Microsoft Entra security operations for Privileged Identity Management - Microsoft Entra | Microsoft Learn - 02/11/2024 09:35

https://learn.microsoft.com/en-us/entra/architecture/security-operations-privileged-identity-management#azure-ad-roles-assignment

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

Sign in

Microsoft Entra   Microsoft Entra ID   External ID   Global Secure Access   ID Governance   Permissions Management   More

Admin center

Learn / Microsoft Entra / Architecture /

Microsoft Entra security operations for Privileged Identity Management

Article • 10/23/2023 • 7 contributors

Feedback

In this article

Where to look

Baselines

Privileged Identity Management Alerts

Microsoft Entra roles assignment

Show 3 more

The security of business assets depends on the integrity of the privileged accounts that administer your IT systems. Cyber-attackers use credential theft attacks to target admin accounts and other privileged access accounts to try gaining access to sensitive data.

For cloud services, prevention and response are the joint responsibilities of the cloud service provider and the customer.

Traditionally, organizational security has focused on the entry and exit points of a network as the security perimeter. However, SaaS apps and personal devices have made this approach less effective. In Microsoft Entra ID, we replace the network security perimeter with authentication in your organization's identity layer. As users are assigned to privileged administrative roles, their access must be protected in on-premises, cloud, and hybrid environments.

You're entirely responsible for all layers of security for your on-premises IT environment. When you use Azure cloud services, prevention and response are joint responsibilities of Microsoft as the cloud service provider and you as the customer.

- For more information on the shared responsibility model, see Shared responsibility in the cloud.

- For more information on securing access for privileged users, see Securing Privileged access for hybrid and cloud deployments in Microsoft Entra ID.

- For a wide range of videos, how-to guides, and content of key concepts for privileged identity, visit Privileged Identity Management documentation.

Privileged Identity Management (PIM) is a Microsoft Entra service that enables you to manage, control, and monitor access to important resources in your organization. These resources include resources in Microsoft Entra ID, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune. You can use PIM to help mitigate the following risks:

- Identify and minimize the number of people who have access to secure information and resources.

- Detect excessive, unnecessary, or misused access permissions on sensitive resources.

- Reduce the chances of a malicious actor getting access to secured information or resources.

- Reduce the possibility of an unauthorized user inadvertently impacting sensitive resources.

Use this article provides guidance to set baselines, audit sign-ins, and usage of privileged accounts. Use the source audit log source to help maintain privileged account integrity.

Where to look

The log files you use for investigation and monitoring are:

- Microsoft Entra audit logs

- Sign-in logs

- Microsoft 365 Audit logs

- Azure Key Vault logs

In the Azure portal, view the Microsoft Entra audit logs and download them as comma-separated value (CSV) or JavaScript Object Notation (JSON) files. The Azure portal has several ways to integrate Microsoft Entra logs with other tools to automate monitoring and alerting:

- **Microsoft Sentinel** – enables intelligent security analytics at the enterprise level by providing security information and event management (SIEM) capabilities.

- **Sigma rules** ⧉ - Sigma is an evolving open standard for writing rules and templates that automated management tools can use to parse log files. Where Sigma templates exist for our recommended search criteria, we've added a link to the Sigma repo. The Sigma templates aren't written, tested, and managed by Microsoft. Rather, the repo and templates are created and collected by the worldwide IT security community.

- **Azure Monitor** – enables automated monitoring and alerting of various conditions. Can create or use workbooks to combine data from different sources.

- **Azure Event Hubs** **integrated with a SIEM**- Microsoft Entra logs can be integrated to other SIEMs such as Splunk, ArcSight, QRadar, and Sumo Logic via the Azure Event Hubs integration.

- **Microsoft Defender for Cloud Apps** – enables you to discover and manage apps, govern across apps and resources, and check your cloud apps' compliance.

- **Securing workload identities with Microsoft Entra ID Protection** - Used to detect risk on workload identities across sign-in behavior and offline indicators of compromise.

The rest of this article has recommendations to set a baseline to monitor and alert on, with a tier model. Links to pre-built solutions appear after the table. You can build alerts using the preceding tools. The content is organized into the following areas:

- Baselines

- Microsoft Entra role assignment

- Microsoft Entra role alert settings

- Azure resource role assignment

- Access management for Azure resources

- Elevated access to manage Azure subscriptions

Baselines

The following are recommended baseline settings:

⛶ Expand table

What to monitor	Risk level	Recommendation	Roles	Notes

Microsoft Entra roles assignment	High	Require justification for activation. Require approval to activate. Set two-level approver process. On activation, require Microsoft Entra multifactor authentication. Set maximum elevation duration to 8 hrs.	Security Administrator, Privileged Role Administrator, Global Administrator	A privileged role administrator can customize PIM in their Microsoft Entra organization, including changing the experience for users activating an eligible role assignment.
Azure Resource Role Configuration	High	Require justification for activation. Require approval to activate. Set two-level approver process. On activation, require Microsoft Entra multifactor authentication. Set maximum elevation duration to 8 hrs.	Owner, User Access Administrator	Investigate immediately if not a planned change. This setting might enable attacker access to Azure subscriptions in your environment.

Privileged Identity Management Alerts

Privileged Identity Management (PIM) generates alerts when there's suspicious or unsafe activity in your Microsoft Entra organization. When an alert is generated, it appears in the Privileged Identity Management dashboard. You can also configure an email notification or send to your SIEM via GraphAPI. Because these alerts focus specifically on administrative roles, you should monitor closely for any alerts.

⛶ Expand table

What to monitor	Risk Level	Where	Filter/sub-filter UX	Notes
Roles are being assigned outside of Privileged Identity Management	High	Privileged Identity Management, Alerts	Roles are being assigned outside of Privileged Identity Management	How to configure security alerts Sigma rules ⧉
Potential stale accounts in a privileged role	Medium	Privileged Identity Management, Alerts	Potential stale accounts in a privileged role	How to configure security alerts Sigma rules ⧉
Administrators aren't using their privileged roles	Low	Privileged Identity Management, Alerts	Administrators aren't using their privileged roles	How to configure security alerts Sigma rules ⧉
Roles don't require multifactor authentication for activation	Low	Privileged Identity Management, Alerts	Roles don't require multifactor authentication for activation	How to configure security alerts Sigma rules ⧉
The organization doesn't have Microsoft Entra ID P2 or Microsoft Entra ID Governance	Low	Privileged Identity Management, Alerts	The organization doesn't have Microsoft Entra ID P2 or Microsoft Entra ID Governance	How to configure security alerts Sigma rules ⧉
There are too many Global Administrators	Low	Privileged Identity Management, Alerts	There are too many Global Administrators	How to configure security alerts Sigma rules ⧉
Roles are being activated too frequently	Low	Privileged Identity Management, Alerts	Roles are being activated too frequently	How to configure security alerts Sigma rules ⧉

Microsoft Entra roles assignment

A privileged role administrator can customize PIM in their Microsoft Entra organization, which includes changing the user experience of activating an eligible role assignment:

- Prevent bad actor to remove Microsoft Entra multifactor authentication requirements to activate privileged access.

- Prevent malicious users bypass justification and approval of activating privileged access.

Download PDF

[ ] Expand table

What to monitor	Risk level	Where	Filter/sub-filter	Notes
Alert on Add changes to privileged account permissions	High	Microsoft Entra audit logs	Category = Role Management -and- Activity Type – Add eligible member (permanent) -and- Activity Type – Add eligible member (eligible) -and- Status = Success/failure -and- Modified properties = Role.DisplayName	Monitor and always alert for any changes to Privileged Role Administrator and Global Administrator. This can be an indication an attacker is trying to gain privilege to modify role assignment settings. If you don't have a defined threshold, alert on 4 in 60 minutes for users and 2 in 60 minutes for privileged accounts. Sigma rules ⧉
Alert on bulk deletion changes to privileged account permissions	High	Microsoft Entra audit logs	Category = Role Management -and- Activity Type – Remove eligible member (permanent) -and- Activity Type – Remove eligible member (eligible) -and- Status = Success/failure -and- Modified properties = Role.DisplayName	Investigate immediately if not a planned change. This setting could enable an attacker access to Azure subscriptions in your environment. Microsoft Sentinel template ⧉ Sigma rules ⧉
Changes to PIM settings	High	Microsoft Entra audit log	Service = PIM -and- Category = Role Management -and- Activity Type = Update role setting in PIM -and- Status Reason = MFA on activation disabled (example)	Monitor and always alert for any changes to Privileged Role Administrator and Global Administrator. This can be an indication an attacker has access to modify role assignment settings. One of these actions could reduce the security of the PIM elevation and make it easier for attackers to acquire a privileged account. Microsoft Sentinel template ⧉ Sigma rules ⧉
Approvals and deny elevation	High	Microsoft Entra audit log	Service = Access Review -and- Category = UserManagement -and- Activity Type = Request Approved/Denied -and- Initiated actor = UPN	All elevations should be monitored. Log all elevations to give a clear indication of timeline for an attack. Microsoft Sentinel template ⧉ Sigma rules ⧉
Alert setting changes to disabled.	High	Microsoft Entra audit logs	Service =PIM -and- Category = Role Management -and- Activity Type = Disable PIM Alert -and- Status = Success /Failure	Always alert. Helps detect bad actor removing alerts associated with Microsoft Entra multifactor authentication requirements to activate privileged access. Helps detect suspicious or unsafe activity. Microsoft Sentinel template ⧉ Sigma rules ⧉

For more information on identifying role setting changes in the Microsoft Entra audit log, see View audit history for Microsoft Entra roles in Privileged Identity Management.

Azure resource role assignment

Monitoring Azure resource role assignments allows visibility into activity and activations for resources roles. These assignments might be misused to create an attack surface to a resource. As you monitor for this type of activity, you're trying to detect:

- Query role assignments at specific resources

- Role assignments for all child resources

- All active and eligible role assignment changes

⌖ Expand table

What to monitor	Risk level	Where	Filter/sub-filter	Notes
Audit Alert Resource Audit log for Privileged account activities	High	In PIM, under Azure Resources, Resource Audit	Action: Add eligible member to role in PIM completed (time bound) -and- Primary Target -and- Type User -and- Status = Succeeded	Always alert. Helps detect bad actor adding eligible roles to manage all resources in Azure.
Audit Alert Resource Audit for Disable Alert	Medium	In PIM, under Azure Resources, Resource Audit	Action: Disable Alert -and- Primary Target: Too many owners assigned to a resource -and- Status = Succeeded	Helps detect bad actor disabling alerts, in the Alerts pane, which can bypass malicious activity being investigated
Audit Alert Resource Audit for Disable Alert	Medium	In PIM, under Azure Resources, Resource Audit	Action: Disable Alert -and- Primary Target: Too many permanent owners assigned to a resource -and- Status = Succeeded	Prevent bad actor from disable alerts, in the Alerts pane, which can bypass malicious activity being investigated
Audit Alert Resource Audit for Disable Alert	Medium	In PIM, under Azure Resources, Resource Audit	Action: Disable Alert -and- Primary Target Duplicate role created -and- Status = Succeeded	Prevent bad actor from disable alerts, from the Alerts pane, which can bypass malicious activity being investigated

For more information on configuring alerts and auditing Azure resource roles, see:

- [Configure security alerts for Azure resource roles in Privileged Identity Management](#)

- [View audit report for Azure resource roles in Privileged Identity Management (PIM)](#)

Access management for Azure resources and subscriptions

Users or group members assigned the Owner or User Access Administrator subscriptions roles, and Microsoft Entra Global Administrators who enabled subscription management in Microsoft Entra ID, have Resource Administrator permissions by default. The administrators assign roles, configure role settings, and review access using Privileged Identity Management (PIM) for Azure resources.

A user who has Resource administrator permissions can manage PIM for Resources. Monitor for and mitigate this introduced risk: the capability can be used to allow bad actors privileged access to Azure subscription resources, such as virtual machines (VMs) or storage accounts.

⌖ Expand table

Microsoft Entra security operations for Privileged Identity Management - Microsoft Entra | Microsoft Learn - 02/11/2024 09:35

https://learn.microsoft.com/en-us/entra/architecture/security-operations-privileged-identity-management#azure-ad-roles-assignment

What to monitor	Risk level	Where	Filter/sub-filter	Notes
Elevations	High	Microsoft Entra ID, under Manage, Properties	Periodically review setting. Access management for Azure resources	Global Administrators can elevate by enabling Access management for Azure resources. Verify bad actors haven't gained permissions to assign roles in all Azure subscriptions and management groups associated with Active Directory.

For more information, see Assign Azure resource roles in Privileged Identity Management

Next steps

Microsoft Entra security operations overview

Security operations for user accounts

Security operations for consumer accounts

Security operations for privileged accounts

Security operations for applications

Security operations for devices

Security operations for infrastructure

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.