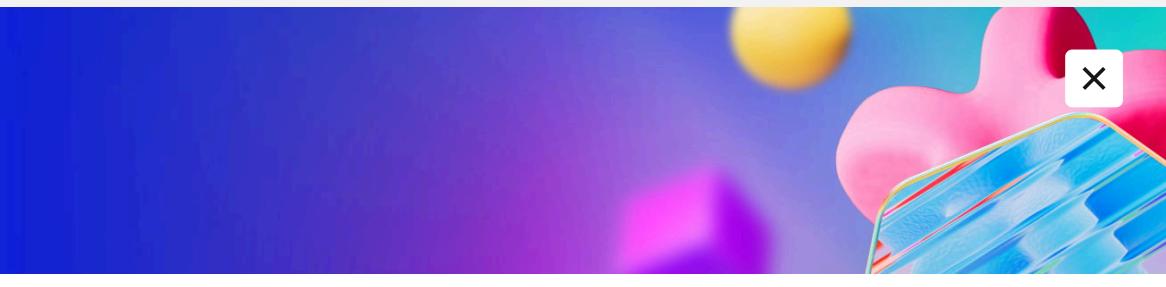
We use optional cookies to improve your experience on our websites, such as through social media connections, and to display personalized advertising based on your online activity. If you reject optional cookies, only cookies necessary to provide you the services will be used. You may change your selection 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



Microsoft Entra security operations guide for applications

Article • 10/23/2023 • 8 contributors

Feedback

In this article

Applications have an attack surface for security breaches and must be monitored. While not targeted as often as user accounts, breaches can occur. Because applications often run without human intervention, the attacks may be harder to detect.

This article provides guidance to monitor and alert on application events. It's regularly updated to help ensure you:

- Prevent malicious applications from getting unwarranted access to data
- Prevent applications from being compromised by bad actors
- Gather insights that enable you to build and configure new applications more securely

If you're unfamiliar with how applications work in Microsoft Entra ID, see Apps and service principals in Microsoft Entra ID.

> **Note**
>
> If you have not yet reviewed the **Microsoft Entra security operations overview**, consider doing so now.

What to look for

As you monitor your application logs for security incidents, review the following list to help differentiate normal activity from malicious activity. The following events might indicate security concerns. Each is covered in the article.

- Any changes occurring outside normal business processes and schedules
- Application credentials changes
- Application permissions
  - Service principal assigned to a Microsoft Entra ID or an Azure role-based access control (RBAC) role

    - Applications granted highly privileged permissions
    - Azure Key Vault changes
    - End user granting applications consent
    - Stopped end-user consent based on level of risk
- Application configuration changes
    - Universal resource identifier (URI) changed or non-standard
    - Changes to application owners
    - Log-out URLs modified

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

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, which allow more automation of monitoring and alerting:

- **Microsoft Sentinel** – enables intelligent security analytics at the enterprise level with 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 there are Sigma templates 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** – 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** – discover and manage apps, govern across apps and resources, and check your cloud apps' compliance.
- **Securing workload identities with Microsoft Entra ID Protection** - detects risk on workload identities across sign-in behavior and offline indicators of compromise.

Much of what you 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. Use the workbook to view a summary, and identify the effects over a time period. You can use the workbook to investigate the sign-ins of a specific user.

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

Application credentials

Many applications use credentials to authenticate in Microsoft Entra ID. Any other credentials added outside expected processes could be a malicious actor using those credentials. We recommend using X509 certificates issued by trusted authorities or Managed Identities instead of using client secrets. However, if you need to use client secrets, follow good hygiene practices to keep applications safe. Note, application and service principal updates are logged as two entries in the audit log.

- Monitor applications to identify long credential expiration times.
- Replace long-lived credentials with a short life span. Ensure credentials don't get committed in code repositories, and are stored securely.

Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
Added credentials to existing applications	High	Microsoft Entra audit logs	Service-Core Directory, Category-ApplicationManagement Activity: Update Application-Certificates and secrets management -and- Activity: Update Service principal/Update Application	Alert when credentials are: added outside of normal business hours or workflows, of types not used in your environment, or added to a non-SAML flow supporting service principal. Microsoft Sentinel template Sigma rules
Credentials with a lifetime longer than your policies allow.	Medium	Microsoft Graph	State and end date of Application Key credentials -and- Application password credentials	You can use MS Graph API to find the start and end date of credentials, and evaluate longer-than-allowed lifetimes. See PowerShell script following this table.

The following pre-built monitoring and alerts are available:

- Microsoft Sentinel – Alert when new app or service principle credentials added
- Azure Monitor – Microsoft Entra workbook to help you assess Solorigate risk - Microsoft Tech Community
- Defender for Cloud Apps – Defender for Cloud Apps anomaly detection alerts investigation guide
- PowerShell - Sample PowerShell script to find credential lifetime .

Application permissions

Like an administrator account, applications can be assigned privileged roles. Apps can be assigned any Microsoft Entra roles, such as User Administrator, or Azure RBAC roles such as Billing Reader. Because they can run without a user, and as a background service, closely monitor when an application is granted privileged roles or permissions.

Service principal assigned to a role

Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
App assigned to Azure RBAC role, or Microsoft Entra role	High to Medium	Microsoft Entra audit logs	Type: service principal Activity: "Add member to role" or "Add eligible member to role" -or- "Add scoped member to role."	For highly privileged roles risk is high. For lower privileged roles risk is medium. Alert anytime an application is assigned to an Azure role or Microsoft Entra role outside of normal change management or configuration procedures. Microsoft Sentinel template Sigma rules

Application granted highly privileged permissions

Applications should follow the principle of least privilege. Investigate application permissions to ensure they're needed. You can create an app consent grant report to help identify applications and highlight privileged permissions.

Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes

App granted highly privileged permissions, such as permissions with *".All" (Directory.ReadWrite.All) or wide ranging permissions (Mail.)*	High	Microsoft Entra audit logs	"Add app role assignment to service principal", - where- Target(s) identifies an API with sensitive data (such as Microsoft Graph) -and- AppRole.Value identifies a highly privileged application permission (app role).	Apps granted broad permissions such as *".All" (Directory.ReadWrite.All) or wide ranging permissions (Mail.)* Microsoft Sentinel template Sigma rules
Administrator granting either application permissions (app roles) or highly privileged delegated permissions	High	Microsoft 365 portal	"Add app role assignment to service principal", -where- Target(s) identifies an API with sensitive data (such as Microsoft Graph) "Add delegated permission grant", -where- Target(s) identifies an API with sensitive data (such as Microsoft Graph) -and- DelegatedPermissionGrant.Scope includes high-privilege permissions.	Alert when an administrator consents to an application. Especially look for consent outside of normal activity and change procedures. Microsoft Sentinel template Microsoft Sentinel template Microsoft Sentinel template Sigma rules
Application is granted permissions for Microsoft Graph, Exchange, SharePoint, or Microsoft Entra ID.	High	Microsoft Entra audit logs	"Add delegated permission grant" -or- "Add app role assignment to service principal", -where- Target(s) identifies an API with sensitive data (such as Microsoft Graph, Exchange Online, and so on)	Alert as in the preceding row. Microsoft Sentinel template Sigma rules
Application permissions (app roles) for other APIs are granted	Medium	Microsoft Entra audit logs	"Add app role assignment to service principal", -where- Target(s) identifies any other API.	Alert as in the preceding row. Sigma rules
Highly privileged delegated permissions are granted on behalf of all users	High	Microsoft Entra audit logs	"Add delegated permission grant", where Target(s) identifies an API with sensitive data (such as Microsoft Graph), DelegatedPermissionGrant.Scope includes high-privilege permissions, -and- DelegatedPermissionGrant.ConsentType is "AllPrincipals".	Alert as in the preceding row. Microsoft Sentinel template Microsoft Sentinel template Microsoft Sentinel template Sigma rules

For more information on monitoring app permissions, see this tutorial: Investigate and remediate risky OAuth apps.

Azure Key Vault

Use Azure Key Vault to store your tenant's secrets. We recommend you pay attention to any changes to Key Vault configuration and activities.

Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
How and when your Key Vaults are accessed and by whom	Medium	Azure Key Vault logs	Resource type: Key Vaults	Look for: any access to Key Vault outside regular processes and hours, any changes to Key Vault ACL. Microsoft Sentinel template Sigma rules

After you set up Azure Key Vault, enable logging. See how and when your Key Vaults are accessed, and configure alerts on Key Vault to notify assigned users or distribution lists via email, phone, text, or Event Grid notification, if health is affected. In addition, setting up monitoring with Key Vault insights gives you a

snapshot of Key Vault requests, performance, failures, and latency. Log Analytics also has some example queries for Azure Key Vault that can be accessed after selecting your Key Vault and then under "Monitoring" selecting "Logs".

End-user consent

Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
End-user consent to application	Low	Microsoft Entra audit logs	Activity: Consent to application / ConsentContext.IsAdminConsent = false	Look for: high profile or highly privileged accounts, app requests high-risk permissions, apps with suspicious names, for example generic, misspelled, and so on. Microsoft Sentinel template Sigma rules

The act of consenting to an application isn't malicious. However, investigate new end-user consent grants looking for suspicious applications. You can restrict user consent operations.

For more information on consent operations, see the following resources:

- Managing consent to applications and evaluating consent requests in Microsoft Entra ID
- Detect and Remediate Illicit Consent Grants - Office 365
- Incident response playbook - App consent grant investigation

End user stopped due to risk-based consent

Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
End-user consent stopped due to risk-based consent	Medium	Microsoft Entra audit logs	Core Directory / ApplicationManagement / Consent to application Failure status reason = Microsoft.online.Security.userConsent BlockedForRiskyAppsExceptions	Monitor and analyze any time consent is stopped due to risk. Look for: high profile or highly privileged accounts, app requests high-risk permissions, or apps with suspicious names, for example generic, misspelled, and so on. Microsoft Sentinel template Sigma rules

Application authentication flows

There are several flows in the OAuth 2.0 protocol. The recommended flow for an application depends on the type of application being built. In some cases, there's a choice of flows available to the application. For this case, some authentication flows are recommended over others. Specifically, avoid resource owner password credentials (ROPC) because these require the user to expose their current password credentials to the application. The application then uses the credentials to authenticate the user against the identity provider. Most applications should use the auth code flow, or auth code flow with Proof Key for Code Exchange (PKCE), because this flow is recommended.

The only scenario where ROPC is suggested is for automated application testing. See Run automated integration tests for details.

Device code flow is another OAuth 2.0 protocol flow for input-constrained devices and isn't used in all environments. When device code flow appears in the environment, and isn't used in an input constrained device scenario. More investigation is warranted for a misconfigured application or potentially something malicious. Device code flow can also be blocked or allowed in Conditional Access. See Conditional Access authentication flows for details.

Monitor application authentication using the following formation:

Download PDF

Expand table

What to monitor	Risk level	Where	Filter/sub-filter	Notes
Applications that are using the ROPC authentication flow	Medium	Microsoft Entra sign-in log	Status=Success Authentication Protocol-ROPC	High level of trust is being placed in this application as the credentials can be cached or stored. Move if possible to a more secure authentication flow. This should only be used in automated testing of applications, if at all. For more information, see Microsoft identity platform and OAuth 2.0 Resource Owner Password Credentials Sigma rules
Applications using the Device code flow	Low to medium	Microsoft Entra sign-in log	Status=Success Authentication Protocol-Device Code	Device code flows are used for input constrained devices, which may not be in all environments. If successful device code flows appear, without a need for them, investigate for validity. For more information, see Microsoft identity platform and the OAuth 2.0 device authorization grant flow Sigma rules

Application configuration changes

Monitor changes to application configuration. Specifically, configuration changes to the uniform resource identifier (URI), ownership, and log-out URL.

Dangling URI and Redirect URI changes

Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
Dangling URI	High	Microsoft Entra logs and Application Registration	Service-Core Directory, Category-ApplicationManagement Activity: Update Application Success – Property Name AppAddress	For example, look for dangling URIs that point to a domain name that no longer exists or one that you don't explicitly own. Microsoft Sentinel template Sigma rules
Redirect URI configuration changes	High	Microsoft Entra logs	Service-Core Directory, Category-ApplicationManagement Activity: Update Application Success – Property Name AppAddress	Look for URIs not using HTTPS*, URIs with wildcards at the end or the domain of the URL, URIs that are NOT unique to the application, URIs that point to a domain you don't control. Microsoft Sentinel template Sigma rules

Alert when these changes are detected.

AppID URI added, modified, or removed

Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
Changes to AppID URI	High	Microsoft Entra logs	Service-Core Directory, Category-ApplicationManagement Activity: Update Application Activity: Update Service principal	Look for any AppID URI modifications, such as adding, modifying, or removing the URI. Microsoft Sentinel template Sigma rules

Alert when these changes are detected outside approved change management procedures.

New owner

Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
Changes to application ownership	Medium	Microsoft Entra logs	Service-Core Directory, Category-ApplicationManagement Activity: Add owner to application	Look for any instance of a user being added as an application owner outside of normal change management activities. Microsoft Sentinel template Sigma rules

Log-out URL modified or removed

Expand table

What to monitor	Risk Level	Where	Filter/sub-filter	Notes
Changes to log-out URL	Low	Microsoft Entra logs	Service-Core Directory, Category-ApplicationManagement Activity: Update Application -and- Activity: Update service principle	Look for any modifications to a sign-out URL. Blank entries or entries to non-existent locations would stop a user from terminating a session. Microsoft Sentinel template Sigma rules

Resources

- GitHub Microsoft Entra toolkit - https://github.com/microsoft/AzureADToolkit
- Azure Key Vault security overview and security guidance - Azure Key Vault security overview
- Solorigate risk information and tools - Microsoft Entra workbook to help you access Solorigate risk
- OAuth attack detection guidance - Unusual addition of credentials to an OAuth app
- Microsoft Entra monitoring configuration information for SIEMs - Partner tools with Azure Monitor integration

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 Privileged Identity Management

Security operations for devices

Security operations for infrastructure

Feedback

Was this page helpful? Yes No

Provide product feedback

Additional resources

Training

Module

Monitor and maintain Microsoft Entra ID - Training

Audit and diagnostic logs within Microsoft Entra ID provide a rich view into how users are accessing your Azure solution. Learn to monitor, troubleshoot, and analyze sign-in data.

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