This ID will be the same for each account you create for your organization. For more information, refer to AWS IAM documentation.

    6. Click **Next**.
    7. On the Add permissions page, click **Next**.
    8. Enter a meaningful **Role name** and **Description** and then click **Create role**.
    9. Open the newly created role and under Permissions, click **Add permissions > Create inline policy**.
    10. Copy the following policy, and paste it into the **JSON** tab to replace the existing text, where `{SQS_ARN}` is the ARN of your SQS queue.

        > **Note:** Replace `{SQS_ARN}` in the snippet below with the ARN of your SQS queue. The ARN is available in the AWS Console, in the **Details** section of the queue.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
     {
         "Effect": "Allow",
         "Action": [
             "sqs:SendMessage"
         ],
         "Resource": "{SQS_ARN}"
     }
 ]
}
```

11. Click **Next**.
12. Enter a meaningful **Policy name** and then click **Create policy**.
13. Copy the **ARN** of the custom role that you created.
14. (AI Exposure Console) Paste the **IAM role ARN** and then click **Finish**
15. (**If your queue is encrypted with KMS**)
    1. In the AWS Management Console, navigate to **KMS > Customer managed keys**.
    2. Click on the relevant key, and in the *Key policy* section click **Edit**.
    3. In the JSON editor, add the following additional statement to the policy and then click **Save changes**:

JSON

```
  {
     "Sid": "Allow Read Access to Key",
     "Effect": "Allow",
     "Principal": {
         "AWS": "<IAM Role ARN>"
     },
     "Action": [
      "kms:GenerateDataKey",
      "kms:Decrypt"
     ],
     "Resource": "*"
```

```
}
```

Sample JSON

JSON


```
{
  "source": "Tenable",
  "action": "Create JIT eligibility",
  "details": {},
  "result": "Success",
  "scope": "Organization\\Azure AD",
  "time": "2024-06-25T10:21:23.7023655Z",
  "approvalRequired": true,
  "approvers": [
    "006"
  ],
  "requesters": [
    "003"
  ],
  "maxDurationHours": 21,
  "name": "More eligibilities for testing",
  "user": "***@customer1.onmicrosoft.com",
  "ticketLinks": [
    "https://tenablecustomer1.atlassian.net/browse/DAV-24140",
    "https://tenablecustomer1.atlassian.net/browse/DAV-24144",
    "https://tenablecustomer1.atlassian.net/browse/DAV-24148",
    "https://tenablecustomer1.atlassian.net/browse/DAV-24152"
  ],
  "comments": [
    {
      "message": "created a ServiceNow incident for this threat story",
      "time": "2026-07-29T09:00:13.124307Z",
      "userName": "Tenable"
    },
    {
      "message": "created a Jira ticket for this threat story",
      "time": "2026-07-29T09:00:05.609867Z",
      "userName": "Tenable"
    }
  ]
}
```


Offboarding Cloud Accounts

You may need to offboard an account from Tenable One AI Exposure in one of the following situations:

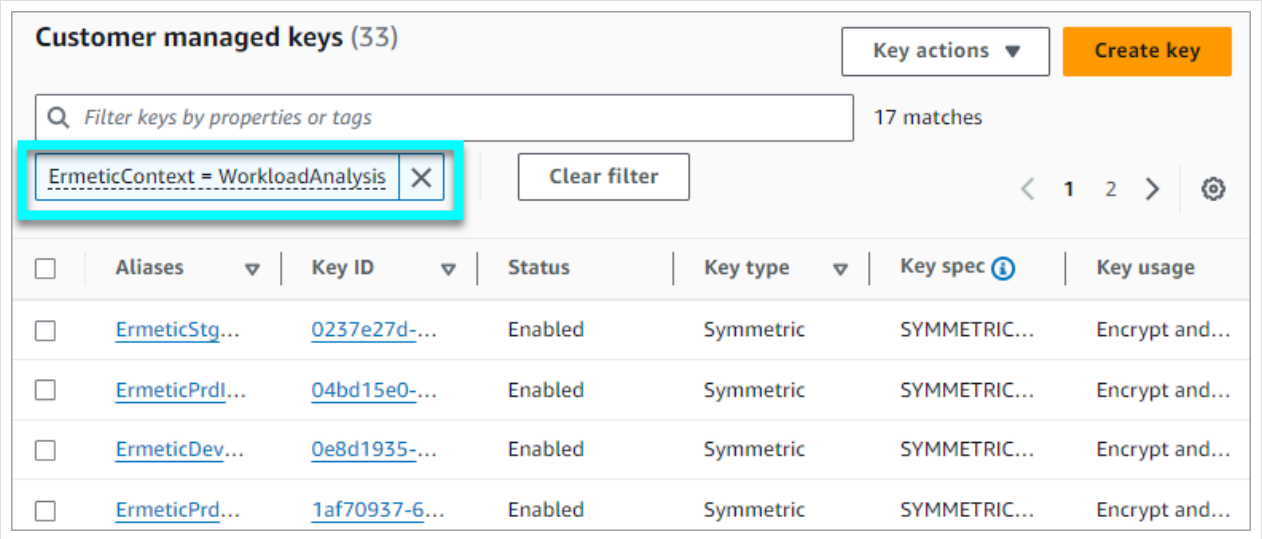
- If you performed an audit for a group of accounts and you completed the audit.
- If you want to shut down your accounts.

> **Note:** Tenable deletes customer data within 30 days of the customer terminating its contract.

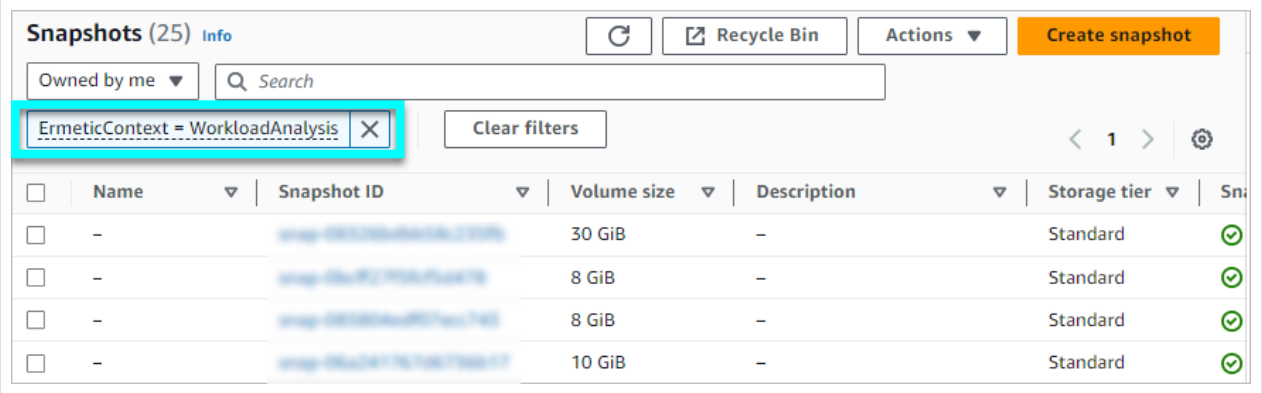
Offboard AWS Accounts

Follow these steps to offboard AWS accounts and/or organizations.

1. Delete any IAM roles that you created during onboarding.
2. (Workload Protection) Delete any KMS keys/snapshots that were created:
    1. In the AWS Console, navigate to **KMS > Customer managed keys**, and search for keys with the tag key/value of `ErmeticContext = WorkloadAnalysis`.



    2. Select the relevant keys and delete them.
    3. Navigate to **EC2 > Elastic Block Store > Snapshots**, and search for snapshots with the tag key/value of `ErmeticContext = WorkloadAnalysis`.



4. Select the relevant keys and click **Actions > Delete Snapshot**.

3. If you used CloudFormation to create an IAM role, delete any Stack instances and StackSets that were created:
    1. In the AWS Console, navigate to **CloudFormation > StackSets** and search for any StackSet you created during onboarding.
    2. Select the StackSet and then click **Actions > Delete stacks from StackSet**.
    3. Enter any required details, and proceed with deleting the stacks.
    4. After any stacks are deleted, select the StackSet again and click **Actions > Delete StackSet**.
    5. Click **Delete** to confirm.
4. Delete the organization/account/s from the AI Exposure Console:
    - **Organization** – Navigate to **Settings > Integrations > AWS Organization**, and then click **Delete** next to the relevant organization. Deleting the organization will automatically delete all associated folders and accounts beneath it.
    - **Account** – Navigate to **Accounts > AWS**, and then click **Delete** next to the relevant account/s.

      > **Note:** If the account/s belongs to an onboarded organization, you should exclude the account from the organization. Otherwise, delete the account from **Settings** > **Accounts** > **AWS**.

Offboard Azure Subscriptions

Follow these steps to offboard Azure subscriptions and/or organizations.

1. Remove the role assignments that you added to the AI Exposure app during onboarding.
2. Remove the AI Exposure app from Microsoft Entra ID.
3. Delete the organization/subscription from the AI Exposure Console:
    - **Organization** – Navigate to **Settings > Integrations > Azure Organization**, and then click **Delete** next to the relevant organization.
    - **Subscription** – Navigate to **Accounts > Azure**, and then click **Delete** next to the relevant subscription.

    > **Note:** If the subscription/s belongs to an onboarded organization, you should exclude the subscription from the organization. Otherwise, delete the subscription from **Settings** > **Accounts** > **Azure**.

Offboard GCP Projects

Follow these steps to offboard GCP projects and/or organizations.

1. Remove the permissions that you granted to the Tenable service account during onboarding.
2. Remove the Tenable service account that you created when you connected a Google Workspace.
3. Delete the organization/project from the AI Exposure Console:
    - **Organization** – Navigate to **Settings > Integrations > GCP Organization**, and then click **Delete** next to the relevant organization.
    - **Project** – Navigate to **Accounts > GCP**, and then click **Delete** next to the relevant account.

    > **Note:** If the project/s belongs to an onboarded organization, you should exclude the project from the organization. Otherwise, delete the project from **Settings** > **Accounts** > **GCP**.

Offboard OCI Tenancy

Follow these steps to offboard OCI tenancies.

1. Remove any group/user/key/credentials that you created when you onboarded your Oracle Cloud tenancy.
2. Delete the tenancy from the AI Exposure Console. Navigate to **Settings > Integrations > OCI Tenancy**, and then click **Delete** next to the relevant tenancy.

Webhooks

Webhooks

If you use HTTP webhooks to share data triggered by events, you can send Tenable One AI Exposure findings to any destination using webhooks. For example, you can use webhook connections to send Tenable findings to:

- Microsoft Sentinel
- Sumo Logic
- Telegram
- PagerDuty
- Any other service supporting incoming webhooks

What to do next:

- To start sending data for findings, you need to also configure automation rules or manually trigger an action after you add the integration. Successfully completing all integration steps doesn't trigger the sending of any data on its own.

Add a Webhook

> **FedRAMP:** If you use Tenable One AI Exposure in a FedRAMP environment, make sure to connect integrations only to FedRAMP authorized services and endpoints. You are responsible for confirming that each service you connect meets your FedRAMP requirements. Sending data to a service outside

our authorization boundary can put your organization out of compliance with FedRAMP equirements.

To add a webhook:

1. In the AI Exposure Console, navigate to **Settings > Integrations** and click on **Webhook**.
2. (Optional) Select an account scope in the Organization dropdown.
3. Click **Add webhook**.
4. Enter a **Name** for the webhook in AI Exposure.
5. Enter the **Webhook URL** belonging to the destination application. For example, in Sumo Logic, this is the Collector API URL.
6. Check **Accept any server SSL certificates** if SSL is enabled for the collector.
7. Add an HTTP header **Name** and **Value** if the webhook expects to receive such a header containing any additional relevant information.
8. Click **Save**.

Microsoft Sentinel (via Webhook)

Send Tenable One AI Exposure findings to Microsoft Sentinel through an Azure Logic App. The Logic App receives findings from a AI Exposure webhook and forwards them to a custom table in your Log Analytics workspace using the Azure Monitor Logs Ingestion API. The Logic App authenticates with a managed identity, so you don't need to store a workspace key.

Caution: If you configured this integration with the **Send Data** (Azure Log Analytics Data Collector) action, Microsoft has deprecated the HTTP Data Collector API that action uses. Follow this guide to replace it.

FedRAMP: If you use Tenable One AI Exposure in a FedRAMP environment, make sure to connect integrations only to FedRAMP authorized services and endpoints. You are responsible for confirming that each service you connect meets your FedRAMP requirements. Sending data to a service outside your authorization boundary can put your organization out of compliance with FedRAMP requirements.

Prerequisites

Before you begin:

- Ensure you have access to a Log Analytics workspace with Microsoft Sentinel enabled.
- Ensure your Azure account has permissions to create tables, data collection rules (DCRs), data collection endpoints (DCEs), and Logic Apps.
- Ensure your Azure account has permissions to assign roles on the DCR (e.g., the **Owner** or **User Access Administrator** role).

To send AI Exposure data to Microsoft Sentinel, follow these steps:

1. Create a Custom Table
2. Copy the DCR and DCE Values
3. Create a Logic App with Managed Identity
4. Grant the Logic App Access to the DCR
5. Create a Sentinel Webhook Integration in Tenable
6. Send data to the webhook in one of the following ways:
    - Automate actions
    - Manually trigger actions based on findings
7. View Data in Microsoft Sentinel

What to do next:

- To start sending data for findings, you need to also configure automation rules or manually trigger an action after you add the integration. Successfully completing all integration steps doesn't trigger the sending of any data on its own.

Create a Custom Table

Create a custom table in your Log Analytics workspace, along with the DCR and DCE that route AI Exposure data to it.

1. In the Azure portal, navigate to **Log Analytics workspaces** and select the workspace where Microsoft Sentinel is enabled.
2. Under **Settings**, select **Tables**.
3. Click **Create** > **New custom log (DCR based)**.
4. Enter a **Table name**, for example `TenableFindings`.

   > **Note:** Azure automatically adds the `_CL` suffix, so the full table name is `TenableFindings_CL`. You need the full name when you create the Logic App and when you View Data in Microsoft Sentinel.

5. For **Table plan**, select **Analytics**.
6. Under **Data collection rule**, select an existing DCR or click **Create a new data collection rule** and specify the **Subscription**, **Resource group**, and **Name** (for example, `dcr-tenable-findings`).
7. Under **Data collection endpoint**, select an existing DCE or create a new one.
8. Click **Next**.
9. Save the following sample payload as a `.json` file, and then upload it to generate the table schema.

   Sample payload

```json
[
  {
    "source": "source",
    "sentBy": "Tenable",
    "comments": [
      {
        "message": "message",
        "time": "2026-01-15T14:30:00.000000Z",
        "userName": "User Name"
      }
    ],
    "creationTime": "2026-01-10T08:00:00.000Z",
    "id": "00000000-0000-0000-0000-000000000000",
```

```
    "link": "https://example.com/customer/00000000-0000-0000-0000-
000000000000/Risks/Cloud/Closed#risk/00000000-0000-0000-0000-000000000000",
    "severity": "High",
    "ticketLinks": [],
    "accountId": "123456789012",
    "accountName": "ExampleAccount",
    "category": "exampleCategory",
    "description": "exampleDescription",
    "openTime": "2026-01-10T08:00:00.000Z",
    "policyName": "example policy",
    "provider": "exampleProvider",
    "status": "exampleStatus",
    "statusUpdateTime": "2026-01-15T14:30:00.000Z",
    "subStatus": "exampleSubStatus",
    "type": "exampleType",
    "compliances": [
      "exampleCompliance1",
      "exampleCompliance2"
    ],
    "ignoredUntil": "2026-01-15T14:30:00.000Z",
    "resource": "ExampleResourceName"
  }
]
```


10. Add a `TimeGenerated` column. Every Azure Monitor log table requires one, and the AI Exposure payload doesn't include it, so the portal displays a warning.
    1. Click **Transformation editor**.
    2. Enter the following query, and then click **Run**:

    ```
    KUSTO

    source
    | extend TimeGenerated = todatetime(statusUpdateTime)
    ```

    3. Click **Apply**.
11. Click **Next**, and then click **Create**.

Copy the DCR and DCE Values

Copy the values that the Logic App needs to send data to your DCR.

1. In the Azure portal, navigate to **Monitor** > **Data collection rules** and select the DCR you created.
2. On the **Overview** page, click **JSON View**.
3. Copy and save the `immutableId` value. It starts with `dcr-`.
4. Navigate to **Monitor** > **Data Collection Endpoints** and select the DCE you selected for the table.
5. Copy and save the **Logs ingestion** URI.

Create a Logic App with Managed Identity

Configure an Azure Logic App to receive data from Tenable and forward it securely to your DCR.

1. In the Azure portal, navigate to the **Logic apps** service.
2. Click **Add**.
3. For hosting option, select **Consumption**.
4. Under Project details, select the relevant **Subscription** and **Resource group**.
5. Under Instance details, enter a **Name** and select a **Region**.
6. Click **Review + Create** and then click **Create**.
7. When the deployment is complete, click **Go to resource**.
8. Create the managed identity:
    1. Navigate to **Settings** > **Identity**.
    2. On the **System assigned** tab, set **Status** to **On**.
    3. Click **Save**.
9. Navigate to **Development tools** > **Logic app designer**.
10. Click **Add a trigger**, and then search for and select **When a HTTP request is received**.
11. Click **+** and then **Add an action**.
12. Search for and select the **HTTP** action.

13. Configure the HTTP action:
    - **Method**: `POST`
    - **URI** – Enter the URI in the following format, using the values you copied earlier and the full table name:

      ```
      {Logs ingestion URI}/dataCollectionRules/{immutableId}/streams/Custom-{Table name}?api-version=2023-01-01
      ```

      For example:

      ```
      https://my-dce-5kyl.eastus-1.ingest.monitor.azure.com/dataCollectionRules/dcr-000a00a000a00000a000000aa000a0aa/streams/Custom-TenableFindings_CL?api-version=2023-01-01
      ```

    - **Headers** – Add `Content-Type` with the value `application/json`.
    - **Body** – Enter the expression `@createArray(triggerBody())`. The Logs Ingestion API accepts only a JSON array, and AI Exposure sends each finding as a single JSON object. This expression wraps the object in an array.
14. Under **Advanced parameters**, select **Authentication** and configure it:
    - **Authentication type**: **Managed identity**
    - **Managed identity**: **System-assigned managed identity**
    - **Audience**: `https://monitor.azure.com`

    > **Note:** If your workspace is in Azure Government, use `https://monitor.azure.us` as the audience.

15. Click **Save**.
16. Open the **When a HTTP request is received** trigger and copy the **HTTP URL**. Azure generates this URL when you save the workflow.

Grant the Logic App Access to the DCR

Assign the Logic App's managed identity a role that allows it to send data to your DCR.

1. In the Azure portal, navigate to **Monitor** > **Data collection rules** and select the DCR you created.
2. Select **Access control (IAM)** > **Add** > **Add role assignment**.
3. Select the **Monitoring Metrics Publisher** role and click **Next**.
4. For **Assign access to**, select **Managed identity**.
5. Click **Select members**, select your Logic App, and then click **Select**.
6. Click **Review + assign**.

> **Note:** The role assignment can take up to 30 minutes to take effect. If the Logic App sends data before then, the HTTP action returns a **403 Forbidden** error.

Create a Sentinel Webhook Integration in Tenable

Create a webhook integration in AI Exposure that sends findings to your Logic App.

1. In the AI Exposure Console, navigate to **Settings** > **Integrations** and click **Webhook**.
2. Click **Add webhook**.
3. Enter a **Name** for the webhook (e.g., `Sentinel_Modern_Integration`.
4. In the **Webhook URL** field, paste the HTTP URL that you copied in the last step of Create a Logic App with Managed Identity.
5. (Optional) Select **Accept any server SSL certificates** if SSL is enabled for the collector.
6. (Optional) For **HTTP Headers**, enter a **Name** and **Value** if the webhook expects to receive a header with additional information.
7. Click **Save**.

View Data in Microsoft Sentinel

Verify that findings reach Microsoft Sentinel.

> **Note:** After you configure the integration, allow up to 30 minutes for the first findings to appear.

1. Verify the Logic App run:
    1. In the Azure portal, open the Logic App that you created.
    2. On the **Overview** page, navigate to the **Run history** tab and click a run **Identifier**.
    3. Click the **HTTP** action and confirm that it succeeded. If it returns **403 Forbidden**, the role assignment hasn't taken effect yet.
2. View the data in Microsoft Sentinel:
    1. In the Azure portal, navigate to the **Microsoft Sentinel** service.
    2. Select your workspace and click **Logs**.
    3. In a new query (KQL mode), enter the full table name (for example, `TenableFindings_CL`) and click **Run**.

Sumo Logic (via Webhook)

If you use HTTP webhooks to share data triggered by events, you can send Tenable One AI Exposure findings to any destination using webhooks.

What to do next:

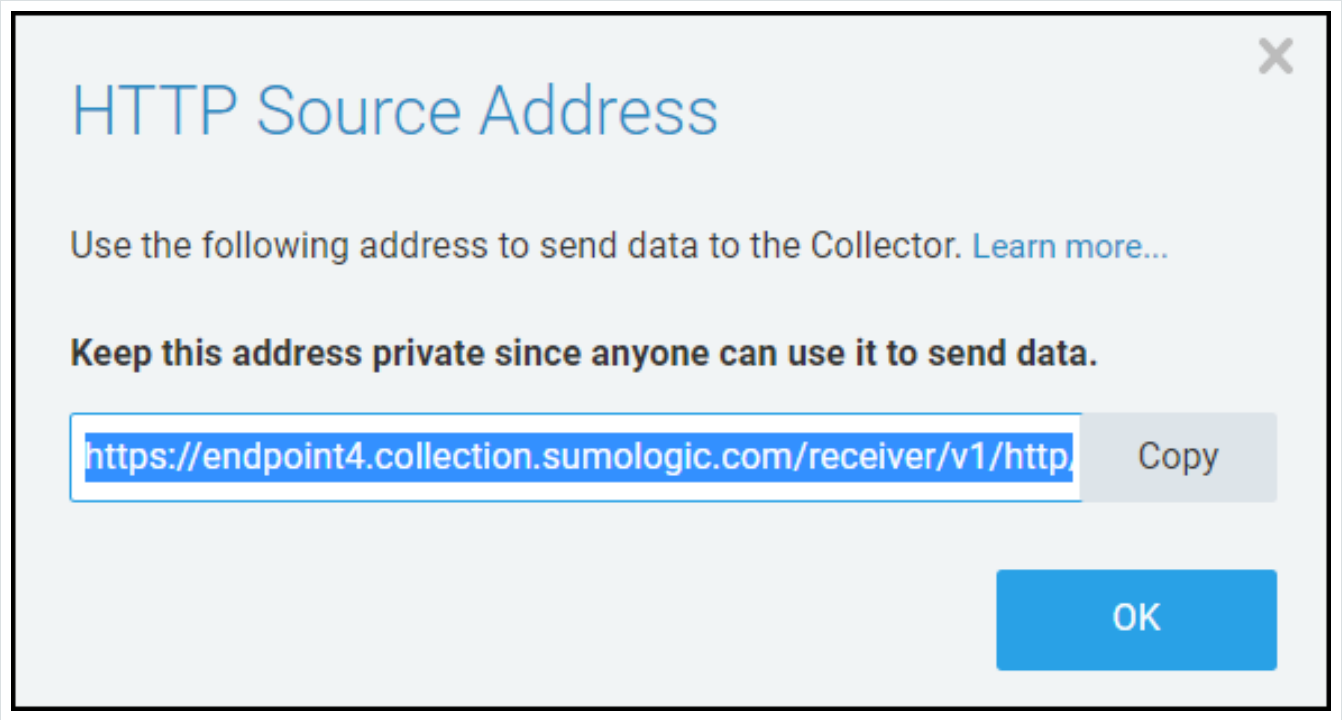
- To start sending data for findings, you need to also configure automation rules or manually trigger an action after you add the integration. Successfully completing all integration steps doesn't trigger the sending of any data on its own.

Send Data to Sumo Logic

> **FedRAMP:** If you use Tenable One AI Exposure in a FedRAMP environment, make sure to connect integrations only to FedRAMP authorized services and endpoints. You are responsible for confirming that each service you connect meets your FedRAMP requirements. Sending data to a service outside your authorization boundary can put your organization out of compliance with FedRAMP requirements.

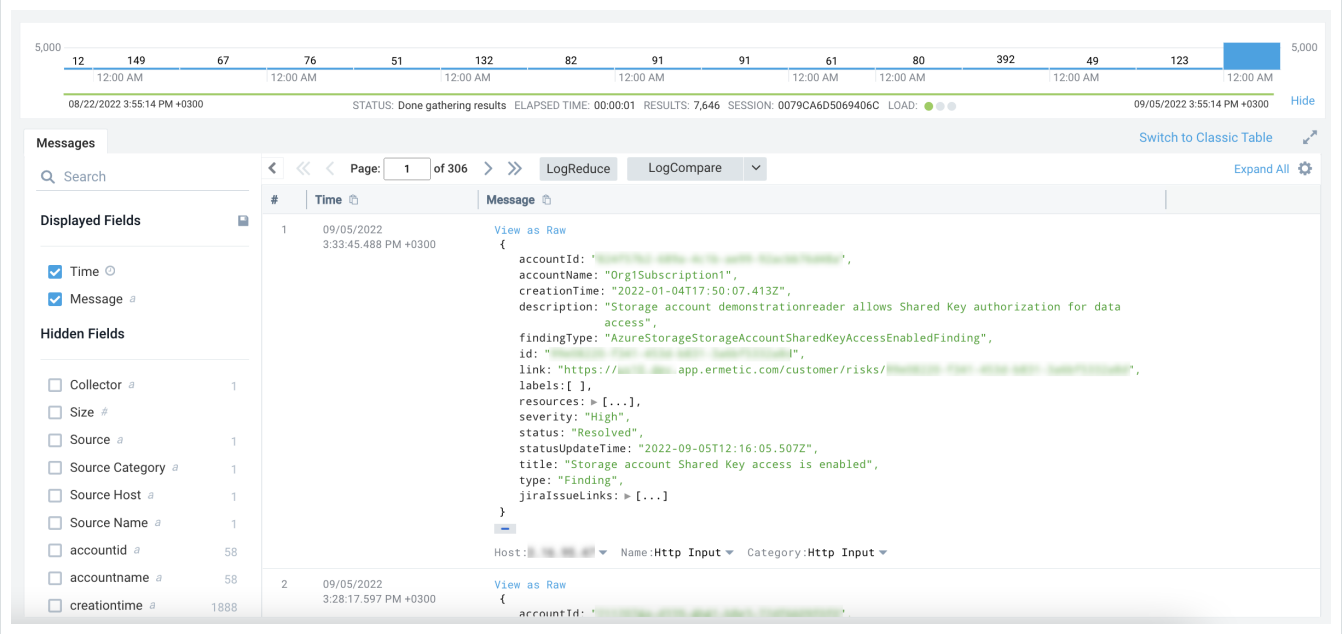
To send data to Sumo Logic:

1. In the Sumo Logic console, go to **Manage Data** > **Collection**.
2. Configure an **HTTP Logs and Metrics** Source for a Hosted Collector. Refer to the Sumo Logic documentation for more information.
    - In the Advanced Options for Logs section, within the Message Processing area, choose **One Message Per Request**. This ensures that each message coming from AI Exposure is displayed on its own row, instead of breaking down a single message into multiple rows (multiline processing).
3. After you finish entering all information and click **Save**, copy the URL that is displayed in the dialog box.



4. In the AI Exposure Console, navigate to **Settings** > **Integration** > **Webhooks** and then click **Lets Start**.
5. Enter a **Display name** for the webhook in Tenable.
6. Enter the **Webhook URL** that you copied from Sumo Logic in an earlier step.
7. Check **Accept any server SSL certificates** if SSL is enabled for the collector.
8. Add an HTTP header **Name** and **Value** if the webhook expects to receive such a header containing any additional relevant information.

9. Click **SAVE**.
10. To see Tenable data in Sumo Logic, go to the Sumo Logic console and search for the source name and collector name you defined above.



Sample JSON

JSON


```
{
  "accountId": "************",
  "accountName": "Org2Account2",
  "creationTime": "2022-01-12T01:10:24.868Z",
  "description": "User FindingsFixer has 2 policies attached granting it permissions on 2 services, but none of them were used for 68 weeks",
  "findingType": "AwsExcessivePermissionUserFinding",
  "id": "************************************",
  "link": "https://us.app.ermetic.com/risks/************************************",
  "labels": [
    "Admin",
    "Access Keys",
    "No MFA"
  ],
  "resource": [
    "arn:aws:iam::***********:user/FindingsFixer"
  ],
  "severity": "High",
```

```
  "source": "Ermetic",
  "status": "Open",
  "statusUpdateTime": "2022-05-21T22:16:44.785Z",
  "title": "Overprivileged IAM user",
  "type": "Finding"
}
```


Telegram (via Webhook)

Integrate with Telegram to send Tenable One AI Exposure findings to Telegram via webhooks. Perform the following steps to complete the integration, using AWS as an intermediary to translate Tenable data so that it is readable by Teams.

What to do next:

- To start sending data for findings, you need to also configure automation rules or manually trigger an action after you add the integration. Successfully completing all integration steps doesn't trigger the sending of any data on its own.

FedRAMP: If you use Tenable One AI Exposure in a FedRAMP environment, make sure to connect integrations only to FedRAMP authorized services and endpoints. You are responsible for confirming that each service you connect meets your FedRAMP requirements. Sending data to a service outside your authorization boundary can put your organization out of compliance with FedRAMP requirements.

Create a New Telegram Bot with BotFather

Create a Telegram bot with BotFather before connecting your bot to Telegram.

Note: Although you can perform most of these steps in the Telegram App, you will need to use Telegram Web for the last step.

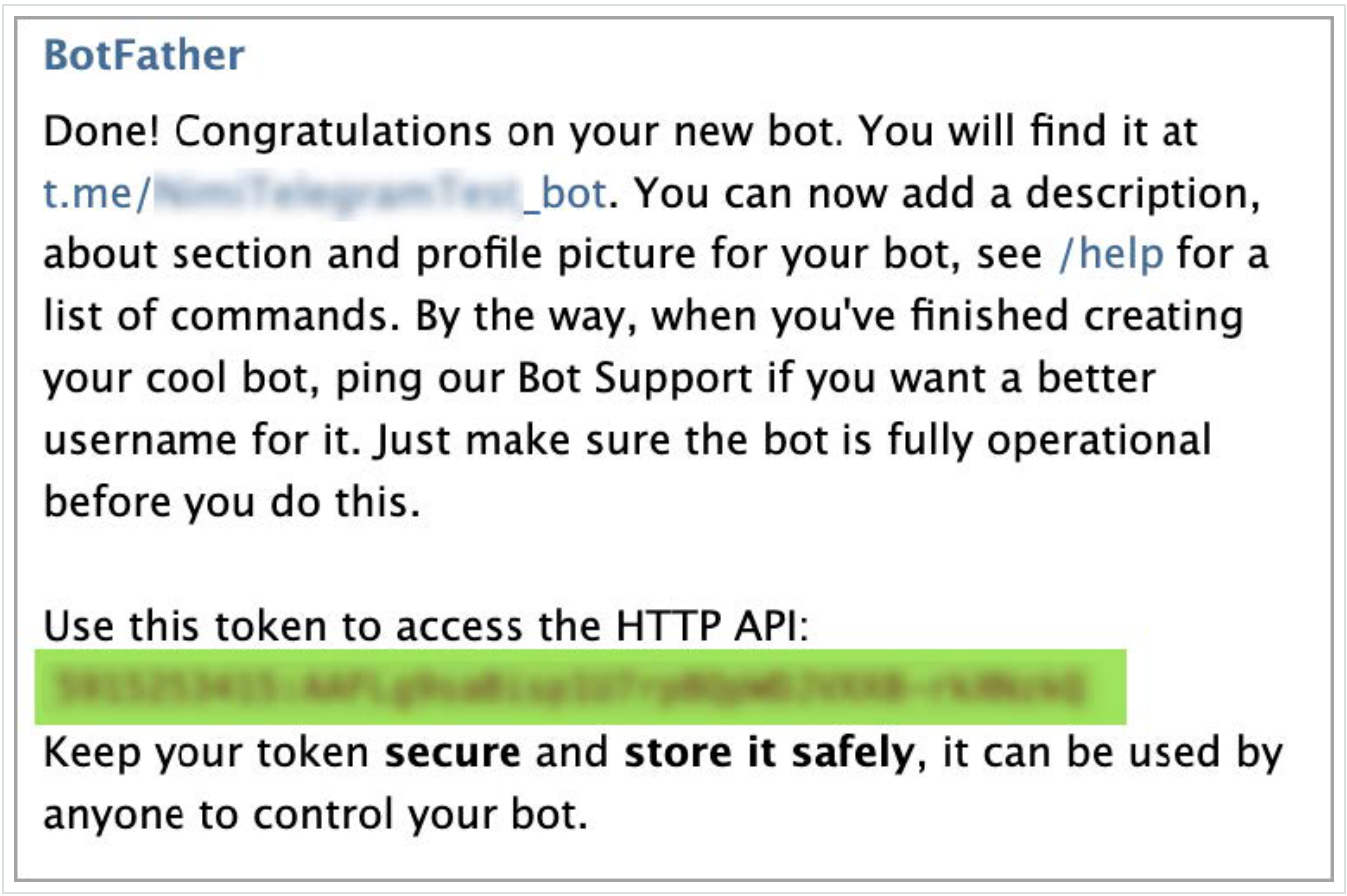
1. In Telegram, start a new conversation with the BotFather.
2. Send the following message to create a new Telegram bot:

   ```
   /newbot
   ```

3. When prompted, enter a name for the bot. Give the Telegram bot a unique username.

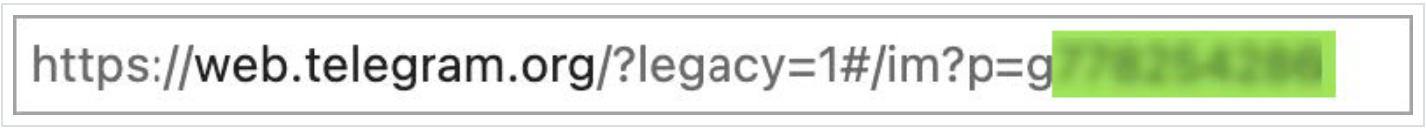
   > **Note:** The bot name must end with the word "bot" (case-insensitive).

4. Copy and save the Telegram bot's access token for use in later steps.



5. (Optional) Set a profile picture for the bot (for example, using the Tenable logo):
   - Send the message `/setuserpic` to BotFather.
   - Select the bot you created for Tenable.
   - Send the profile picture.
6. Create a new group in Telegram.
7. Select the bot you created earlier, and add any relevant users.
8. (Optional) Give the group a name and add a picture, and then click **Create**.
9. In Telegram Web, click on the new group that you created. In the browser URL, identify and save the chat ID (the numbers that appear after the letter 'g'). Save this value for later.

> **Note:** Although you can perform the previous steps in the Telegram App, you will need to use Telegram Web for this step.



Use AWS to Create a CloudFormation Stack

Use AWS to parse the finding payload from Tenable to a format suitable for Telegram notifications by performing the following steps:

- Configure the SSM Parameter
- Create a CloudFormation Stack

Configure the SSM Parameter

To configure the SSM parameter:

1. In the AWS Console, navigate to **Systems Manager** > **Parameter Store**.
2. Click **Create parameter**, and then enter the following details:
    - Name: **TelegramErmeticToken**

      > **Important:** The name must be entered exactly as is for the integration to work.

    - Tier: **Standard**
    - Type: **SecureString**
    - KMS key source: *Leave the default value*
    - Data type: **text**
    - Value: *Enter the Telegram **bot access token** you configured earlier*
3. Click **Create parameter**.

4. Click **Create parameter** to add another parameter, and then enter the following details:
    - Name: **TelegramErmeticChatID**

      Important: The name must be entered exactly as is for the integration to work.

    - Tier: **Standard**
    - Type: **SecureString**
    - KMS key source: *Leave the default value*
    - Data type: **text**
    - Value: *Enter the Telegram **chat ID** you configured earlier*
5. Click **Create parameter**.

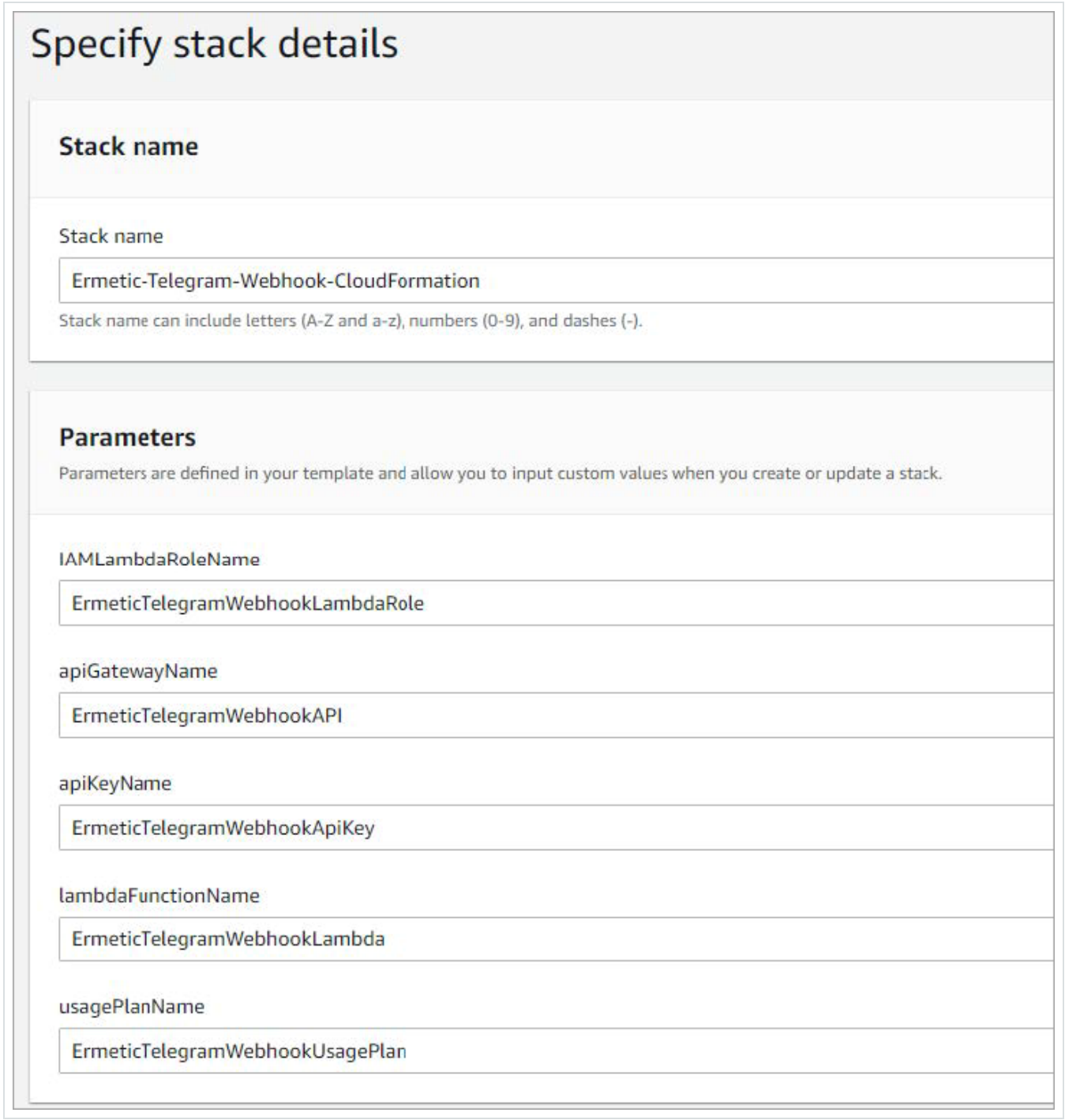
Create a CloudFormation Stack

Contact Technical Support to obtain the following files required in this procedure:

- CloudFormation template file
- .zip file deployment package for a lambda function

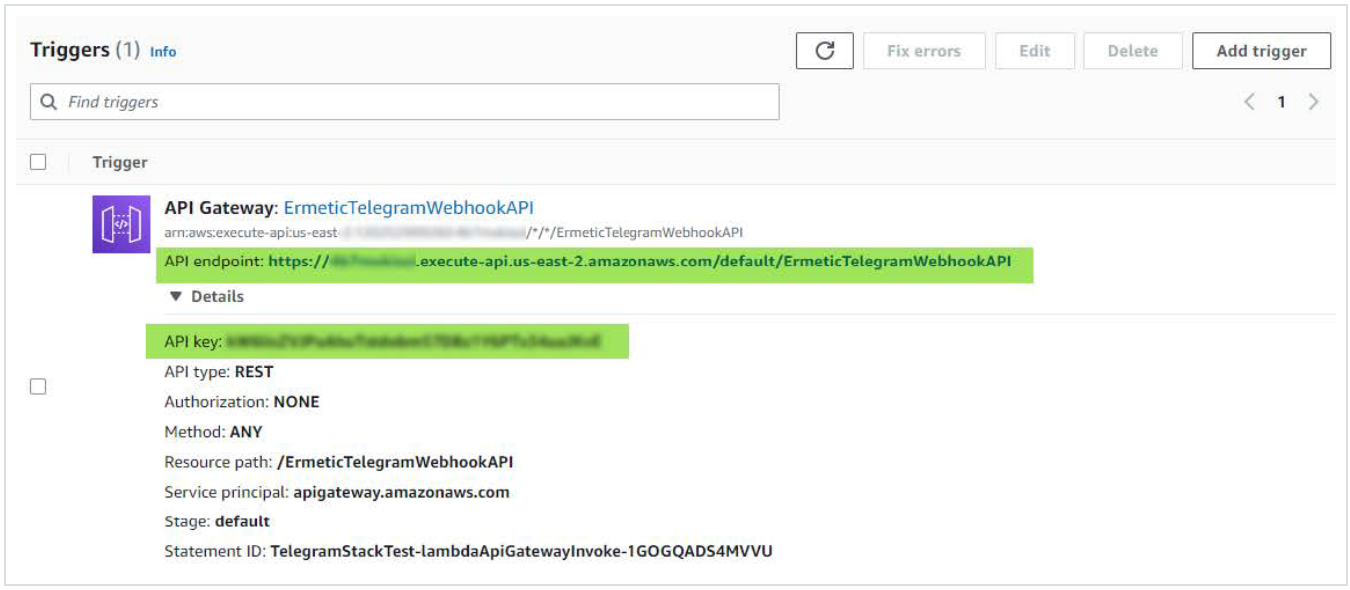
To create a CloudFormation stack:

1. In the AWS Console, navigate to **CloudFormation** > **Stacks** and and then click **Create Stack (With new resources – standard)**. The Create stack wizard opens.
2. In the Prerequisite - Prepare template section, select **Template is ready**.
3. In the Specify template section, select **Upload a template file** and then click **Choose file** to upload the template file provided by Technical Support.
4. Click **Next**.
5. Enter a **Stack name** for the cloud formation stack. For example, *Tenable-Telegram-Webhook-CloudFormation*.
6. (Optional) The stack creates several resources (Lambda function, API gateway, IAM Role, API Key). You can rename the resources, or use the default names. Click **Next**.



7. On the Configure stack options page, click **Next** (There are no fields on this page that are mandatory for completing the task at hand).
8. On the Review page, acknowledge the checkbox at the bottom of the page (*I acknowledge that AWS CloudFormation might create IAM resources with custom names*), and then click **Submit**.

9. After completing stack creation, navigate to the **Resources** tab and click on the lambda function **Physical ID** link.
10. Navigate to the **Code** tab and in the Code source section, click **Upload from** > **.zip file**, and then upload the *Ermetic_Telegram_lambda_code* .zip file provided by Technical Support.
11. Navigate to the **Configuration** tab. You will need to enter lambda trigger information from this tab in the next step.
12. Find the API Gateway trigger and click **Details** to see additional information. Copy and save the API endpoint and API key, as you will need them when you create a webhook integration in Tenable in the next step.

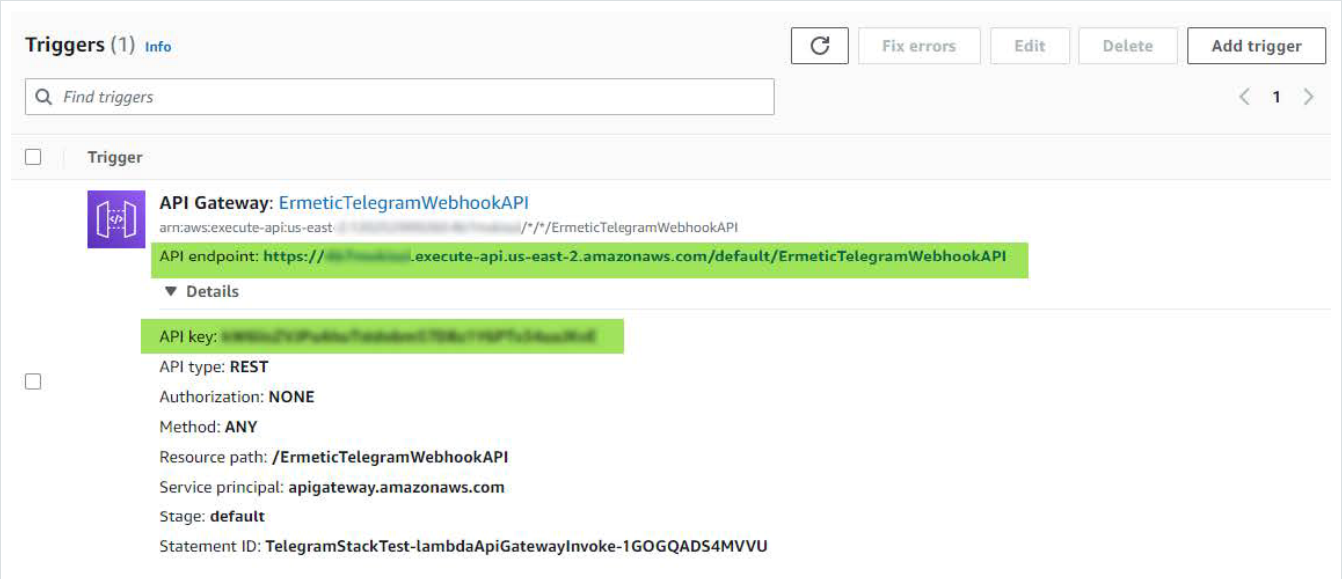


Create a Telegram Webhook Integration in Tenable

To create a webhook integration:

1. In the AI Exposure Console, navigate to **Settings** > **Integrations** and click on **Webhook**.
2. Click **Lets Start**.
3. Enter a **Display name** for the webhook in Tenable. For example, Telegram Webhook.
4. For the **Webhook URL**, enter the API endpoint URL of the API Gateway for the lambda trigger that was created when you created a CloudFormation stack.

5. For **HTTP Headers**, enter the following details:
    - Name: **x-api-key**
    - Value: Enter the API key of the API Gateway for the lambda trigger that was created when you created a CloudFormation stack.



6. Click **SAVE**.

    You can now create automation rules or manually trigger actions to send AI Exposure finding data to Telegram via webhook.

Configure In-Account Scanning

To configure in-account scanning, create and connect a dedicated account, and then grant Tenable One AI Exposure permissions to provision the necessary infrastructure resources in the target account.

To configure in-account scanning:

1. Create one or more dedicated account/s for scanning purposes.

   > **Note:** Only one scanning account can be defined per scope in AI Exposure. A scanning account can only be mapped to a single scope. Customers are responsible for any relevant compute costs associated with such accounts (estimated at about $300 per region). See Resources Provisioned per Region for more information.

2. Connect the account in AI Exposure.
3. Depending on your cloud provider, add the following to the account to grant Tenable the necessary permissions required to manage compute resources:
   - **AWS** – Add all required permissions.
   - **Alibaba Cloud** – Attach all required permissions to the Tenable RAM role.
   - **Azure** – Assign all required permissions the AI Exposure Connector app.
   - **GCP** – Add all required permissions.
   - **OCI** – Add all required permissions.
4. Contact Support for help completing the process. At this point:
   - Tenable will provision the necessary compute resources for each region in which you have virtual machines. See Resources Provisioned per Region for more information.
   - Tenable will orchestrate the scanning on a regular basis.

Required Alibaba Cloud Permissions

Grant Tenable the permissions required to deploy, manage, and scan workloads in the dedicated, in-account Alibaba Cloud account by creating a custom RAM policy and attaching it to the Tenable RAM role. These permissions allow Tenable to:

- Provision and manage the ACK cluster and its node pools, including the ROS stack, Auto Scaling resources, and ECS disks and security groups.
- Create and manage the VPC networking components, such as VSwitches, NAT gateways, Elastic IPs, route tables, and the VPC gateway endpoint.

- Manage the RAM roles, resource groups, and KMS instance and key used to encrypt and decrypt Kubernetes secrets and to scan encrypted disks.

Most create and delete actions are limited by condition to resources tagged with a `Namespace` value that starts with `Tenable`.

JSON

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeDisks",
        "ecs:DescribeSecurityGroupAttribute",
        "ecs:DescribeSecurityGroups",
        "ecs:TagResources"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ecs:CreateSecurityGroup",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "acs:RequestTag/Namespace": "Tenable*"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecs:AuthorizeSecurityGroup",
        "ecs:AuthorizeSecurityGroupEgress",
        "ecs:DeleteDisk",
        "ecs:DeleteSecurityGroup",
        "ecs:RevokeSecurityGroup",
        "ecs:RevokeSecurityGroupEgress"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "acs:ResourceTag/Namespace": "Tenable*"
```

```
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ram:GetResourceGroup",
        "ram:GetRole",
        "ram:ListResourceGroups",
        "ram:ListRoles",
        "ram:UpdateAssociatedTransferSetting"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ram:CreateResourceGroup",
        "ram:CreateServiceLinkedRole",
        "ram:DeleteResourceGroup"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "ram:CreateRole",
      "Resource": "acs:ram:*:*:role/Aliyun*Role"
    },
    {
      "Effect": "Allow",
      "Action": "ram:CreateRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "acs:RequestTag/Namespace": "Tenable*"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ram:AttachPolicyToRole",
      "Resource": "acs:ram:*:*:role/Aliyun*Role"
    },
    {
      "Effect": "Allow",
      "Action": "ram:AttachPolicyToRole",
      "Resource": "acs:ram:*:system:policy/Aliyun*Policy"
```

```
    },
    {
      "Effect": "Allow",
      "Action": "ram:AttachPolicyToRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "acs:ResourceTag/Namespace": "Tenable*"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ram:TagResources",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "resourcemanager:GetAutoGroupingRule",
        "resourcemanager:GetAutoGroupingStatus",
        "resourcemanager:ListAssociatedTransferSetting",
        "resourcemanager:ListAutoGroupingRules"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "resourcemanager:CreateAutoGroupingRule",
        "resourcemanager:DeleteAutoGroupingRule",
        "resourcemanager:EnableAccount",
        "resourcemanager:EnableAssociatedTransfer",
        "resourcemanager:EnableAutoGrouping",
        "resourcemanager:TagResources",
        "resourcemanager:UpdateAssociatedTransferSetting",
        "resourcemanager:UpdateResourceGroupAdminSetting"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ros:GetStack",
        "ros:ListStacks",
        "ros:TagResources"
```

```
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "cs:DescribeClusterDetail",
        "cs:DescribeClusterNodePoolDetail",
        "cs:DescribeClusterNodePools",
        "cs:DescribeClusterResources",
        "cs:DescribeClusterUserKubeconfig",
        "cs:DescribeKubernetesVersionMetadata",
        "cs:DescribeTaskInfo",
        "cs:GetClusterAddonInstance",
        "cs:GetClusters",
        "cs:ListClusterAddonInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "cs:CreateCluster",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "acs:RequestTag/Namespace": "Tenable*"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "cs:CreateClusterNodePool",
      "Resource": "acs:cs:*:*:cluster/*",
      "Condition": {
        "StringLike": {
          "acs:ResourceTag/Namespace": "Tenable*"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "cs:DeleteCluster",
        "cs:DeleteClusterNodepool",
        "cs:EnableSecretEncryption",
        "cs:ModifyClusterNodePool",
        "cs:ModifyClusterTags",
```

```
        "cs:UpdateUserPermissions",
        "cs:UpgradeCluster",
        "cs:UpgradeClusterNodepool"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "acs:ResourceTag/Namespace": "Tenable*"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:DescribeAccountKmsStatus",
        "kms:DescribeKey",
        "kms:GetKmsInstance",
        "kms:ListAliases",
        "kms:ListKeys",
        "kms:ListKmsInstances",
        "kms:ListTagResources"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:ConnectKmsInstance",
        "kms:CreateAlias",
        "kms:CreateKey",
        "kms:DeleteAlias",
        "kms:OpenKmsService",
        "kms:SetKeyPolicy",
        "kms:ReleaseKmsInstance",
        "kms:TagResources",
        "kms:UpdateDKMSInstance"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:ScheduleKeyDeletion",
        "kms:SetDeletionProtection"
      ],
      "Resource": "*",
      "Condition": {
```

```
      "StringLike": {
        "kms:tag/Namespace": "Tenable*"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "vpc:DescribeEipAddresses",
      "vpc:DescribeNatGateways",
      "vpc:DescribeRouteEntryList",
      "vpc:DescribeRouteTableList",
      "vpc:DescribeSnatTableEntries",
      "vpc:DescribeVpcAttribute",
      "vpc:DescribeVpcs",
      "vpc:DescribeVSwitches",
      "vpc:ListDhcpOptionsSets",
      "vpc:ListTagResources",
      "vpc:ListVpcGatewayEndpoints"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "vpc:CreateRouteEntry",
      "vpc:CreateSnatEntry",
      "vpc:CreateVSwitch",
      "vpc:TagResources"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "vpc:AllocateEipAddress",
      "vpc:CreateNatGateway",
      "vpc:CreateRouteTable",
      "vpc:CreateVpc",
      "vpc:CreateVpcGatewayEndpoint"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "acs:RequestTag/Namespace": "Tenable*"
      }
```

```
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "vpc:AssociateEipAddress",
      "vpc:AssociateRouteTable",
      "vpc:AssociateRouteTablesWithVpcGatewayEndpoint",
      "vpc:DeleteDhcpOptionsSet",
      "vpc:DeleteNatGateway",
      "vpc:DeleteRouteEntry",
      "vpc:DeleteRouteTable",
      "vpc:DeleteSnatEntry",
      "vpc:DeleteVpc",
      "vpc:DeleteVpcGatewayEndpoint",
      "vpc:DeleteVSwitch",
      "vpc:DissociateRouteTablesFromVpcGatewayEndpoint",
      "vpc:ModifyVpcAttribute",
      "vpc:ReleaseEipAddress",
      "vpc:UnassociateEipAddress",
      "vpc:UnassociateRouteTable"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "acs:ResourceTag/Namespace": "Tenable*"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "bss:DescribeInstances",
      "bss:ModifyInstance",
      "bss:QueryAvailableInstances"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "tag:ListTagResources",
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "tag:TagResources",
    "Resource": "*",
```

```
      "Condition": {
        "StringLike": {
          "acs:RequestTag/Namespace": "Tenable*"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecs:CreateDisk",
        "ecs:DescribeSnapshots"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "resourcesharing:ListResourceShareInvitations",
        "resourcesharing:AcceptResourceShareInvitation"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "cs:DescribeRegions",
        "cs:DescribeClusterNodes"
      ],
      "Resource": "*"
    }
  ]
}
```

Disk Securing for Scanning

When a disk is created for scan in the outpost account, Tenable encrypts it. ECS uses a RAM role named `AliyunECSDiskEncryptDefaultRole` to create the encrypted disks for scanning.

Tenable creates the role once per account. If the role already exists in your account, Tenable keeps it and attaches the `AliyunECSDiskEncryptRolePolicy` system policy to it. The policy you created in Required Alibaba Cloud Permissions already covers role creation, so you have nothing extra to add.

For disks encrypted with Alibaba-managed keys, Tenable re-encrypts the snapshots with a KMS key it provisions, so the disks can be scanned. See Alibaba Cloud for details.

If you want to check the role, or create it yourself, use the following policies.

Trust Policy

JSON

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "ecs.aliyuncs.com"
        ]
      }
    }
  ],
  "Version": "1"
}
```

Permissions

Attach the `AliyunECSDiskEncryptRolePolicy` system policy to the role. If this policy is not available in your Alibaba Cloud console, create a custom policy with the following content and attach it to the role:

JSON

```
{
  "Version": "1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:List*",
        "kms:DescribeKey",
        "kms:TagResource",
        "kms:UntagResource"
```

```
      ],
      "Resource": [
        "acs:kms:*:*:*",
        "acs:kms:*:*:*/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": [
        "acs:kms:*:*:*/*"
      ]
    }
  ]
}
```

Required AWS Permissions

The required AWS permissions consist of an AWS managed policy and a custom inline policy.

- Attach the following AWS managed policy: AmazonVPCFullAccess.
- Add the below custom inline policy to the IAM role you created during integration.

These permissions are needed to deploy, manage, and scan workloads in a customer's environment. This includes provisioning and modifying compute resources (EC2, Auto Scaling, EKS), managing IAM roles and policies for authentication and access control, handling encryption keys for secure data access (KMS), and organizing resources efficiently (Resource Groups). These permissions ensure the necessary infrastructure is in place for workload scanning while maintaining security and compliance.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": [
                "autoscaling:UpdateAutoScalingGroup"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:DetachVolume"
              ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVolume",
            "Resource": "arn:aws:ec2:*:*:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Context": "WorkloadAnalysis"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVolume",
            "Resource": "arn:aws:ec2:*:*:snapshot/*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteVolume",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Context": "WorkloadAnalysis"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateLaunchTemplate",
                "ec2:CreateLaunchTemplateVersion",
                "ec2:DeleteLaunchTemplate",
                "ec2:ModifyLaunchTemplate",
                "ec2:RunInstances"
```

```
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "eks:AssociateEncryptionConfig",
                "eks:CreateAddon",
                "eks:CreateCluster",
                "eks:CreateNodegroup",
                "eks:CreatePodIdentityAssociation",
                "eks:DeleteCluster",
                "eks:DeleteNodegroup",
                "eks:TagResource",
                "eks:UpdateAddon",
                "eks:UpdateClusterVersion",
                "eks:UpdateNodegroupConfig",
                "eks:UpdateNodegroupVersion"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreateRole",
                "iam:CreateServiceLinkedRole",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:List*Tags",
                "iam:PassRole",
                "iam:PutRolePolicy",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:Tag*",
                "iam:UpdateAssumeRolePolicy"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:CreateAlias",
                "kms:CreateGrant",
                "kms:CreateKey",
                "kms:Decrypt",
                "kms:DeleteAlias",
```

```
                "kms:DescribeKey",
                "kms:EnableKeyRotation",
                "kms:GenerateDataKeyWithoutPlaintext",
                "kms:ListAliases",
                "kms:ListKeys",
                "kms:ListResourceTags",
                "kms:ReEncryptFrom",
                "kms:ReEncryptTo",
                "kms:ScheduleKeyDeletion",
                "kms:TagResource"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "license-manager:ListReceivedLicenses",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "rds:AddTagsToResource",
                "rds:CopyDBClusterSnapshot",
                "rds:CopyDBSnapshot",
                "rds:CreateDBClusterParameterGroup",
                "rds:CreateDBInstance",
                "rds:CreateDBSnapshot",
                "rds:CreateDBSubnetGroup",
                "rds:DeleteDBCluster",
                "rds:DeleteDBClusterParameterGroup",
                "rds:DeleteDBClusterSnapshot",
                "rds:DeleteDBInstance",
                "rds:DeleteDBSnapshot",
                "rds:DeleteDBSubnetGroup",
                "rds:ModifyDBCluster",
                "rds:ModifyDBClusterParameterGroup",
                "rds:ModifyDBInstance",
                "rds:RestoreDBClusterFromSnapshot",
                "rds:RestoreDBInstanceFromDBSnapshot"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "resource-groups:CreateGroup",
                "resource-groups:DeleteGroup",
```

```
                "resource-groups:Get*",
                "resource-groups:Tag"
            ],
            "Resource": "*"
        }
    ]
}
```

Required Azure Permissions

Assign the following **custom role** to the *AI Exposure Connector* app in the dedicated, in-account subscription. This role enables Tenable to:

- Oversee managed disks, including the creation and deletion of disks.
- Create the role definition (`TenableRoleDefinitionWorkloadAnalysisScanning`) responsible for allowing the Kubernetes cluster to attach a disk to the scan job.

JSON

```
{
    "properties": {
        "assignableScopes": [
            "/subscriptions/<SubscriptionId>"
        ],
        "description": "",
        "permissions": [
            {
                "actions": [
                    "Microsoft.Authorization/roleAssignments/delete",
                    "Microsoft.Authorization/roleAssignments/write",
                    "Microsoft.Authorization/roleDefinitions/delete",
                    "Microsoft.Authorization/roleDefinitions/write",
                    "Microsoft.Compute/disks/delete",
                    "Microsoft.Compute/disks/write",
                    "Microsoft.Compute/register/action",
                    "Microsoft.Compute/skus/read",
                    "Microsoft.Compute/virtualMachines/attachDetachDataDisks/action",
                    "Microsoft.Compute/virtualMachines/write",
                    "Microsoft.Compute/virtualMachineScaleSets/virtualMachines/restart/action",
                    "Microsoft.Compute/virtualMachineScaleSets/write",
                    "Microsoft.ContainerService/managedClusters/agentPools/abort/action",
                    "Microsoft.ContainerService/managedClusters/agentPools/deleteMachines/action",
```

```
                    "Microsoft.ContainerService/managedClusters/agentPools/machines/read",
                    "Microsoft.ContainerService/managedClusters/agentPools/machines/write",
                    "Microsoft.ContainerService/managedClusters/agentPools/read",
                    "Microsoft.ContainerService/managedClusters/agentPools/upgradeNodeImageVersion/action"
,
                    "Microsoft.ContainerService/managedClusters/agentPools/write",
                    "Microsoft.ContainerService/managedClusters/delete",
                    "Microsoft.ContainerService/managedClusters/listClusterUserCredential/action",
                    "Microsoft.ContainerService/managedClusters/write",
                    "Microsoft.ContainerService/register/action",
                    "Microsoft.Features/providers/features/register/action",
                    "Microsoft.KeyVault/*",
                    "Microsoft.ManagedIdentity/register/action",
                    "Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
                    "Microsoft.ManagedIdentity/userAssignedIdentities/delete",
                    "Microsoft.ManagedIdentity/userAssignedIdentities/federatedIdentityCredentials/delete"
,
                    "Microsoft.ManagedIdentity/userAssignedIdentities/federatedIdentityCredentials/write",
                    "Microsoft.ManagedIdentity/userAssignedIdentities/write",
                    "Microsoft.Network/natGateways/delete",
                    "Microsoft.Network/natGateways/write",
                    "Microsoft.Network/networkSecurityGroups/delete",
                    "Microsoft.Network/networkSecurityGroups/join/action",
                    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
                    "Microsoft.Network/networkSecurityGroups/securityRules/write",
                    "Microsoft.Network/networkSecurityGroups/write",
                    "Microsoft.Network/publicIPAddresses/delete",
                    "Microsoft.Network/publicIPAddresses/write",
                    "Microsoft.Network/register/action",
                    "Microsoft.Network/routeTables/delete",
                    "Microsoft.Network/routeTables/join/action",
                    "Microsoft.Network/routeTables/write",
                    "Microsoft.Network/virtualNetworks/delete",
                    "Microsoft.Network/virtualNetworks/subnets/delete",
                    "Microsoft.Network/virtualNetworks/subnets/join/action",
                    "Microsoft.Network/virtualNetworks/subnets/write",
                    "Microsoft.Network/virtualNetworks/write",
                    "Microsoft.Resources/subscriptions/providers/read",
                    "Microsoft.Resources/subscriptions/resourceGroups/delete",
                    "Microsoft.Resources/subscriptions/resourceGroups/write",
                    "Microsoft.Resources/tags/write",
                    "Microsoft.Storage/register/action",
                    "Microsoft.Storage/storageAccounts/blobServices/containers/delete",
                    "Microsoft.Storage/storageAccounts/blobServices/containers/write",
                    "Microsoft.Storage/storageAccounts/delete",
                    "Microsoft.Storage/storageAccounts/listkeys/action",
                    "Microsoft.Storage/storageAccounts/managementPolicies/delete",
```

```
                    "Microsoft.Storage/storageAccounts/managementPolicies/write",
                    "Microsoft.Storage/storageAccounts/write"
                ],
                "dataActions": [
                    "Microsoft.ContainerService/managedClusters/*",
                    "Microsoft.KeyVault/vaults/keyrotationpolicies/*",
                    "Microsoft.KeyVault/vaults/keys/*",
                    "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete",
                    "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read",
                    "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write"
                ],
                "notActions": [],
                "notDataActions": []
            }
        ],
        "roleName": "InAccountCustomRole"
    }
}
```

Required GCP Permissions

Add the following predefined roles to the AI Exposure service account you created during integration:

GCP Role	Description
`Cloud KMS Admin`	Needed to manage encryption keys used for decrypting and scanning workloads that are encrypted at rest.
`Editor`	Grants permissions to read and modify resources, enabling workload scanning across various GCP services.
`Kubernetes Engine Admin`	Required to inspect workloads running in Google Kubernetes Engine (GKE) clusters and ensure security compliance.
`Project IAM Admin`	Needed to manage IAM policies, ensuring the scanner has the necessary permissions to access and inspect workloads across the project.

GCP Role	Description
`Service Account Admin`	Allows the creation and management of service accounts needed for authentication and scanning operations.

Required OCI Permissions

Grant AI Exposure permissions to scan OCI In-Account workloads by adding the below statements to the OCI policy that you created during integration.

- `Allow group TenableCS to manage all-resources in compartment <InAccount compartment OCID>`
- `Allow group TenableCS to use volumes in tenancy`

To scan volumes **encrypted with customer-managed keys**, add the following statement to the OCI policy:

- `Allow group TenableCS to use key-delegate in tenancy`

Resources Provisioned per Region

This section focuses on detailing the **specific cloud infrastructure components** (resources) that Tenable deploys and uses within each distinct geographical **cloud region**, along with the **specific technical requirements and context** for each component.

- Alibaba Cloud
- AWS
- Azure
- GCP
- OCI

Resource	Requirement	Context
Compute	• ACK (Managed Kubernetes) cluster • 2 Auto Scaling Groups • ROS (Resource Orchestration Service) Stack • Scanning virtual machines	• **ACK cluster** – Manages scanning operations and orchestration • **Auto Scaling Groups** – One per node pool (Default and Spot), manage scaling of worker nodes • **ROS Stack** – Infrastructure stack auto-created by ACK for cluster resources • **Scanning virtual machines** – Execute the scanning operations. Scalable on demand, with a maximum capacity of 32 vCPUs and 64 GB RAM The number and size of nodes are automatically managed by Tenable to minimize costs while meeting scanning demands
Identities	3 RAM roles	• Used by the ACK cluster (node pools) • Used by the management pod • `AliyunECSDiskEncryptDefaultRole` – Used by ECS to create encrypted disks for scanning. Created once per account. If the role already exists, Tenable keeps it and attaches the `AliyunECSDiskEncryptRolePolicy` system policy
Storage	N/A	N/A

Resource	Requirement	Context
Network	• 1 DHCP Options Set • 2 Elastic IPs • 2 ENIs (Elastic Network Interfaces) • 1 NAT gateway • 3 Route tables • 3 Security groups • 1 SLB (Server Load Balancer) • 2 VSwitches • 1 VPC • 1 VPC Gateway Endpoint (OSS)	• **VSwitches** – 1 Egress VSwitch for outbound traffic; 1 Private VSwitch for internal communication • **Elastic IPs** – Used by the NAT gateway and ACK cluster • **NAT gateway** – Used for egress traffic • **SLB** – Internal load balancer for Kubernetes API server • **VPC** – Network container • **VPC Gateway Endpoint** – Private access to Object Storage
Security	• KMS instance • 2 KMS keys	• **KMS instance** – Key Management Service for the region • **KMS key** – Used to encrypt and decrypt Kubernetes secrets • **KMS key** – Used to re-encrypt snapshots of disks encrypted with Alibaba-managed keys so they can be scanned. Shared with the accounts the outpost scans

AWS

Resource	Requirement	Context
Compute	• EKS cluster • 2 On-demand management virtual machine, 4 vCPU, and 16 GB RAM • Scanning virtual machines	• **EKS cluster** – Manages scanning operations and orchestration • **Management virtual machines** – Orchestrate scanning processes initiated by the EKS cluster • **Scanning virtual machines** – Execute the scanning operations. Scalable on demand, with a maximum capacity of 32 vCPUs and 64 GB RAM **Note**: Could be increased if needed The number and size of provisioned nodes are automatically managed by Tenable to minimize costs while meeting scanning demands
Identities	5 IAM roles	• Used by the EKS cluster (control plane) • Used by Kublet management nodes • Used by Karpenter nodes Kublet for launching and scanning VMs • Used by the EBS CSI driver for attaching disks to a EC2 instance for scanning • Used by the management pod
Storage	N/A	N/A
Network	• 2 Elastic IPs • 1 Internet gateway • 2 NAT gateways	• **Subnets** – 2 Egress subnets to communicate externally; 2 private subnets to communicate internally • **Internet gateway** – Used for egress traffic

Resource	Requirement	Context
	• 6 Route tables • 4 Security groups • 6 Subnets • 1 VPC	• **NAT gateways** – Used by the NAT • **VPC** – Network container The subnets are used for private subnets, EKS (control plane and workers), and VPC
Security	KMS key	Used to encrypt and decrypt Kubernetes secrets
Minimum Estimated Cost (per month)	$300	Minimum cost for infrastructure, not including scanning costs. Learn more about scanning costs for Workload and Data Protection.

Azure

Resource	Requirement	Context
Compute	• AKS cluster • 2 On-demand management virtual machine, 4 vCPU, and 16 GB RAM • Scanning virtual machines • Internal load balancer	• **AKS cluster** – Manages scanning operations and orchestration • **Management virtual machines** – Orchestrates scanning processes within the AKS cluster • **Scanning virtual machines** – Execute the scanning operations. Scalable on demand, with a maximum capacity of 32 vCPUs and 64 GB RAM. **Note**: Could be increased if needed • **Load balancer** – Used for managing inbound and outbound traffic for the ASK API server

Resource	Requirement	Context

Identities	3 User-managed identities	• Used by the AKS cluster (control plane) for:
		  • Attach disks to a VM for scanning
		  • Encrypt and decrypt Kubernetes secrets
		• Used by Kublet (created by Azure automatically upon AKS creation)
		• Used by Karpenter for launching and scanning VMs

Storage	• 1 Storage account • 1 Blob container	Copies managed disks from the scanned subscription to the scanning subscription

Network	• 3 Subnets
	  • 3 Network security groups
	• 1 Private endpoint
	• 1 NAT gateway
	• 1 Public IP
	• 1 Virtual network
	• 3 Route tables
		• **Subnets** – 1 egress subnet to communicate externally; 1 private subnet to communicate internally; 1 subnet for ASK API server VNet integration
		  • **Security groups** – Used per network subnet
		• **Private endpoint** – Maps a private IP from the AKS virtual network to Azure key vault, isolating API traffic from the internet.
		• **NAT gateway** – Used for egress traffic
		• **Public IP** – Used by the NAT
		• **Virtual network** – Network container
		• **Route tables** – Used by the subnets

Resource	Requirement	Context
Security	Key vault key	Used to encrypt and decrypt Kubernetes secrets
Minimum Estimated Cost (per month)	$325	Minimum cost for infrastructure, not including scanning costs. Learn more about scanning costs for Workload and Data protection.

GCP

Resource	Requirement	Context
Compute	• 1 GKE cluster • 1 Spot machine - e2-standard-2 (2vCPU and 8GB RAM)	• **GKE Cluster** – Manages scanning operations and orchestration The number and size of provisioned nodes are automatically managed by Tenable to minimize costs while meeting scanning demands
Identities	1 Service account (per project)	Used by the GKE cluster nodes Kubelet (control plane)
Storage	N/A	N/A
Network	• 1 Egress subnet • 1 Private subnet • 1 IP address • 1 Router	• **Subnets** – 1 egress subnet to communicate externally; 1 private subnet to communicate internally • **Router + NAT** – Used for egress traffic • **IP** – Used by the NAT • **VPC** (Network container): Provides network

Resource	Requirement	Context
	• 1 NAT gateway • 1 VPC (per project)	isolation for the private subnet and GKE (control plane and nodes)
Security	Cloud key ring key	Used to encrypt and decrypt Kubernetes secrets
Minimum Estimated Cost (per month)	$300	Minimum cost for infrastructure, not including scanning costs. Learn more about scanning costs for Workload and Data Protection.

OCI

Resource	Requirement	Context
Compute	• 1 OKE cluster • Nodes	• **Nodes** – One node per Availability Domain Tenable automatically manages the number and size of provisioned nodes to minimize costs while meeting scanning demands
Identities	N/A	N/A
Storage	N/A	N/A
Network	• 3 Subnets • 3 Route tables • VCN • 3 Security	• **Subnets** – 2 egress subnets to communicate externally; 1 private subnet to communicate internally • **NAT gateway** – Used for egress traffic • **IP** – Used by the NAT

Resource	Requirement	Context
	lists • 1 Internet gateway • 1 Reserved IP • 1 NAT gateway • 1 Service gateway	• **VCN** (Network container): Provides network isolation for private subnets and OKE (control plane and nodes)
Security	• Vault • Key	Used to encrypt and decrypt Kubernetes secrets
Minimum Estimated Cost (per month)	$300	Minimum cost for infrastructure, not including scanning costs. Learn more about scanning costs for Workload and Data Protection.