



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 Graph

Guides

API Reference

Resources ▾

Download SDKs

Open Graph Explorer

Version



Filter by title

## riskDetection resource type

Article • 02/15/2024 • 15 contributors



Feedback

### In this article

[Methods](#)

[Properties](#)

[Relationships](#)

[JSON representation](#)

Namespace: microsoft.graph

- › Service principal risk detection
- › Risky service principal
- › Identity provider
- › Identity provider (deprecated)
- › Invitation
- › Multitenant organization
- › OAuth2 (delegated) permission grant

 **Download PDF**

Represents information about a detected risk in a Microsoft Entra tenant.

Microsoft Entra ID continually evaluates [user risks](#) and app or user [sign-in](#) risks based on various signals and machine learning. This API provides programmatic access to all risk detections in your Microsoft Entra environment.

For more information about risk detection, see [Microsoft Entra ID Protection](#) and [What are risk detections?](#)

**ⓘ Note**

The availability of risk detection data is governed by the [Microsoft Entra data retention policies](#).

## Methods

Expand table

Method	Return type	Description
List	<code>riskDetection</code> collection	Get a list of the <code>riskDetection</code> objects and their properties.
Get	<code>riskDetection</code>	Read the properties and relationships of a <code>riskDetection</code> object.

# Properties

 Expand table


Property	Type	Description
activity	activityType	Indicates the activity type that the user is performing. Possible values are: <code>signi</code>

		unknownFutureValue.
activityDateTime	DateTimeOffset	Date and time that the risky DateTimeOffset type represents information using ISO 8601 UTC time. For example, midnight is look like this: 2014-01-01T00:00:00Z
additionalInfo	String	Additional information associated with the detection in JSON format. For example, [{"Key": "userAgent", "Value": "(Windows NT 10.0; Win64; x64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36"}]. Possible keys in the additionalInfo object are: userAgent, alertUrl, relatedUserAgent, deviceId, relatedLocation, requestId, lastActivityTimeInUtc, mailAddress, clientLocation, clientIp, and clientUserAgent. For more information about the values, see <a href="#">riskReasons</a> value.
correlationId	String	Correlation ID of the sign-in detection. This property is null if the detection is not associated with a sign-in.
detectedDateTime	DateTimeOffset	Date and time that the risk was detected. The DateTimeOffset type represents information using ISO 8601 UTC time. For example, midnight looks like this: 2014-01-01T00:00:00Z
detectionTimingType	riskDetectionTimingType	Timing of the detected risk (reason). The values are: notDefined, realTime, offline, and unknownFutureValue.
id	String	Unique ID of the risk detection.
ipAddress	String	Provides the IP address of the device where the risk occurred.
lastUpdatedDateTime	DateTimeOffset	Date and time that the risk was last updated. The DateTimeOffset type represents information using ISO 8601 UTC time. For example, midnight looks like this: 2014-01-01T00:00:00Z

		and time information using I always in UTC time. For exam Jan 1, 2014 is look like this:
location	<a href="#">signInLocation</a>	Location of the sign-in.
requestId	String	Request ID of the sign-in ass detection. This property is nu not associated with a sign-in
riskDetail	riskDetail	Details of the detected risk. 1 none, adminGeneratedTempo userChangedPasswordOnPren userPerformedSecuredPassv userPerformedSecuredPassv adminConfirmedSigninSafe, aiConfirmedSigninSafe, userPassedMFADrivenByRisk adminDismissedAllRiskForl adminConfirmedSigninCompr adminConfirmedUserCompron unknownFutureValue, m365DAdminDismissedDetect use the Prefer: include - request header to get the fo <a href="#">evolvable enum</a> : m365DAdmin

riskEventType	String	The type of risk event detected are <code>adminConfirmedUserCompromised</code> , <code>anomalousToken</code> , <code>anomalousAnonymizedIPAddress</code> , <code>generalInvestigationsThreatIntellectualPropertySuspiciousSendingPatterns</code> , <code>maliciousIPAddress</code> , <code>malwareInboxManipulation</code> , <code>newCountry</code> , <code>passwordSpray</code> , <code>suspiciousAPITraffic</code> , <code>suspiciousBrowser</code> , <code>suspiciousIPAddress</code> , <code>tokenUnfamiliarFeatures</code> , <code>unlikelyDetection</code> is a premium detection. For more information about <a href="#">types and detection</a> .
riskLevel	riskLevel	Level of the detected risk. Possible values are: <code>medium</code> , <code>high</code> , <code>hidden</code> , <code>none</code> .
riskState	riskState	The state of a detected risky value. Possible values are: <code>none</code> , <code>confirmed</code> , <code>dismissed</code> , <code>atRisk</code> , <code>confirmedFutureValue</code> , <code>unknownFutureValue</code> .
source	String	Source of the risk detection. Possible values are: <code>activeDirectory</code> .
tokenIssuerType	tokenIssuerType	Indicates the type of token issued in sign-in risk. Possible values are: <code>ADFS</code> , <code>ADFServices</code> , <code>Unknown</code> .
userDisplayName	String	The user principal name (UPN) of the user.
userId	String	Unique ID of the user.
userPrincipalName	String	The user principal name (UPN) of the user.

riskReasons values

 Expand table

riskEventType	Value	UI display string
investigationsThreatIntelligence	suspiciousIP	This sign-in was from a suspicious IP address
investigationsThreatIntelligence	passwordSpray	This user account was attacked by a password spray.

# Relationships

None.

# JSON representation

The following JSON representation shows the resource type.

```
{
  "@odata.type": "#microsoft.graph.riskDetection",
  "id": "String (identifier)",
  "requestId": "String",
  "correlationId": "String",
  "riskEventType": "String",
  "riskState": "String",
  "riskLevel": "String",
  "riskDetail": "String",
  "source": "String",
  "detectionTimingType": "String",
  "activity": "String",
  "tokenIssuerType": "String",
  "ipAddress": "String",
  "location": {
    "@odata.type": "microsoft.graph.signInLocation"
  },
  "activityDateTime": "String (timestamp)",
  "detectedDateTime": "String (timestamp)",
  "lastUpdatedDateTime": "String (timestamp)",
  "userId": "String",
  "userDisplayName": "String",
}
```

```
"userPrincipalName": "String",  
"additionalInfo": "String"  
}
```

## Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)


## Additional resources

### Events



Nov 20, 12 AM - Nov 22, 12 AM

Join online sessions at Microsoft Ignite created to expand your skills and help you tackle today's complex issues.

[Register now](#)

 English (United States)

 Your Privacy Choices

 Theme 

[Manage cookies](#)


[Previous Versions](#)

[Blog](#) 

[Contribute](#)

[Privacy](#) 

[Terms of Use](#)

[Trademarks](#) 

© Microsoft 2024