Microsoft | 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

Microsoft Entra security operations for user accounts

Article • 23/10/2023 • 8 contributors

👍 Feedback

In this article

User identity is one of the most important aspects of protecting your organization and data. This article provides guidance for monitoring account creation, deletion, and account usage. The first portion covers how to monitor for unusual account creation and deletion. The second portion covers how to monitor for unusual account usage.

If you have not yet read the Microsoft Entra security operations overview, we recommend you do so before proceeding.

This article covers general user accounts. For privileged accounts, see Security operations – privileged accounts.

Define a baseline

To discover anomalous behavior, you first must define what normal and expected behavior is. Defining what expected behavior for your organization is, helps you determine when unexpected behavior occurs. The definition also helps to reduce the noise level of false positives when monitoring and alerting.

Once you define what you expect, you perform baseline monitoring to validate your expectations. With that information, you can monitor the logs for anything that falls outside of tolerances you define.

Use the Microsoft Entra audit logs, Microsoft Entra sign-in logs, and directory attributes as your data sources for accounts created outside of normal processes. The following are suggestions to help you think about and define what normal is for your organization.

- **Users account creation** – evaluate the following:

  - Strategy and principles for tools and processes used for creating and managing user accounts. For example, are there standard attributes, formats that are applied to user account attributes.

  - Approved sources for account creation. For example, originating in Active Directory (AD), Microsoft Entra ID or HR systems like Workday.

  - Alert strategy for accounts created outside of approved sources. Is there a controlled list of organizations your organization collaborates with?

  - Provisioning of guest accounts and alert parameters for accounts created outside of entitlement management or other normal processes.

  - Strategy and alert parameters for accounts created, modified, or disabled by an account that isn't an approved user administrator.

  - Monitoring and alert strategy for accounts missing standard attributes, such as employee ID or not following organizational naming conventions.

  - Strategy, principles, and process for account deletion and retention.

- **On-premises user accounts** – evaluate the following for accounts synced with Microsoft Entra Connect:

- The forests, domains, and organizational units (OUs) in scope for synchronization. Who are the approved administrators who can change these settings and how often is the scope checked?

- The types of accounts that are synchronized. For example, user accounts and or service accounts.

- The process for creating privileged on-premises accounts and how the synchronization of this type of account is controlled.

- The process for creating on-premises user accounts and how the synchronization of this type of account is managed.

For more information for securing and monitoring on-premises accounts, see Protecting Microsoft 365 from on-premises attacks.

- **Cloud user accounts** – evaluate the following:

  - The process to provision and manage cloud accounts directly in Microsoft Entra ID.

  - The process to determine the types of users provisioned as Microsoft Entra cloud accounts. For example, do you only allow privileged accounts or do you also allow user accounts?

  - The process to create and maintain a list of trusted individuals and or processes expected to create and manage cloud user accounts.

  - The process to create and maintained an alert strategy for non-approved cloud-based accounts.

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

- Risky Users log

- UserRiskEvents log

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'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.

Much of what you will monitor and alert on are the effects of your Conditional Access policies. You can use the Conditional Access insights and reporting workbook to examine the effects of one or more Conditional Access policies on your sign-ins, and the results of policies, including device state. This workbook enables you to view a summary, and identify the effects over a specific time period. You can also use the workbook to investigate the sign-ins of a specific user.

The remainder of this article describes what we recommend you monitor and alert on, and is organized by the type of threat. Where there are specific pre-built solutions we link to them or provide samples following the table. Otherwise, you can build alerts using the preceding tools.

Account creation

Anomalous account creation can indicate a security issue. Short lived accounts, accounts not following naming standards, and accounts created outside of normal processes should be investigated.

Short-lived accounts

Account creation and deletion outside of normal identity management processes should be monitored in Microsoft Entra ID. Short-lived accounts are accounts created and deleted in a short time span. This type of account creation and quick deletion could mean a bad actor is trying to avoid detection by creating accounts, using them, and then deleting the account.

Short-lived account patterns might indicate non-approved people or processes might have the right to create and delete accounts that fall outside of established processes and policies. This type of behavior removes visible markers from the directory.

If the data trail for account creation and deletion is not discovered quickly, the information required to investigate an incident may no longer exist. For example, accounts might be deleted and then purged from the recycle bin. Audit logs are retained for 30 days. However, you can export your logs to Azure Monitor or a security information and event management (SIEM) solution for longer term retention.

⌄⌃ **Expand table**

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
Account creation and deletion events within a close time frame.	High	Microsoft Entra audit logs	Activity: Add user Status = success -and- Activity: Delete user Status = success	Search for user principal name (UPN) events. Look for accounts created and then deleted in under 24 hours. Microsoft Sentinel template ↗
Accounts created and deleted by non-approved users or processes.	Medium	Microsoft Entra audit logs	Initiated by (actor) – USER PRINCIPAL NAME -and- Activity: Add user Status = success and-or Activity: Delete user Status = success	If the actors are non-approved users, configure to send an alert. Microsoft Sentinel template ↗
Accounts from non-approved sources.	Medium	Microsoft Entra audit logs	Activity: Add user Status = success Target(s) = USER PRINCIPAL NAME	If the entry isn't from an approved domain or is a known blocked domain, configure to send an alert. Microsoft Sentinel template ↗
Accounts assigned to a privileged role.	High	Microsoft Entra audit logs	Activity: Add user Status = success -and- Activity: Delete user Status = success -and- Activity: Add member to role Status = success	If the account is assigned to a Microsoft Entra role, Azure role, or privileged group membership, alert and prioritize the investigation. Microsoft Sentinel template ↗ Sigma rules ↗

Both privileged and non-privileged accounts should be monitored and alerted. However, since privileged accounts have administrative permissions, they should have higher priority in your monitor, alert, and respond processes.

Accounts not following naming policies

User accounts not following naming policies might have been created outside of organizational policies.

A best practice is to have a naming policy for user objects. Having a naming policy makes management easier and helps provide consistency. The policy can also help discover when users have been created outside of approved processes. A bad actor might not be aware of your naming standards and might make it easier to detect an account provisioned outside of your organizational processes.

Organizations tend to have specific formats and attributes that are used for creating user and or privileged accounts. For example:

- Admin account UPN = ADM_firstname.lastname@tenant.onmicrosoft.com

- User account UPN = Firstname.Lastname@contoso.com

Frequently, user accounts have an attribute that identifies a real user. For example, EMPID = XXXNNN. Use the following suggestions to help define normal for your organization, and when defining a baseline for log entries when accounts don't follow your naming convention:

- Accounts that don't follow the naming convention. For example, `nnnnnnn@contoso.com` versus `firstname.lastname@contoso.com`.

- Accounts that don't have the standard attributes populated or aren't in the correct format. For example, not having a valid employee ID.

⛶ Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
User accounts that don't have expected attributes defined.	Low	Microsoft Entra audit logs	Activity: Add user Status = success	Look for accounts with your standard attributes either null or in the wrong format. For example, EmployeeID Microsoft Sentinel template ⧉
User accounts created using incorrect naming format.	Low	Microsoft Entra audit logs	Activity: Add user Status = success	Look for accounts with a UPN that does not follow your naming policy. Microsoft Sentinel template ⧉
Privileged accounts that don't follow naming policy.	High	Azure Subscription	List Azure role assignments using the Azure portal - Azure RBAC	List role assignments for subscriptions and alert where sign-in name does not match your organizations format. For example, ADM_ as a prefix.
Privileged accounts that don't follow naming policy.	High	Microsoft Entra directory	List Microsoft Entra role assignments	List roles assignments for Microsoft Entra roles alert where UPN doesn't match your organizations format. For example, ADM_ as a prefix.

For more information on parsing, see:

- Microsoft Entra audit logs - Parse text data in Azure Monitor Logs

- Azure Subscriptions - List Azure role assignments using Azure PowerShell

- Microsoft Entra ID - List Microsoft Entra role assignments

Accounts created outside normal processes

Having standard processes to create users and privileged accounts is important so that you can securely control the lifecycle of identities. If users are provisioned and deprovisioned outside of established processes, it can introduce security risks. Operating outside of established processes can also introduce identity management problems. Potential risks include:

- User and privileged accounts might not be governed to adhere to organizational policies. This can lead to a wider attack surface on accounts that aren't managed correctly.

- It becomes harder to detect when bad actors create accounts for malicious purposes. By having valid accounts created outside of established procedures, it becomes harder to detect when accounts are created, or permissions modified for malicious purposes.

We recommend that user and privileged accounts only be created following your organization policies. For example, an account should be created with the correct naming standards, organizational information and under scope of the appropriate identity governance. Organizations should have rigorous controls for who has the rights to create, manage, and delete identities. Roles to create these accounts should be

tightly managed and the rights only available after following an established workflow to approve and obtain these permissions.

⌞⌝ **Expand table**

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
User accounts created or deleted by non-approved users or processes.	Medium	Microsoft Entra audit logs	Activity: Add user Status = success and-or- Activity: Delete user Status = success -and- Initiated by (actor) = USER PRINCIPAL NAME	Alert on accounts created by non-approved users or processes. Prioritize accounts created with heightened privileges. Microsoft Sentinel template ☒
User accounts created or deleted from non-approved sources.	Medium	Microsoft Entra audit logs	Activity: Add user Status = success -or- Activity: Delete user Status = success -and- Target(s) = USER PRINCIPAL NAME	Alert when the domain is non-approved or known blocked domain.

Unusual sign-ins

Seeing failures for user authentication is normal. But seeing patterns or blocks of failures can be an indicator that something is happening with a user's Identity. For example, during Password spray or Brute Force attacks, or when a user account is compromised. It's critical that you monitor and alert when patterns emerge. This helps ensure you can protect the user and your organization's data.

Success appears to say all is well. But it can mean that a bad actor has successfully accessed a service. Monitoring successful logins helps you detect user accounts that are gaining access but aren't user accounts that should have access. User authentication successes are normal entries in Microsoft Entra sign-in logs. We recommend you monitor and alert to detect when patterns emerge. This helps ensure you can protect user accounts and your organization's data.

As you design and operationalize a log monitoring and alerting strategy, consider the tools available to you through the Azure portal. Microsoft Entra ID Protection enables you to automate the detection, protection, and remediation of identity-based risks. ID Protection uses intelligence-fed machine learning and heuristic systems to detect risk and assign a risk score for users and sign-ins. Customers can configure policies based on a risk level for when to allow or deny access or allow the user to securely self-remediate from a risk. The following ID Protection risk detections inform risk levels today:

⌞⌝ **Expand table**

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
Leaked credentials user risk detection	High	Microsoft Entra risk detection logs	UX: Leaked credentials API: See riskDetection resource type - Microsoft Graph	See What is risk? Microsoft Entra ID Protection Sigma rules ☒
Microsoft Entra Threat Intelligence user risk detection	High	Microsoft Entra risk detection logs	UX: Microsoft Entra threat intelligence API: See riskDetection resource type - Microsoft Graph	See What is risk? Microsoft Entra ID Protection Sigma rules ☒
Anonymous IP address sign-in risk detection	Varies	Microsoft Entra risk detection logs	UX: Anonymous IP address API: See riskDetection resource type - Microsoft Graph	See What is risk? Microsoft Entra ID Protection Sigma rules ☒
Atypical travel sign-in risk detection	Varies	Microsoft Entra risk detection	UX: Atypical travel	See What is risk? Microsoft Entra ID

			logs	API: See riskDetection resource type - Microsoft Graph	Protection Sigma rules [link]
Anomalous Token	Varies	Microsoft Entra risk detection logs	UX: Anomalous Token API: See riskDetection resource type - Microsoft Graph	See What is risk? Microsoft Entra ID Protection Sigma rules [link]
Malware linked IP address sign-in risk detection	Varies	Microsoft Entra risk detection logs	UX: Malware linked IP address API: See riskDetection resource type - Microsoft Graph	See What is risk? Microsoft Entra ID Protection Sigma rules [link]
Suspicious browser sign-in risk detection	Varies	Microsoft Entra risk detection logs	UX: Suspicious browser API: See riskDetection resource type - Microsoft Graph	See What is risk? Microsoft Entra ID Protection Sigma rules [link]
Unfamiliar sign-in properties sign-in risk detection	Varies	Microsoft Entra risk detection logs	UX: Unfamiliar sign-in properties API: See riskDetection resource type - Microsoft Graph	See What is risk? Microsoft Entra ID Protection Sigma rules [link]
Malicious IP address sign-in risk detection	Varies	Microsoft Entra risk detection logs	UX: Malicious IP address API: See riskDetection resource type - Microsoft Graph	See What is risk? Microsoft Entra ID Protection Sigma rules [link]
Suspicious inbox manipulation rules sign-in risk detection	Varies	Microsoft Entra risk detection logs	UX: Suspicious inbox manipulation rules API: See riskDetection resource type - Microsoft Graph	See What is risk? Microsoft Entra ID Protection Sigma rules [link]
Password Spray sign-in risk detection	High	Microsoft Entra risk detection logs	UX: Password spray API: See riskDetection resource type - Microsoft Graph	See What is risk? Microsoft Entra ID Protection Sigma rules [link]
Impossible travel sign-in risk detection	Varies	Microsoft Entra risk detection logs	UX: Impossible travel API: See riskDetection resource type - Microsoft Graph	See What is risk? Microsoft Entra ID Protection Sigma rules [link]
New country/region sign-in risk detection	Varies	Microsoft Entra risk detection logs	UX: New country/region API: See riskDetection resource type - Microsoft Graph	See What is risk? Microsoft Entra ID Protection Sigma rules [link]
Activity from anonymous IP address sign-in risk detection	Varies	Microsoft Entra risk detection logs	UX: Activity from Anonymous IP address API: See riskDetection resource type - Microsoft Graph	See What is risk? Microsoft Entra ID Protection Sigma rules [link]
Suspicious inbox forwarding sign-in risk detection	Varies	Microsoft Entra risk detection logs	UX: Suspicious inbox forwarding API: See riskDetection resource type - Microsoft Graph	See What is risk? Microsoft Entra ID Protection Sigma rules [link]
Microsoft Entra threat intelligence sign-in risk detection	High	Microsoft Entra risk detection logs	UX: Microsoft Entra threat intelligence API: See riskDetection resource type - Microsoft Graph	See What is risk? Microsoft Entra ID Protection Sigma rules [link]

For more information, visit What is ID Protection.

What to look for

Configure monitoring on the data within the Microsoft Entra sign-in logs to ensure that alerting occurs and adheres to your organization's security policies. Some examples of this are:

- **Failed Authentications**: As humans we all get our passwords wrong from time to time. However, many failed authentications can indicate that a bad actor is trying to obtain access. Attacks differ in ferocity but can range from a few attempts per hour to a much higher rate. For example, Password Spray normally preys on easier passwords against many accounts, while Brute Force attempts many passwords against targeted accounts.

- **Interrupted Authentications**: An Interrupt in Microsoft Entra ID represents an injection of a process to satisfy authentication, such as when enforcing a control in a Conditional Access policy. This is a normal event and can happen when applications aren't configured correctly. But when you see many interrupts for a user account it could indicate something is happening with that account.
  - For example, if you filtered on a user in Sign-in logs and see a large volume of sign in status = Interrupted and Conditional Access = Failure. Digging deeper it may show in authentication details that the password is correct, but that strong authentication is required. This could mean the user isn't completing multi-factor authentication (MFA) which could indicate the user's password is compromised and the bad actor is unable to fulfill MFA.

- **Smart lock-out**: Microsoft Entra ID provides a smart lock-out service which introduces the concept of familiar and non-familiar locations to the authentication process. A user account visiting a familiar location might authenticate successfully while a bad actor unfamiliar with the same location is blocked after several attempts. Look for accounts that have been locked out and investigate further.

- **IP changes**: It is normal to see users originating from different IP addresses. However, Zero Trust states never trust and always verify. Seeing a large volume of IP addresses and failed sign-ins can be an indicator of intrusion. Look for a pattern of many failed authentications taking place from multiple IP addresses. Note, virtual private network (VPN) connections can cause false positives. Regardless of the challenges, we recommend you monitor for IP address changes and if possible, use Microsoft Entra ID Protection to automatically detect and mitigate these risks.

- **Locations**: Generally, you expect a user account to be in the same geographical location. You also expect sign-ins from locations where you have employees or business relations. When the user account comes from a different international location in less time than it would take to travel there, it can indicate the user account is being abused. Note, VPNs can cause false positives, we recommend you monitor for user accounts signing in from geographically distant locations and if possible, use Microsoft Entra ID Protection to automatically detect and mitigate these risks.

For this risk area, we recommend you monitor standard user accounts and privileged accounts but prioritize investigations of privileged accounts. Privileged accounts are the most important accounts in any Microsoft Entra tenant. For specific guidance for privileged accounts, see Security operations – privileged accounts.

How to detect

You use Microsoft Entra ID Protection and the Microsoft Entra sign-in logs to help discover threats indicated by unusual sign-in characteristics. For more information, see the article What is ID Protection. You can also replicate the data to Azure Monitor or a SIEM for monitoring and alerting purposes. To define normal for your environment and to set a baseline, determine:

- the parameters you consider normal for your user base.

- the average number of tries of a password over a time before the user calls the service desk or performs a self-service password reset.

- how many failed attempts you want to allow before alerting, and if it will be different for user accounts and privileged accounts.

- how many MFA attempts you want to allow before alerting, and if it will be different for user accounts and privileged accounts.

- if legacy authentication is enabled and your roadmap for discontinuing usage.

- the known egress IP addresses are for your organization.

- the countries/regions your users operate from.

- whether there are groups of users that remain stationary within a network location or country/region.

- Identify any other indicators for unusual sign-ins that are specific to your organization. For example days or times of the week or year that your organization doesn't operate.

After you scope what normal is for the accounts in your environment, consider the following list to help determine scenarios you want to monitor and alert on, and to fine-tune your alerting.

- Do you need to monitor and alert if Microsoft Entra ID Protection is configured?

- Are there stricter conditions applied to privileged accounts that you can use to monitor and alert on? For example, requiring privileged accounts only be used from trusted IP addresses.

- Are the baselines you set too aggressive? Having too many alerts might result in alerts being ignored or missed.

Configure ID Protection to help ensure protection is in place that supports your security baseline policies. For example, blocking users if risk = high. This risk level indicates with a high degree of confidence that a user account is compromised. For more information on setting up sign in risk policies and user risk policies, visit ID Protection policies.

The following are listed in order of importance based on the effect and severity of the entries.

Monitoring external user sign ins

⛶ Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
Users authenticating to other Microsoft Entra tenants.	Low	Microsoft Entra sign-in log	Status = success Resource tenantID != Home Tenant ID	Detects when a user has successfully authenticated to another Microsoft Entra tenant with an identity in your organization's tenant. Alert if Resource TenantID isn't equal to Home Tenant ID Microsoft Sentinel template ↗ Sigma rules ↗
User state changed from Guest to Member	Medium	Microsoft Entra audit logs	Activity: Update user Category: UserManagement UserType changed from Guest to Member	Monitor and alert on change of user type from Guest to Member. Was this expected? Microsoft Sentinel template ↗ Sigma rules ↗
Guest users invited to tenant by non-approved inviters	Medium	Microsoft Entra audit logs	Activity: Invite external user Category: UserManagement Initiated by (actor): User Principal Name	Monitor and alert on non-approved actors inviting external users. Microsoft Sentinel template ↗ Sigma rules ↗

Monitoring for failed unusual sign ins

⛶ Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
Failed sign-in attempts.	Medium - if Isolated Incident High - if many accounts are experiencing the same pattern or a VIP.	Microsoft Entra sign-in log	Status = failed -and- Sign-in error code 50126 - Error validating credentials due to invalid username or password.	Define a baseline threshold, and then monitor and adjust to suit your organizational behaviors and limit false alerts from being generated. Microsoft Sentinel template ↗ Sigma rules ↗

| Smart lock-out events. | Medium - if Isolated Incident High - if many accounts are experiencing the same pattern or a VIP. | Microsoft Entra sign-in log | Status = failed -and- Sign-in error code = 50053 – IdsLocked | Define a baseline threshold, and then monitor and adjust to suit your organizational behaviors and limit false alerts from being generated. Microsoft Sentinel template ↗ Sigma rules ↗ |
| Interrupts | Medium - if Isolated Incident High - if many accounts are experiencing the same pattern or a VIP. | Microsoft Entra sign-in log | 500121, Authentication failed during strong authentication request. -or- 50097, Device authentication is required or 50074, Strong Authentication is required. -or- 50155, DeviceAuthenticationFailed -or- 50158, ExternalSecurityChallenge - External security challenge wasn't satisfied -or- 53003 and Failure reason = blocked by Conditional Access | Monitor and alert on interrupts. Define a baseline threshold, and then monitor and adjust to suit your organizational behaviors and limit false alerts from being generated. Microsoft Sentinel template ↗ Sigma rules ↗ |

The following are listed in order of importance based on the effect and severity of the entries.

⛶ Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
Multi-factor authentication (MFA) fraud alerts.	High	Microsoft Entra sign-in log	Status = failed -and- Details = MFA Denied	Monitor and alert on any entry. Microsoft Sentinel template ↗ Sigma rules ↗
Failed authentications from countries/regions you don't operate out of.	Medium	Microsoft Entra sign-in log	Location = <unapproved location>	Monitor and alert on any entries. Microsoft Sentinel template ↗ Sigma rules ↗
Failed authentications for legacy protocols or protocols that aren't used.	Medium	Microsoft Entra sign-in log	Status = failure -and- Client app = Other Clients, POP, IMAP, MAPI, SMTP, ActiveSync	Monitor and alert on any entries. Microsoft Sentinel template ↗ Sigma rules ↗
Failures blocked by Conditional Access.	Medium	Microsoft Entra sign-in log	Error code = 53003 -and- Failure reason = blocked by Conditional Access	Monitor and alert on any entries. Microsoft Sentinel template ↗ Sigma rules ↗
Increased failed authentications of any type.	Medium	Microsoft Entra sign-in log	Capture increases in failures across the board. That is, the failure total for today is >10% on the same day, the previous week.	If you don't have a set threshold, monitor and alert if failures increase by 10% or greater. Microsoft Sentinel template ↗
Authentication occurring at times and days of the week when countries/regions don't conduct normal business operations.	Low	Microsoft Entra sign-in log	Capture interactive authentication occurring outside of normal operating days\time. Status = success -and- Location = <location> -and- Day\Time = <not normal working hours>	Monitor and alert on any entries. Microsoft Sentinel template ↗
Account disabled/blocked for sign-ins	Low	Microsoft Entra sign-in log	Status = Failure -and- error code = 50057, The user account is disabled.	This could indicate someone is trying to gain access to an account once they have left an organization. Although the account is blocked, it is

				important to log and alert on this activity. [Microsoft Sentinel template](#) [Sigma rules](#)

Monitoring for successful unusual sign ins

⛶ Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
Authentications of privileged accounts outside of expected controls.	High	Microsoft Entra sign-in log	Status = success -and- UserPricipalName = <Admin account> -and- Location = <unapproved location> -and- IP Address = <unapproved IP> Device Info= <unapproved Browser, Operating System>	Monitor and alert on successful authentication for privileged accounts outside of expected controls. Three common controls are listed. [Microsoft Sentinel template](#) [Sigma rules](#)
When only single-factor authentication is required.	Low	Microsoft Entra sign-in log	Status = success Authentication requirement = Single-factor authentication	Monitor periodically and ensure expected behavior. [Sigma rules](#)
Discover privileged accounts not registered for MFA.	High	Azure Graph API	Query for IsMFARegistered eq false for administrator accounts. [List credentialUserRegistrationDetails - Microsoft Graph beta](#)	Audit and investigate to determine if intentional or an oversight.
Successful authentications from countries/regions your organization doesn't operate out of.	Medium	Microsoft Entra sign-in log	Status = success Location = <unapproved country/region>	Monitor and alert on any entries not equal to the city names you provide. [Sigma rules](#)
Successful authentication, session blocked by Conditional Access.	Medium	Microsoft Entra sign-in log	Status = success -and- error code = 53003 – Failure reason, blocked by Conditional Access	Monitor and investigate when authentication is successful, but session is blocked by Conditional Access. [Microsoft Sentinel template](#) [Sigma rules](#)
Successful authentication after you have disabled legacy authentication.	Medium	Microsoft Entra sign-in log	status = success -and- Client app = Other Clients, POP, IMAP, MAPI, SMTP, ActiveSync	If your organization has disabled legacy authentication, monitor and alert when successful legacy authentication has taken place. [Microsoft Sentinel template](#) [Sigma rules](#)

We recommend you periodically review authentications to medium business impact (MBI) and high business impact (HBI) applications where only single-factor authentication is required. For each, you want to determine if single-factor authentication was expected or not. In addition, review for successful authentication increases or at unexpected times, based on the location.

⛶ Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
Authentications to MBI and HBI application using single-factor authentication.	Low	Microsoft Entra sign-in log	status = success -and- Application ID = <HBI app> -and- Authentication requirement = single-factor authentication.	Review and validate this configuration is intentional. [Sigma rules](#)

Authentications at days and times of the week or year that countries/regions do not conduct normal business operations.	Low	Microsoft Entra sign-in log	Capture interactive authentication occurring outside of normal operating days\time. Status = success Location = <location> Date\Time = <not normal working hours>	Monitor and alert on authentications days and times of the week or year that countries/regions do not conduct normal business operations. Sigma rules
Measurable increase of successful sign ins.	Low	Microsoft Entra sign-in log	Capture increases in successful authentication across the board. That is, success totals for today are >10% on the same day, the previous week.	If you don't have a set threshold, monitor and alert if successful authentications increase by 10% or greater. Microsoft Sentinel template Sigma rules

Next steps

See these security operations guide articles:

Microsoft Entra security operations overview

Security operations for consumer accounts

Security operations for privileged 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

Monitor and report on security events in Microsoft Entra ID - Training

Monitor Microsoft Entra security events with built-in reporting and monitoring capabilities to prevent unauthorized access and potential data loss.

Certification

Microsoft Certified: Security Operations Analyst Associate - Certifications

Investigate, search for, and mitigate threats using Microsoft Sentinel, Microsoft Defender for Cloud, and Microsoft 365 Defender.