

Version

Microsoft Graph REST API v1.0 ▾

 Filter by title

- ▾ Identity protection
- Overview
- ▾ Risk detection
- Risk detection**
- List
- Get
- Risky user
- Risky user history item
- Service principal risk detection
- Risky service principal
- Identity provider
- Identity provider (deprecated)
- Invitation
- Multitenant organization
- OAuth2 (delegated) permission grant
- Organizational branding
- Policies
- User flows in external tenants
- User flows in workforce tenants
- Granular delegated admin privileges
- Mail
- Notes
- People and workplace intelligence
- Personal contacts
- Reports
- Search
- Security
- Sites and lists
- Tasks and plans
- Teamwork and communications
- To-do tasks
- Workbooks and charts

 **Download PDF**



# riskDetection resource type

Article • 02/15/2024 • [15 contributors](#)

 [Feedback](#)

## In this article

- [Methods](#)
- [Properties](#)
- [Relationships](#)
- [JSON representation](#)

Namespace: microsoft.graph

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
<a href="#">List</a>	<a href="#">riskDetection</a> collection	Get a list of the <a href="#">riskDetection</a> objects and their properties.
<a href="#">Get</a>	<a href="#">riskDetection</a>	Read the properties and relationships of a <a href="#">riskDetection</a> object.

## Properties

 **Expand table**

Property	Type	Description
activity	activityType	Indicates the activity type the detected risk is linked to. Possible values are: <code>signin</code> , <code>user</code> , <code>unknownFutureValue</code> .
activityDateTime	DateTimeOffset	Date and time that the risky activity occurred. The DateTimeOffset type represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is look like this: <code>2014-01-01T00:00:00Z</code>

additionalInfo	String	<p>Additional information associated with the risk detection in JSON format. For example, "[{"Key":"userAgent","Value":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/68.0.3440.106 Safari/537.36"}]".</p> <p>Possible keys in the additionalInfo JSON string are: userAgent, alertUrl, relatedEventTimeInUtc, relatedUserAgent, deviceInformation, relatedLocation, requestId, correlationId, lastActivityTimeInUtc, malwareName, clientLocation, clientIp, riskReasons.</p> <p>For more information about riskReasons and possible values, see <a href="#">riskReasons values</a>.</p>
correlationId	String	<p>Correlation ID of the sign-in associated with the risk detection. This property is null if the risk detection is not associated with a sign-in.</p>
detectedDateTime	DateTimeOffset	<p>Date and time that the risk was detected. The DateTimeOffset type represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 looks like this: 2014-01-01T00:00:00Z</p>
detectionTimingType	riskDetectionTimingType	<p>Timing of the detected risk (real-time/offline). Possible values are: notDefined, realtime, nearRealtime, offline, unknownFutureValue.</p>
id	String	<p>Unique ID of the risk detection. Inherited from <a href="#">entity</a></p>
ipAddress	String	<p>Provides the IP address of the client from where the risk occurred.</p>
lastUpdatedDateTime	DateTimeOffset	<p>Date and time that the risk detection was last updated. The DateTimeOffset type represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is look like this: 2014-01-01T00:00:00Z</p>
location	<a href="#">signInLocation</a>	<p>Location of the sign-in.</p>
requestId	String	<p>Request ID of the sign-in associated with the risk detection. This property is null if the risk detection is not associated with a sign-in.</p>
riskDetail	riskDetail	<p>Details of the detected risk. The possible values are: none, adminGeneratedTemporaryPassword, userChangedPasswordOnPremises, userPerformedSecuredPasswordChange, userPerformedSecuredPasswordReset, adminConfirmedSignInSafe, aiConfirmedSignInSafe, userPassedMFADrivenByRiskBasedPolicy, adminDismissedAllRiskForUser, adminConfirmedSignInCompromised, hidden, adminConfirmedUserCompromised, unknownFutureValue, m365DAdminDismissedDetection. Note that you must use the Prefer: include - unknown -enum-members request header to get the following value(s) in this <a href="#">evolvable enum</a>: m365DAdminDismissedDetection.</p>
riskEventType	String	<p>The type of risk event detected. The possible values are adminConfirmedUserCompromised, anomalousToken, anomalousUserActivity, anonymizedIPAddress, generic, impossibleTravel, investigationsThreatIntelligence, suspiciousSendingPatterns, leakedCredentials, maliciousIPAddress, malwareInfectedIPAddress, mcasSuspiciousInboxManipulationRules,</p>

		<code>newCountry</code> , <code>passwordSpray</code> , <code>riskyIPAddress</code> , <code>suspiciousAPITraffic</code> , <code>suspiciousBrowser</code> , <code>suspiciousInboxForwarding</code> , <code>suspiciousIPAddress</code> , <code>tokenIssuerAnomaly</code> , <code>unfamiliarFeatures</code> , <code>unlikelyTravel</code> . If the risk detection is a premium detection, will show <code>generic</code> . For more information about each value, see <a href="#">Risk types and detection</a> .
riskLevel	riskLevel	Level of the detected risk. Possible values are: <code>low</code> , <code>medium</code> , <code>high</code> , <code>hidden</code> , <code>none</code> , <code>unknownFutureValue</code> .
riskState	riskState	The state of a detected risky user or sign-in. Possible values are: <code>none</code> , <code>confirmedSafe</code> , <code>remediated</code> , <code>dismissed</code> , <code>atRisk</code> , <code>confirmedCompromised</code> , <code>unknownFutureValue</code> .
source	String	Source of the risk detection. For example, <code>activeDirectory</code> .
tokenIssuerType	tokenIssuerType	Indicates the type of token issuer for the detected sign-in risk. Possible values are: <code>AzureAD</code> , <code>ADFederationServices</code> , <code>UnknownFutureValue</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
<code>investigationsThreatIntelligence</code>	<code>suspiciousIP</code>	This sign-in was from a suspicious IP address
<code>investigationsThreatIntelligence</code>	<code>passwordSpray</code>	This user account was attacked by a password spray.

## Relationships

None.

## JSON representation

The following JSON representation shows the resource type.

JSONCopy

```
{
  "@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](#)