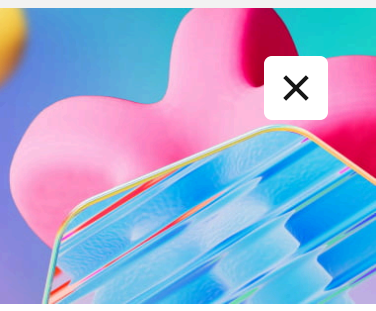

riskDetection resource type

Article • 02/15/2024 • 15 contributors

Feedback

In this article

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
List	riskDetection collection	Get a list of the riskDetection objects and their properties.
Get	riskDetection	Read the properties and relationships of a riskDetection object.

Properties

Expand table

Download PDF

Property	Type	Description
activity	activityType	Indicates the activity type the detected risk is linked to. Possible values are: `signin`, `user`, `unknownFutureValue`.
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: `2014-01-01T00:00:00Z`
additionalInfo	String	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\"}]"`. Possible keys in the additionalInfo JSON string are: `userAgent`, `alertUrl`, `relatedEventTimeInUtc`, `relatedUserAgent`, `deviceInformation`, `relatedLocation`, `requestId`, `correlationId`, `lastActivityTimeInUtc`, `malwareName`, `clientLocation`, `clientIp`, `riskReasons`. For more information about riskReasons and possible values, see riskReasons values.
correlationId	String	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.
detectedDateTime	DateTimeOffset	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`
detectionTimingType	riskDetectionTimingType	Timing of the detected risk (real-time/offline). Possible values are: `notDefined`, `realtime`, `nearRealtime`, `offline`, `unknownFutureValue`.
id	String	Unique ID of the risk detection. Inherited from entity
ipAddress	String	Provides the IP address of the client from where the risk occurred.
lastUpdatedDateTime	DateTimeOffset	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`
location	signInLocation	Location of the sign-in.
requestId	String	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.
riskDetail	riskDetail	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 evolvable enum: `m365DAdminDismissedDetection`.
riskEventType	String	The type of risk event detected. The possible values are `adminConfirmedUserCompromised`, `anomalousToken`, `anomalousUserActivity`, `anonymizedIPAddress`, `generic`, `impossibleTravel`, `investigationsThreatIntelligence`, `suspiciousSendingPatterns`, `leakedCredentials`, `maliciousIPAddress`,`malwareInfectedIPAddress`, `mcasSuspiciousInboxManipulationRules`, `newCountry`, `passwordSpray`,`riskyIPAddress`, `suspiciousAPITraffic`, `suspiciousBrowser`,`suspiciousInboxForwarding`, `suspiciousIPAddress`, `tokenIssuerAnomaly`, `unfamiliarFeatures`, `unlikelyTravel`. If the risk detection is a premium detection, will show `generic`. For more information about each value, see Risk types and detection.
riskLevel	riskLevel	Level of the detected risk. Possible values are: `low`, `medium`, `high`, `hidden`, `none`, `unknownFutureValue`.
riskState	riskState	The state of a detected risky user or sign-in. Possible values are: `none`, `confirmedSafe`, `remediated`, `dismissed`, `atRisk`, `confirmedCompromised`, `unknownFutureValue`.
source	String	Source of the risk detection. For example, `activeDirectory`.
tokenIssuerType	tokenIssuerType	Indicates the type of token issuer for the detected sign-in risk. Possible values are: `AzureAD`, `ADFederationServices`, `UnknownFutureValue`.
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.

JSON Copy

```
{
  "@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