



We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection by clicking "Manage Cookies" at the bottom of the page. [Privacy Statement](#) [Third-Party Cookies](#)

Accept

Reject

Manage cookies

Microsoft Ignite

Nov 19–22, 2024

Register now >



Learn

Discover ▾

Product documentation ▾

Development languages ▾

Topics ▾

Search Sign in

Microsoft Entra

Microsoft Entra ID

External ID

Global Secure Access

ID Governance

Permissions Management

More ▾

Admin center

Learn / Microsoft Entra / Microsoft Entra ID Governance / Privileged Identity Management



Configure security alerts for Microsoft Entra roles in Privileged Identity Management

Article • 03/25/2024 • 18 contributors

Feedback

In this article

[License requirements](#)

[Security alerts](#)

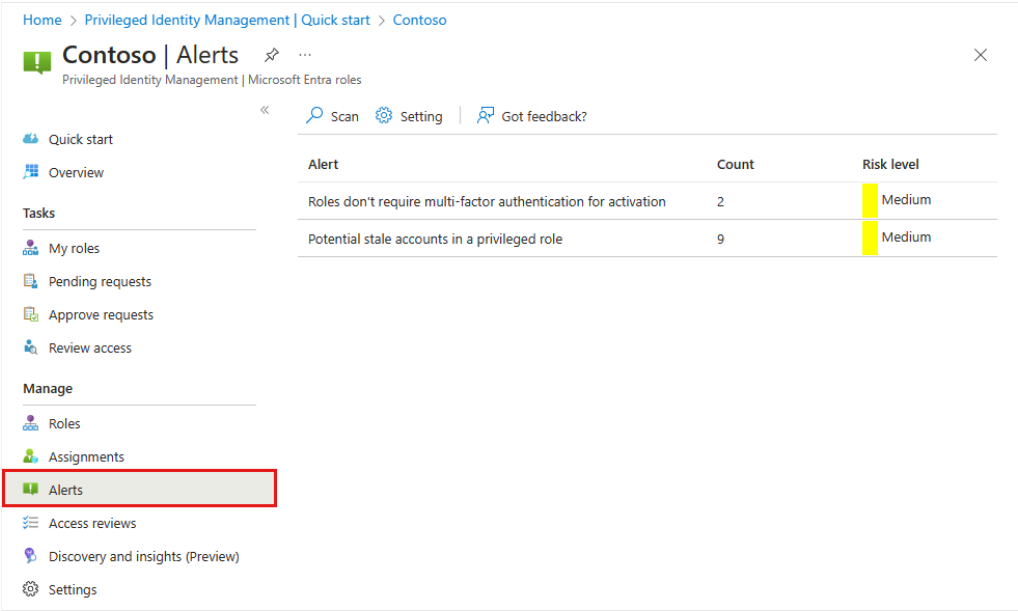
[Customize security alert settings](#)

[Next steps](#)

Privileged Identity Management (PIM) generates alerts when there's suspicious or unsafe activity in your organization in Microsoft Entra ID. When an alert is triggered, it shows up on the Privileged Identity Management dashboard. Select the alert to see a report that lists the users or roles that triggered the alert.

Note

One event in Privileged Identity Management can generate email notifications to multiple recipients – assignees, approvers, or administrators. The maximum number of notifications sent per one event is 1000. If the number of recipients exceeds 1000 – only the first 1000 recipients will receive an email notification. This does not prevent other assignees, administrators, or approvers from using their permissions in Microsoft Entra ID and Privileged Identity Management.




License requirements

Using Privileged Identity Management requires licenses. For more information on licensing, see [Microsoft Entra ID Governance licensing fundamentals](#).

Security alerts

This section lists all the security alerts for Microsoft Entra roles, along with how to fix and how to prevent. Severity has the following meaning:

- **High:** Requires immediate action because of a policy violation.
- **Medium:** Doesn't require immediate action but signals a potential policy violation.
- **Low:** Doesn't require immediate action but suggests a preferable policy change.

 **Note**

Only the following roles are able to read PIM security alerts for Microsoft Entra roles: **Global Administrator, Privileged Role Administrator, Global Reader, Security Administrator, and Security Reader.**

Administrators aren't using their privileged roles

Severity: Low

 Expand table

Description	
Why do I get this alert?	Users that have been assigned privileged roles they don't need increases the chance of an attack. It's also easier for attackers to remain unnoticed in accounts that aren't

	actively being used.
How to fix?	Review the users in the list and remove them from privileged roles that they don't need.
Prevention	Assign privileged roles only to users who have a business justification. Schedule regular access reviews to verify that users still need their access.
In-portal mitigation action	Removes the account from their privileged role.
Trigger	Triggered if a user goes over a specified number of days without activating a role.
Number of days	This setting specifies the maximum number of days, from 0 to 100, that a user can go without activating a role.

Roles don't require multifactor authentication for activation

Severity: Low

 Expand table

	Description
Why do I get this alert?	Without multifactor authentication, compromised users can activate privileged roles.
How to fix?	Review the list of roles and require multifactor authentication for every role.
Prevention	Require MFA for every role.
In-portal mitigation action	Makes multifactor authentication required for activation of the privileged role.

The organization doesn't have Microsoft Entra ID P2 or Microsoft Entra ID Governance

Severity: Low

 Expand table

	Description
Why do I get this alert?	The current Microsoft Entra organization doesn't have Microsoft Entra ID P2 or Microsoft Entra ID Governance.
How to fix?	Review information about Microsoft Entra editions . Upgrade to Microsoft Entra ID P2 or Microsoft Entra ID Governance.

Potential stale accounts in a privileged role

Severity: Medium

Expand table

Description	
Why do I get this alert?	This alert is no longer triggered based on the last password change date of for an account. This alert is for accounts in a privileged role that haven't signed in during the past <i>n</i> days, where <i>n</i> is many days that is configurable between 1-365 days. These accounts might be service or shared accounts that aren't being maintained and are vulnerable to attackers.
How to fix?	Review the accounts in the list. If they no longer need access, remove them from their privileged roles.
Prevention	Ensure that accounts that are shared are rotating strong passwords when there's a change in the users that know the password. Regularly review accounts with privileged roles using access reviews and remove role assignments that are no longer needed.
In-portal mitigation action	Removes the account from their privileged role.
Best practices	<p>Shared, service, and emergency access accounts that authenticate using a password and are assigned to highly privileged administrative roles such as Global Administrator or Security Administrator should have their passwords rotated for the following cases:</p> <ul style="list-style-type: none">• After a security incident involving misuse or compromise of administrative access rights• After any user's privileges are changed so that they're no longer an administrator (for example, after an employee who was an administrator leaves IT or leaves the organization)• At regular intervals (for example, quarterly or yearly), even if there was no known breach or change to IT staffing <p>Since multiple people have access to these accounts' credentials, the credentials should be rotated to ensure that people that have left their roles can no longer access the accounts. Learn more about securing accounts</p>

Roles are being assigned outside of Privileged Identity Management

Severity: High

Expand table

Description	
Why do I get this alert?	Privileged role assignments made outside of Privileged Identity Management aren't properly monitored and may indicate an active attack.
How to fix?	Review the users in the list and remove them from privileged roles assigned outside of Privileged Identity Management. You can also enable or disable both the alert and its accompanying email notification in the alert settings.
Prevention	Investigate where users are being assigned privileged roles outside of Privileged Identity Management and prohibit future assignments from there.
In-portal mitigation	Removes the user from their privileged role.

Filter by title

- Privileged Identity Management documentation
- > Overview
 - > Concepts
 - > How-to guides
 - Deploy PIM
 - Start using PIM
 - > Bring under management
 - > Assign
 - > Activate
 - > Approve
 - > Extend or renew
 - > Set role settings

- Set up alerts
- Microsoft Entra roles
- Microsoft Entra roles - Microsoft Graph
- Azure roles
- Audits
- Review access
- Discovery & Insights for Microsoft Entra roles
- Elevate access to manage Azure subscriptions
- Troubleshoot resource access denied
- Reference

action

ⓘ Note

PIM sends email notifications for the **Role assigned outside of PIM** alert when the alert is enabled from [alert settings](#). For Microsoft Entra roles in PIM, emails are sent to **Privileged Role Administrators, Security Administrators, and Global Administrators** that have enabled Privileged Identity Management. For Azure resources in PIM, emails are sent to **Owners** and **User Access Administrators**.

There are too many Global Administrators

Severity: Low

Expand table

Description	
Why do I get this alert?	Global Administrator is the highest privileged role. If a Global Administrator is compromised, the attacker gains access to all of their permissions, which put your whole system at risk.
How to fix?	Review the users in the list and remove any that don't absolutely need the Global Administrator role. Assign lower privileged roles to these users instead.
Prevention	Assign users the least privileged role they need.
In-portal mitigation action	Removes the account from their privileged role.
Trigger	Triggered if two different criteria are met, and you can configure both of them. First, you need to reach a certain threshold of Global Administrator role assignments. Second, a certain percentage of your total role assignments must be Global Administrators. If you only meet one of these measurements, the alert doesn't appear.
Minimum number of Global Administrators	This setting specifies the number of Global Administrator role assignments, from 2 to 100, that you consider to be too few for your Microsoft Entra organization.
Percentage of Global Administrators	This setting specifies the minimum percentage of administrators who are Global Administrators, from 0% to 100%, below which you do not want your Microsoft Entra organization to dip.

Download PDF

Roles are being activated too frequently

Severity: Low

Expand table

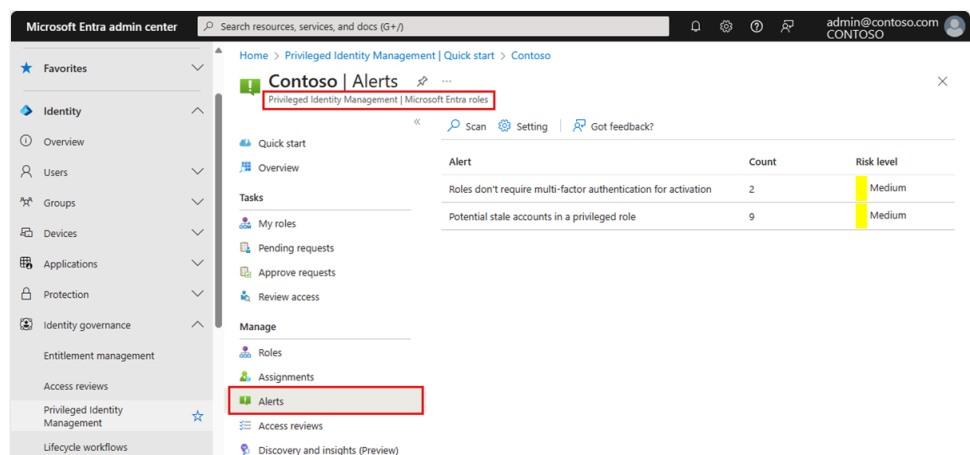
Description

Why do I get this alert?	Multiple activations to the same privileged role by the same user is a sign of an attack.
How to fix?	Review the users in the list and ensure that the activation duration for their privileged role is set long enough for them to perform their tasks.
Prevention	Ensure that the activation duration for privileged roles is set long enough for users to perform their tasks. Require multifactor authentication for privileged roles that have accounts shared by multiple administrators.
In-portal mitigation action	N/A
Trigger	Triggered if a user activates the same privileged role multiple times within a specified period. You can configure both the time period and the number of activations.
Activation renewal timeframe	This setting specifies in days, hours, minutes, and second the time period you want to use to track suspicious renewals.
Number of activation renewals	This setting specifies the number of activations, from 2 to 100, at which you would like to be notified, within the timeframe you chose. You can change this setting by moving the slider, or typing a number in the text box.

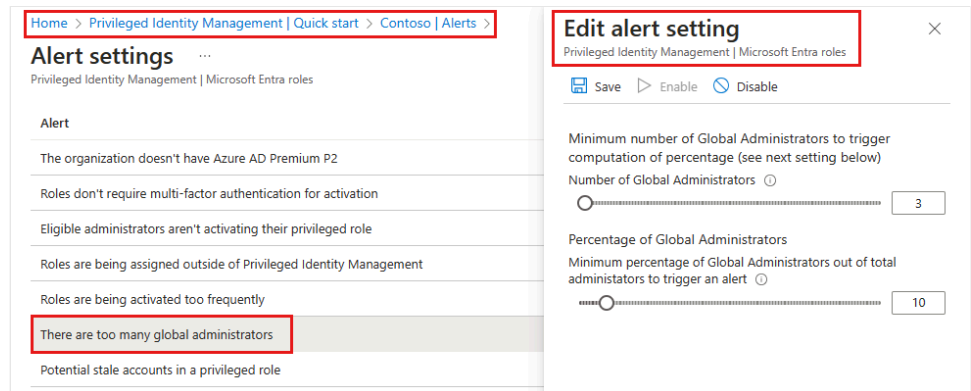
Customize security alert settings

Follow these steps to configure security alerts for Microsoft Entra roles in Privileged Identity Management:

1. Sign in to the [Microsoft Entra admin center](#) as at least a [Privileged Role Administrator](#).
2. Browse to **Identity governance** > **Privileged Identity Management** > **Microsoft Entra roles** > **Alerts** > **Setting**. For information about how to add the Privileged Identity Management tile to your dashboard, see [Start using Privileged Identity Management](#).



3. Customize settings on the different alerts to work with your environment and security goals.



Next steps

- [Configure Microsoft Entra role settings in Privileged Identity Management](#)

Feedback

Was this page helpful?

☒ Yes

☐ No

[Provide product feedback](#)

Additional resources

Training

Module


[Plan and implement privileged access - Training](#)


Ensuring that administrative roles are protected and managed to increase your Azure solution security is a must. Explore how to use PIM to protect your data and resources.


Certification

[Microsoft Certified: Identity and Access Administrator Associate - Certifications](#)

Demonstrate the features of Microsoft Entra ID to modernize identity solutions, implement hybrid solutions, and implement identity governance.

 English (United States)

 Your Privacy Choices

 Theme

[Manage cookies](#)

[Previous Versions](#)

[Blog](#)

[Contribute](#)

[Privacy](#)

[Terms of Use](#)

[Trademarks](#)

© Microsoft 2024