

Table of Contents


Cloud Onboarding

AWS FAQs	2
--------------------------------	---


AWS FAQs

Frequently Asked Questions - Contents

- [Why is Tenable trying to gain Console access to my account?](#)
 - [Why does Tenable need both an inline and managed policy?](#)
 - [Why does Tenable need the GetObject permission for Elastic Beanstalk Buckets?](#)
 - [How soon are new services or permissions added to Tenable?](#)
 - [Why does the CloudTrail have to be multi-region?](#)
 - [Why does Tenable need to access the US East Region?](#)
-

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 Tenable Cloud Security require such access? 


A: Generally speaking, Tenable Cloud Security 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.

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? 

A: 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 Tenable Cloud Security. 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.

Why does Tenable need the GetObject permission for Elastic Beanstalk buckets in onboarded accounts? 


A: 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.

When AWS adds new services or permissions to their offering, how soon are they reflected in Tenable? 

A: As soon as the new services or permissions become available, but it may take up to one week before they are displayed in the Tenable Cloud Security Console. The process of detecting such changes is done programmatically, and not manually.

Why does the CloudTrail that Tenable needs to read data from have to be multi-region? 

A: Tenable Cloud Security 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.

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? 

A: 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](#) and [here](#).

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.