# Security operations for privileged accounts in Microsoft Entra ID

Article • 23/10/2023 • 7 contributors

Feedback

## In this article



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

Traditionally, organizational security has focused on the entry and exit points of a network as the security perimeter. However, software as a service (SaaS) applications and personal devices on the internet have made this approach less effective.

Microsoft Entra ID uses identity and access management (IAM) as the control plane. In your organization's identity layer, users assigned to privileged administrative roles are in control. The accounts used for access must be protected, whether the environment is on-premises, in the cloud, or a hybrid environment.

You're entirely responsible for all layers of security for your on-premises IT environment. When you use Azure services, prevention and response are the 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, see Privileged Identity Management documentation.

# Log files to monitor

The log files you use for investigation and monitoring are:

- Microsoft Entra audit logs
- Microsoft 365 Audit logs
- Azure Key Vault insights

From the Azure portal, you can view the Microsoft Entra audit logs and download 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 that allow for greater automation of 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 have added a link to the Sigma repo. The Sigma templates are not 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. Enables Microsoft Entra logs to be pushed to other SIEMs such as Splunk, ArcSight, QRadar, and Sumo Logic via the Azure Event Hubs integration. For more information, see Stream Microsoft Entra logs to an Azure event hub.
- **Microsoft Defender for Cloud Apps**. Enables you to discover and manage apps, govern across apps and resources, and check your cloud apps' compliance.
- **Microsoft Graph**. Enables you to export data and use Microsoft Graph to do more analysis. For more information, see Microsoft Graph PowerShell SDK and Microsoft Entra ID Protection.
- **Microsoft Entra ID Protection**. Generates three key reports you can use to help with your investigation:
  - **Risky users**. Contains information about which users are at risk, details about detections, history of all risky sign-ins, and risk history.
  - **Risky sign-ins**. Contains information about a sign-in that might indicate suspicious circumstances. For more information on investigating information from this report, see

Investigate risk.

  - **Risk detections**. Contains information about other risks triggered when a risk is detected and other pertinent information such as sign-in location and any details from Microsoft Defender for Cloud Apps.

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

Although we discourage the practice, privileged accounts can have standing administration rights. If you choose to use standing privileges, and the account is compromised, it can have a strongly negative effect. We recommend you prioritize monitoring privileged accounts and include the accounts in your Privileged Identity Management (PIM) configuration. For more information on PIM, see Start using Privileged Identity Management. Also, we recommend you validate that admin accounts:

- Are required.
- Have the least privilege to execute the require activities.
- Are protected with multifactor authentication at a minimum.
- Are run from privileged access workstation (PAW) or secure admin workstation (SAW) devices.

The rest of this article describes what we recommend you monitor and alert on. The article is organized by the type of threat. Where there are specific prebuilt solutions, we link to them following the table. Otherwise, you can build alerts by using the tools described above.

This article provides details on setting baselines and auditing sign-in and usage of privileged accounts. It also discusses tools and resources you can use to help maintain the integrity of your privileged accounts. The content is organized into the following subjects:

- Emergency "break-glass" accounts
- Privileged account sign-in
- Privileged account changes
- Privileged groups
- Privilege assignment and elevation

# Emergency access accounts

It's important that you prevent being accidentally locked out of your Microsoft Entra tenant.

Microsoft recommends that organizations have two cloud-only emergency access accounts permanently assigned the Global Administrator role. These accounts are highly privileged and aren't assigned to specific individuals. The accounts are limited to emergency or "break glass" scenarios where normal accounts can't be used or all other administrators are accidentally locked out. These accounts should be created following the emergency access account recommendations.

Send a high-priority alert every time an emergency access account is used.

## Discovery

Because break-glass accounts are only used if there's an emergency, your monitoring should discover no account activity. Send a high-priority alert every time an emergency access account is used or changed. Any of the following events might indicate a bad actor is trying to compromise your environments:

- Sign-in.
- Account password change.
- Account permission or roles changed.
- Credential or auth method added or changed.

For more information on managing emergency access accounts, see Manage emergency access admin accounts in Microsoft Entra ID. For detailed information on creating an alert for an emergency account, see Create an alert rule.

# Privileged account sign-in

Monitor all privileged account sign-in activity by using the Microsoft Entra sign-in logs as the data source. In addition to sign-in success and failure information, the logs contain the following details:

- Interrupts
- Device
- Location
- Risk
- Application
- Date and time
- Is the account disabled
- Lockout
- MFA fraud
- Conditional Access failure

## Things to monitor

You can monitor privileged account sign-in events in the Microsoft Entra sign-in logs. Alert on and investigate the following events for privileged accounts.

Expand table

| What to monitor | Risk level | Where | Filter/subfilter | Notes |
|---|---|---|---|---|
| Sign-in failure, bad password threshold | High | Microsoft Entra sign-in log | Status = Failure<br>-and-<br>error code = 50126 | Define a baseline threshold and then monitor and adjust to suit your organizational behaviors and limit false alerts from being generated.<br>Microsoft Sentinel template<br><br>Sigma rules |

| | | | | |
|---|---|---|---|---|
| Failure because of Conditional Access requirement | High | Microsoft Entra sign-in log | Status = Failure<br>-and-<br>error code = 53003<br>-and-<br>Failure reason = Blocked by Conditional Access | This event can be an indication an attacker is trying to get into the account.<br>Microsoft Sentinel template<br><br>Sigma rules |
| Privileged accounts that don't follow naming policy | | Azure subscription | List Azure role assignments using the Azure portal | List role assignments for subscriptions and alert where the sign-in name doesn't match your organization's format. An example is the use of ADM_ as a prefix. |
| Interrupt | High, medium | Microsoft Entra Sign-ins | Status = Interrupted<br>-and-<br>error code = 50074<br>-and-<br>Failure reason = Strong auth required<br>Status = Interrupted<br>-and-<br>Error code = 500121<br>Failure reason = Authentication failed during strong authentication request | This event can be an indication an attacker has the password for the account but can't pass the multi-factor authentication challenge.<br>Microsoft Sentinel template<br><br>Sigma rules |
| Privileged accounts that don't follow naming policy | High | Microsoft Entra directory | List Microsoft Entra role assignments | List role assignments for Microsoft Entra roles and alert where the UPN doesn't match your organization's format. An example is the use of ADM_ as a prefix. |
| Discover privileged accounts not registered for multi-factor authentication | High | Microsoft Graph API | Query for IsMFARegistered eq false for admin accounts. List credentialUserRegistrationDetails - Microsoft Graph beta | Audit and investigate to determine if the event is intentional or an oversight. |
| Account lockout | High | Microsoft Entra sign-in log | Status = Failure<br>-and-<br>error code = 50053 | Define a baseline threshold, and then monitor and adjust to suit your organizational behaviors and limit false alerts from being generated.<br>Microsoft Sentinel template<br><br>Sigma rules |

| | | | | |
|---|---|---|---|---|
| Account disabled or blocked for sign-ins | Low | Microsoft Entra sign-in log | Status = Failure<br>-and-<br>Target = User UPN<br>-and-<br>error code = 50057 | This event could indicate someone is trying to gain access to an account after they've left the organization. Although the account is blocked, it's still important to log and alert on this activity.<br>Microsoft Sentinel template<br><br>Sigma rules |
| MFA fraud alert or block | High | Microsoft Entra sign-in log/Azure Log Analytics | Sign-ins>Authentication details<br>Result details = MFA denied, fraud code entered | Privileged user has indicated they haven't instigated the multi-factor authentication prompt, which could indicate an attacker has the password for the account.<br>Microsoft Sentinel template<br><br>Sigma rules |
| MFA fraud alert or block | High | Microsoft Entra audit log log/Azure Log Analytics | Activity type = Fraud reported - User is blocked for MFA or fraud reported - No action taken (based on tenant-level settings for fraud report) | Privileged user has indicated they haven't instigated the multi-factor authentication prompt, which could indicate an attacker has the password for the account.<br>Microsoft Sentinel template<br><br>Sigma rules |
| Privileged account sign-ins outside of expected controls | | Microsoft Entra sign-in log | Status = Failure<br>UserPricipalName = <Admin account><br>Location = <unapproved location><br>IP address = <unapproved IP><br>Device info = <unapproved Browser, Operating System> | Monitor and alert on any entries that you've defined as unapproved.<br>Microsoft Sentinel template<br><br>Sigma rules |
| Outside of normal sign-in times | High | Microsoft Entra sign-in log | Status = Success<br>-and-<br>Location =<br>-and-<br>Time = Outside of working hours | Monitor and alert if sign-ins occur outside of expected times. It's important to find the normal working pattern for each privileged account and to alert if there are unplanned changes outside of normal working times. Sign-ins outside of |

| | | | | |
|---|---|---|---|---|
| | | | | normal working hours could indicate compromise or possible insider threats. Microsoft Sentinel template<br><br>Sigma rules |
| Microsoft Entra ID Protection risk | High | ID Protection logs | Risk state = At risk<br>-and-<br>Risk level = Low, medium, high<br>-and-<br>Activity = Unfamiliar sign-in/TOR, and so on | This event indicates there's some abnormality detected with the sign-in for the account and should be alerted on. |
| Password change | High | Microsoft Entra audit logs | Activity actor = Admin/self-service<br>-and-<br>Target = User<br>-and-<br>Status = Success or failure | Alert when any administrator account password changes. Write a query for privileged accounts. Microsoft Sentinel template<br><br>Sigma rules |
| Change in legacy authentication protocol | High | Microsoft Entra sign-in log | Client App = Other client, IMAP, POP3, MAPI, SMTP, and so on<br>-and-<br>Username = UPN<br>-and-<br>Application = Exchange (example) | Many attacks use legacy authentication, so if there's a change in auth protocol for the user, it could be an indication of an attack. Microsoft Sentinel template<br><br>Sigma rules |
| New device or location | High | Microsoft Entra sign-in log | Device info = Device ID<br>-and-<br>Browser<br>-and-<br>OS<br>-and-<br>Compliant/Managed<br>-and-<br>Target = User<br>-and-<br>Location | Most admin activity should be from privileged access devices, from a limited number of locations. For this reason, alert on new devices or locations. Microsoft Sentinel template<br><br>Sigma rules |
| Audit alert setting is changed | High | Microsoft Entra audit logs | Service = PIM<br>-and-<br>Category = Role management<br>-and-<br>Activity = Disable PIM alert<br>-and-<br>Status = Success | Changes to a core alert should be alerted if unexpected. Microsoft Sentinel template<br><br>Sigma rules |
| Administrators authenticating | Medium | Microsoft Entra sign-in | Status = success | When scoped to Privileged Users, this |

| | | | | |
|---|---|---|---|---|
| to other Microsoft Entra tenants | | log | Resource tenantID != Home Tenant ID | monitor detects when an administrator has successfully authenticated to another Microsoft Entra tenant with an identity in your organization's tenant.<br><br>Alert if Resource TenantID isn't equal to Home Tenant ID<br>Microsoft Sentinel template<br><br>Sigma rules |
| Admin User state changed from Guest to Member | Medium | Microsoft Entra audit logs | Activity: Update user<br><br>Category: UserManagement<br><br>UserType changed from Guest to Member | Monitor and alert on change of user type from Guest to Member.<br><br>Was this change expected?<br>Microsoft Sentinel template<br><br>Sigma rules |
| Guest users invited to tenant by non-approved inviters | Medium | Microsoft Entra audit logs | Activity: Invite external user<br><br>Category: UserManagement<br><br>Initiated by (actor): User Principal Name | Monitor and alert on non-approved actors inviting external users.<br>Microsoft Sentinel template<br><br>Sigma rules |

# Changes by privileged accounts

Monitor all completed and attempted changes by a privileged account. This data enables you to establish what's normal activity for each privileged account and alert on activity that deviates from the expected. The Microsoft Entra audit logs are used to record this type of event. For more information on Microsoft Entra audit logs, see Audit logs in Microsoft Entra ID.

## Microsoft Entra Domain Services

Privileged accounts that have been assigned permissions in Microsoft Entra Domain Services can perform tasks for Microsoft Entra Domain Services that affect the security posture of your Azure-hosted virtual machines that use Microsoft Entra Domain Services. Enable security audits on virtual machines and monitor the logs. For more information on enabling Microsoft Entra Domain Services audits and for a list of sensitive privileges, see the following resources:

- Enable security audits for Microsoft Entra Domain Services
- Audit Sensitive Privilege Use

Expand table

| What to monitor | Risk level | Where | Filter/subfilter | Notes |
|---|---|---|---|---|
| Attempted and completed changes | High | Microsoft Entra audit logs | Date and time<br>-and-<br>Service<br>-and-<br>Category and name of the activity (what)<br>-and-<br>Status = Success or failure<br>-and-<br>Target<br>-and-<br>Initiator or actor (who) | Any unplanned changes should be alerted on immediately. These logs should be retained to help with any investigation. Any tenant-level changes should be investigated immediately (link out to Infra doc) that would lower the security posture of your tenant. An example is excluding accounts from multifactor authentication or Conditional Access. Alert on any additions or changes to applications. See Microsoft Entra security operations guide for Applications. |
| **Example**<br>Attempted or completed change to high-value apps or services | High | Audit log | Service<br>-and-<br>Category and name of the activity | Date and time, Service, Category and name of the activity, Status = Success or failure, Target, Initiator or actor (who) |
| Privileged changes in Microsoft Entra Domain Services | High | Microsoft Entra Domain Services | Look for event 4673 | Enable security audits for Microsoft Entra Domain Services<br>For a list of all privileged events, see Audit Sensitive Privilege use. |

# Changes to privileged accounts

Investigate changes to privileged accounts' authentication rules and privileges, especially if the change provides greater privilege or the ability to perform tasks in your Microsoft Entra environment.

Expand table

| What to monitor | Risk level | Where | Filter/subfilter | Notes |
|---|---|---|---|---|
| Privileged account creation | Medium | Microsoft Entra audit logs | Service = Core Directory<br>-and-<br>Category = User management<br>-and-<br>Activity type = Add user<br>-correlate with-<br>Category type = Role | Monitor creation of any privileged accounts. Look for correlation that's of a short time span between creation and deletion of accounts.<br>Microsoft Sentinel template<br><br>Sigma rules |

| | | | | |
|---|---|---|---|---|
| | | | management<br>-and-<br>Activity type = Add member to role<br>-and-<br>Modified properties = Role.DisplayName | |
| Changes to authentication methods | High | Microsoft Entra audit logs | Service = Authentication Method<br>-and-<br>Activity type = User registered security information<br>-and-<br>Category = User management | This change could be an indication of an attacker adding an auth method to the account so they can have continued access.<br>Microsoft Sentinel template<br><br>Sigma rules |
| Alert on changes to privileged account permissions | High | Microsoft Entra audit logs | Category = Role management<br>-and-<br>Activity type = Add eligible member (permanent)<br>-or-<br>Activity type = Add eligible member (eligible)<br>-and-<br>Status = Success or failure<br>-and-<br>Modified properties = Role.DisplayName | This alert is especially for accounts being assigned roles that aren't known or are outside of their normal responsibilities.<br><br>Sigma rules |
| Unused privileged accounts | Medium | Microsoft Entra access reviews | | Perform a monthly review for inactive privileged user accounts.<br>Sigma rules |
| Accounts exempt from Conditional Access | High | Azure Monitor Logs<br>-or-<br>Access Reviews | Conditional Access = Insights and reporting | Any account exempt from Conditional Access is most likely bypassing security controls and is more vulnerable to compromise. Break-glass accounts are exempt. See information on how to monitor break-glass accounts later in this article. |
| Addition of a Temporary Access Pass to a privileged account | High | Microsoft Entra audit logs | Activity: Admin registered security info<br><br>Status Reason: Admin registered temporary access pass method for user<br><br>Category: UserManagement | Monitor and alert on a Temporary Access Pass being created for a privileged user.<br>Microsoft Sentinel template<br><br>Sigma rules |

| | |
|---|---|
| | Initiated by (actor):<br>User Principal Name<br><br>Target: User Principal Name |

For more information on how to monitor for exceptions to Conditional Access policies, see Conditional Access insights and reporting.

For more information on discovering unused privileged accounts, see Create an access review of Microsoft Entra roles in Privileged Identity Management.

# Assignment and elevation

Having privileged accounts that are permanently provisioned with elevated abilities can increase the attack surface and risk to your security boundary. Instead, employ just-in-time access by using an elevation procedure. This type of system allows you to assign eligibility for privileged roles. Admins elevate their privileges to those roles only when they perform tasks that need those privileges. Using an elevation process enables you to monitor elevations and non-use of privileged accounts.

## Establish a baseline

To monitor for exceptions, you must first create a baseline. Determine the following information for these elements

- **Admin accounts**
  - Your privileged account strategy
  - Use of on-premises accounts to administer on-premises resources
  - Use of cloud-based accounts to administer cloud-based resources
  - Approach to separating and monitoring administrative permissions for on-premises and cloud-based resources
- **Privileged role protection**
  - Protection strategy for roles that have administrative privileges
  - Organizational policy for using privileged accounts
  - Strategy and principles for maintaining permanent privilege versus providing time-bound and approved access

The following concepts and information help determine policies:

- **Just-in-time admin principles**. Use the Microsoft Entra logs to capture information for performing administrative tasks that are common in your environment. Determine the typical amount of time needed to complete the tasks.
- **Just-enough admin principles**. Determine the least-privileged role, which might be a custom role, that's needed for administrative tasks. For more information, see Least privileged roles by task in Microsoft Entra ID.
- **Establish an elevation policy**. After you have insight into the type of elevated privilege needed and how long is needed for each task, create policies that reflect elevated privileged

usage for your environment. As an example, define a policy to limit role elevation to one hour.

After you establish your baseline and set policy, you can configure monitoring to detect and alert usage outside of policy.

## Discovery

Pay particular attention to and investigate changes in assignment and elevation of privilege.

## Things to monitor

You can monitor privileged account changes by using Microsoft Entra audit logs and Azure Monitor logs. Include the following changes in your monitoring process.

Expand table

| What to monitor | Risk level | Where | Filter/subfilter | Notes |
|---|---|---|---|---|
| Added to eligible privileged role | High | Microsoft Entra audit logs | Service = PIM<br>-and-<br>Category = Role management<br>-and-<br>Activity type = Add member to role completed (eligible)<br>-and-<br>Status = Success or failure<br>-and-<br>Modified properties = Role.DisplayName | Any account eligible for a role is now being given privileged access. If the assignment is unexpected or into a role that isn't the responsibility of the account holder, investigate.<br>Microsoft Sentinel template<br><br>Sigma rules |
| Roles assigned out of PIM | High | Microsoft Entra audit logs | Service = PIM<br>-and-<br>Category = Role management<br>-and-<br>Activity type = Add member to role (permanent)<br>-and-<br>Status = Success or failure<br>-and-<br>Modified properties = Role.DisplayName | These roles should be closely monitored and alerted. Users shouldn't be assigned roles outside of PIM where possible.<br>Microsoft Sentinel template<br><br>Sigma rules |
| Elevations | Medium | Microsoft Entra audit logs | Service = PIM<br>-and-<br>Category = Role management<br>-and-<br>Activity type = Add member to role | After a privileged account is elevated, it can now make changes that could affect the security of your tenant. All elevations should be logged and, if happening outside of the standard pattern for that user, should be |

| | | | | |
|---|---|---|---|---|
| | | | completed (PIM activation)<br>-and-<br>Status = Success or failure<br>-and-<br>Modified properties = Role.DisplayName | alerted and investigated if not planned. |
| Approvals and deny elevation | Low | Microsoft Entra audit logs | Service = Access Review<br>-and-<br>Category = UserManagement<br>-and-<br>Activity type = Request approved or denied<br>-and-<br>Initiated actor = UPN | Monitor all elevations because it could give a clear indication of the timeline for an attack.<br>Microsoft Sentinel template<br><br>Sigma rules |
| Changes to PIM settings | High | Microsoft Entra audit logs | Service = PIM<br>-and-<br>Category = Role management<br>-and-<br>Activity type = Update role setting in PIM<br>-and-<br>Status reason = MFA on activation disabled (example) | One of these actions could reduce the security of the PIM elevation and make it easier for attackers to acquire a privileged account.<br>Microsoft Sentinel template<br><br>Sigma rules |
| Elevation not occurring on SAW/PAW | High | Microsoft Entra sign-in logs | Device ID<br>-and-<br>Browser<br>-and-<br>OS<br>-and-<br>Compliant/Managed<br>Correlate with:<br>Service = PIM<br>-and-<br>Category = Role management<br>-and-<br>Activity type = Add member to role completed (PIM activation)<br>-and-<br>Status = Success or failure<br>-and-<br>Modified properties = Role.DisplayName | If this change is configured, any attempt to elevate on a non-PAW/SAW device should be investigated immediately because it could indicate an attacker is trying to use the account.<br>Sigma rules |
| Elevation to manage all Azure subscriptions | High | Azure Monitor | Activity Log tab<br>Directory Activity tab<br>Operations Name = Assigns the caller to user | This change should be investigated immediately if it isn't planned. This setting could allow an attacker access |

| | | |
|---|---|---|
| | access admin<br>-and-<br>Event category = Administrative<br>-and-<br>Status = Succeeded, start, fail<br>-and-<br>Event initiated by | to Azure subscriptions in your environment. |

For more information about managing elevation, see Elevate access to manage all Azure subscriptions and management groups. For information on monitoring elevations by using information available in the Microsoft Entra logs, see Azure Activity log, which is part of the Azure Monitor documentation.

For information about configuring alerts for Azure roles, see Configure security alerts for Azure resource roles in Privileged Identity Management.

# Next steps

See these security operations guide articles:

Microsoft Entra security operations overview

Security operations for user accounts

Security operations for consumer accounts

Security operations for Privileged Identity Management

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.