



Welcome

Amazon Fraud Detector



API Version 2019-11-15

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Fraud Detector: Welcome

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

.....	xxiii
Welcome	1
Actions	2
BatchCreateVariable	5
Request Syntax	5
Request Parameters	5
Response Syntax	6
Response Elements	6
Errors	6
See Also	7
BatchGetVariable	8
Request Syntax	8
Request Parameters	8
Response Syntax	8
Response Elements	9
Errors	9
See Also	10
CancelBatchImportJob	11
Request Syntax	11
Request Parameters	11
Response Elements	11
Errors	11
See Also	12
CancelBatchPredictionJob	14
Request Syntax	14
Request Parameters	14
Response Elements	14
Errors	14
See Also	15
CreateBatchImportJob	17
Request Syntax	17
Request Parameters	17
Response Elements	19
Errors	19

See Also	20
CreateBatchPredictionJob	21
Request Syntax	21
Request Parameters	21
Response Elements	23
Errors	23
See Also	24
CreateDetectorVersion	26
Request Syntax	26
Request Parameters	26
Response Syntax	28
Response Elements	28
Errors	29
See Also	30
CreateList	31
Request Syntax	31
Request Parameters	31
Response Elements	33
Errors	33
See Also	33
CreateModel	35
Request Syntax	35
Request Parameters	35
Response Elements	36
Errors	36
See Also	37
CreateModelVersion	39
Request Syntax	39
Request Parameters	39
Response Syntax	41
Response Elements	41
Errors	42
See Also	43
CreateRule	44
Request Syntax	44
Request Parameters	44

Response Syntax	46
Response Elements	46
Errors	46
See Also	47
CreateVariable	48
Request Syntax	48
Request Parameters	48
Response Elements	50
Errors	50
See Also	51
DeleteBatchImportJob	52
Request Syntax	52
Request Parameters	52
Response Elements	52
Errors	52
See Also	53
DeleteBatchPredictionJob	54
Request Syntax	54
Request Parameters	54
Response Elements	54
Errors	54
See Also	55
DeleteDetector	56
Request Syntax	56
Request Parameters	56
Response Elements	56
Errors	56
See Also	57
DeleteDetectorVersion	59
Request Syntax	59
Request Parameters	59
Response Elements	60
Errors	60
See Also	61
DeleteEntityType	62
Request Syntax	62

Request Parameters	62
Response Elements	62
Errors	62
See Also	63
DeleteEvent	65
Request Syntax	65
Request Parameters	65
Response Elements	66
Errors	66
See Also	67
DeleteEventsByEventType	68
Request Syntax	68
Request Parameters	68
Response Syntax	68
Response Elements	68
Errors	69
See Also	70
DeleteEventType	71
Request Syntax	71
Request Parameters	71
Response Elements	71
Errors	71
See Also	72
DeleteExternalModel	74
Request Syntax	74
Request Parameters	74
Response Elements	74
Errors	74
See Also	75
DeleteLabel	77
Request Syntax	77
Request Parameters	77
Response Elements	77
Errors	77
See Also	78
DeleteList	79

Request Syntax	79
Request Parameters	79
Response Elements	79
Errors	79
See Also	80
DeleteModel	82
Request Syntax	82
Request Parameters	82
Response Elements	83
Errors	83
See Also	84
DeleteModelVersion	85
Request Syntax	85
Request Parameters	85
Response Elements	86
Errors	86
See Also	87
DeleteOutcome	88
Request Syntax	88
Request Parameters	88
Response Elements	88
Errors	88
See Also	89
DeleteRule	91
Request Syntax	91
Request Parameters	91
Response Elements	91
Errors	91
See Also	92
DeleteVariable	94
Request Syntax	94
Request Parameters	94
Response Elements	94
Errors	94
See Also	95
DescribeDetector	97

Request Syntax	97
Request Parameters	97
Response Syntax	98
Response Elements	98
Errors	99
See Also	100
DescribeModelVersions	101
Request Syntax	101
Request Parameters	101
Response Syntax	102
Response Elements	106
Errors	106
See Also	107
GetBatchImportJobs	109
Request Syntax	109
Request Parameters	109
Response Syntax	110
Response Elements	110
Errors	111
See Also	112
GetBatchPredictionJobs	113
Request Syntax	113
Request Parameters	113
Response Syntax	114
Response Elements	114
Errors	115
See Also	116
GetDeleteEventsByEventStatus	117
Request Syntax	117
Request Parameters	117
Response Syntax	117
Response Elements	117
Errors	118
See Also	119
GetDetectors	120
Request Syntax	120

Request Parameters	120
Response Syntax	121
Response Elements	121
Errors	122
See Also	122
GetDetectorVersion	124
Request Syntax	124
Request Parameters	124
Response Syntax	125
Response Elements	125
Errors	127
See Also	128
GetEntityTypes	130
Request Syntax	130
Request Parameters	130
Response Syntax	131
Response Elements	131
Errors	132
See Also	132
GetEvent	134
Request Syntax	134
Request Parameters	134
Response Syntax	134
Response Elements	135
Errors	135
See Also	136
GetEventPrediction	137
Request Syntax	137
Request Parameters	137
Response Syntax	140
Response Elements	141
Errors	141
See Also	142
GetEventPredictionMetadata	144
Request Syntax	144
Request Parameters	144

Response Syntax	145
Response Elements	147
Errors	150
See Also	150
GetEventTypes	152
Request Syntax	152
Request Parameters	152
Response Syntax	153
Response Elements	153
Errors	154
See Also	155
GetExternalModels	156
Request Syntax	156
Request Parameters	156
Response Syntax	157
Response Elements	157
Errors	158
See Also	159
GetKMSEncryptionKey	160
Response Syntax	160
Response Elements	160
Errors	160
See Also	161
GetLabels	162
Request Syntax	162
Request Parameters	162
Response Syntax	163
Response Elements	163
Errors	164
See Also	164
GetListElements	166
Request Syntax	166
Request Parameters	166
Response Syntax	167
Response Elements	167
Errors	168

See Also	168
GetListsMetadata	170
Request Syntax	170
Request Parameters	170
Response Syntax	171
Response Elements	171
Errors	172
See Also	172
GetModels	174
Request Syntax	174
Request Parameters	174
Response Syntax	175
Response Elements	175
Errors	176
See Also	177
GetModelVersion	178
Request Syntax	178
Request Parameters	178
Response Syntax	179
Response Elements	179
Errors	182
See Also	182
GetOutcomes	184
Request Syntax	184
Request Parameters	184
Response Syntax	185
Response Elements	185
Errors	186
See Also	186
GetRules	188
Request Syntax	188
Request Parameters	188
Response Syntax	189
Response Elements	190
Errors	190
See Also	191

GetVariables	192
Request Syntax	192
Request Parameters	192
Response Syntax	193
Response Elements	193
Errors	194
See Also	194
ListEventPredictions	196
Request Syntax	196
Request Parameters	196
Response Syntax	198
Response Elements	198
Errors	199
See Also	199
ListTagsForResource	201
Request Syntax	201
Request Parameters	201
Response Syntax	202
Response Elements	202
Errors	202
See Also	203
PutDetector	205
Request Syntax	205
Request Parameters	205
Response Elements	206
Errors	206
See Also	207
PutEntityType	208
Request Syntax	208
Request Parameters	208
Response Elements	209
Errors	209
See Also	210
PutEventType	211
Request Syntax	211
Request Parameters	211

Response Elements	213
Errors	213
See Also	214
PutExternalModel	215
Request Syntax	215
Request Parameters	215
Response Elements	217
Errors	217
See Also	218
PutKMSEncryptionKey	219
Request Syntax	219
Request Parameters	219
Response Elements	219
Errors	219
See Also	220
PutLabel	222
Request Syntax	222
Request Parameters	222
Response Elements	223
Errors	223
See Also	224
PutOutcome	225
Request Syntax	225
Request Parameters	225
Response Elements	226
Errors	226
See Also	227
SendEvent	228
Request Syntax	228
Request Parameters	228
Response Elements	230
Errors	230
See Also	231
TagResource	232
Request Syntax	232
Request Parameters	232

Response Elements	233
Errors	233
See Also	233
UntagResource	235
Request Syntax	235
Request Parameters	235
Response Elements	236
Errors	236
See Also	236
UpdateDetectorVersion	238
Request Syntax	238
Request Parameters	238
Response Elements	240
Errors	240
See Also	241
UpdateDetectorVersionMetadata	243
Request Syntax	243
Request Parameters	243
Response Elements	244
Errors	244
See Also	245
UpdateDetectorVersionStatus	246
Request Syntax	246
Request Parameters	246
Response Elements	247
Errors	247
See Also	248
UpdateEventLabel	249
Request Syntax	249
Request Parameters	249
Response Elements	250
Errors	250
See Also	251
UpdateList	252
Request Syntax	252
Request Parameters	252

Response Elements	254
Errors	254
See Also	255
UpdateModel	256
Request Syntax	256
Request Parameters	256
Response Elements	257
Errors	257
See Also	258
UpdateModelVersion	259
Request Syntax	259
Request Parameters	259
Response Syntax	261
Response Elements	261
Errors	262
See Also	263
UpdateModelVersionStatus	264
Request Syntax	264
Request Parameters	264
Response Elements	265
Errors	265
See Also	266
UpdateRuleMetadata	268
Request Syntax	268
Request Parameters	268
Response Elements	268
Errors	269
See Also	269
UpdateRuleVersion	271
Request Syntax	271
Request Parameters	271
Response Syntax	272
Response Elements	273
Errors	273
See Also	274
UpdateVariable	275

Request Syntax	275
Request Parameters	275
Response Elements	276
Errors	276
See Also	277
Data Types	278
AggregatedLogOddsMetric	281
Contents	281
See Also	281
AggregatedVariablesImpactExplanation	282
Contents	282
See Also	282
AggregatedVariablesImportanceMetrics	284
Contents	284
See Also	284
AllowDenyList	285
Contents	285
See Also	286
ATIMetricDataPoint	287
Contents	287
See Also	288
ATIModelPerformance	289
Contents	289
See Also	289
ATITrainingMetricsValue	290
Contents	290
See Also	290
BatchCreateVariableError	291
Contents	291
See Also	291
BatchGetVariableError	292
Contents	292
See Also	292
BatchImport	293
Contents	293
See Also	296

BatchPrediction	297
Contents	297
See Also	300
DataValidationMetrics	301
Contents	301
See Also	301
Detector	302
Contents	302
See Also	303
DetectorVersionSummary	304
Contents	304
See Also	305
Entity	306
Contents	306
See Also	306
EntityType	307
Contents	307
See Also	308
EvaluatedExternalModel	309
Contents	309
See Also	309
EvaluatedModelVersion	311
Contents	311
See Also	311
EvaluatedRule	313
Contents	313
See Also	314
Event	315
Contents	315
See Also	316
EventOrchestration	317
Contents	317
See Also	317
EventPredictionSummary	318
Contents	318
See Also	319

EventType	320
Contents	320
See Also	322
EventVariableSummary	323
Contents	323
See Also	323
ExternalEventsDetail	324
Contents	324
See Also	324
ExternalModel	325
Contents	325
See Also	327
ExternalModelOutputs	328
Contents	328
See Also	328
ExternalModelSummary	329
Contents	329
See Also	329
FieldValidationMessage	330
Contents	330
See Also	331
FileValidationMessage	332
Contents	332
See Also	332
FilterCondition	333
Contents	333
See Also	333
IngestedEventsDetail	334
Contents	334
See Also	334
IngestedEventStatistics	335
Contents	335
See Also	336
IngestedEventsTimeWindow	337
Contents	337
See Also	337

KMSKey	338
Contents	338
See Also	338
Label	339
Contents	339
See Also	340
LabelSchema	341
Contents	341
See Also	342
LogOddsMetric	343
Contents	343
See Also	343
MetricDataPoint	344
Contents	344
See Also	345
Model	346
Contents	346
See Also	347
ModelEndpointDataBlob	349
Contents	349
See Also	349
ModelInputConfiguration	350
Contents	350
See Also	351
ModelOutputConfiguration	352
Contents	352
See Also	352
ModelScores	353
Contents	353
See Also	353
ModelVersion	354
Contents	354
See Also	355
ModelVersionDetail	356
Contents	356
See Also	358

ModelVersionEvaluation	360
Contents	360
See Also	360
OFIMetricDataPoint	361
Contents	361
See Also	362
OFIModelPerformance	363
Contents	363
See Also	363
OFITrainingMetricsValue	364
Contents	364
See Also	364
Outcome	365
Contents	365
See Also	366
PredictionExplanations	367
Contents	367
See Also	367
PredictionTimeRange	368
Contents	368
See Also	368
Rule	369
Contents	369
See Also	370
RuleDetail	371
Contents	371
See Also	373
RuleResult	374
Contents	374
See Also	374
Tag	375
Contents	375
See Also	375
TFIMetricDataPoint	376
Contents	376
See Also	377

TFIModelPerformance	378
Contents	378
See Also	378
TFITrainingMetricsValue	379
Contents	379
See Also	379
TrainingDataSchema	380
Contents	380
See Also	380
TrainingMetrics	381
Contents	381
See Also	381
TrainingMetricsV2	382
Contents	382
See Also	382
TrainingResult	383
Contents	383
See Also	383
TrainingResultV2	384
Contents	384
See Also	385
UncertaintyRange	386
Contents	386
See Also	386
Variable	387
Contents	387
See Also	389
VariableEntry	390
Contents	390
See Also	391
VariableImpactExplanation	392
Contents	392
See Also	392
VariableImportanceMetrics	394
Contents	394
See Also	394

Common Parameters	395
Common Errors	398

Amazon Fraud Detector is no longer be open to new customers as of November 7, 2025. For capabilities similar to Amazon Fraud Detector, explore Amazon SageMaker AI, AutoGluon, and AWS WAF.

Welcome

This is the Amazon Fraud Detector API Reference. This guide is for developers who need detailed information about Amazon Fraud Detector API actions, data types, and errors. For more information about Amazon Fraud Detector features, see the [Amazon Fraud Detector User Guide](#).

We provide the Query API as well as AWS software development kits (SDK) for Amazon Fraud Detector in Java and Python programming languages.

The Amazon Fraud Detector Query API provides HTTPS requests that use the HTTP verb GET or POST and a Query parameter `Action`. AWS SDK provides libraries, sample code, tutorials, and other resources for software developers who prefer to build applications using language-specific APIs instead of submitting a request over HTTP or HTTPS. These libraries provide basic functions that automatically take care of tasks such as cryptographically signing your requests, retrying requests, and handling error responses, so that it is easier for you to get started. For more information about the AWS SDKs, go to [Tools to build on AWS](#) page, scroll down to the **SDK** section, and choose plus (+) sign to expand the section.

This document was last published on March 13, 2026.

Actions

The following actions are supported:

- [BatchCreateVariable](#)
- [BatchGetVariable](#)
- [CancelBatchImportJob](#)
- [CancelBatchPredictionJob](#)
- [CreateBatchImportJob](#)
- [CreateBatchPredictionJob](#)
- [CreateDetectorVersion](#)
- [CreateList](#)
- [CreateModel](#)
- [CreateModelVersion](#)
- [CreateRule](#)
- [CreateVariable](#)
- [DeleteBatchImportJob](#)
- [DeleteBatchPredictionJob](#)
- [DeleteDetector](#)
- [DeleteDetectorVersion](#)
- [DeleteEntityType](#)
- [DeleteEvent](#)
- [DeleteEventsByEventType](#)
- [DeleteEventType](#)
- [DeleteExternalModel](#)
- [DeleteLabel](#)
- [DeleteList](#)
- [DeleteModel](#)
- [DeleteModelVersion](#)
- [DeleteOutcome](#)
- [DeleteRule](#)

- [DeleteVariable](#)
- [DescribeDetector](#)
- [DescribeModelVersions](#)
- [GetBatchImportJobs](#)
- [GetBatchPredictionJobs](#)
- [GetDeleteEventsByEventTypeStatus](#)
- [GetDetectors](#)
- [GetDetectorVersion](#)
- [GetEntityTypes](#)
- [GetEvent](#)
- [GetEventPrediction](#)
- [GetEventPredictionMetadata](#)
- [GetEventTypes](#)
- [GetExternalModels](#)
- [GetKMSEncryptionKey](#)
- [GetLabels](#)
- [GetListElements](#)
- [GetListsMetadata](#)
- [GetModels](#)
- [GetModelVersion](#)
- [GetOutcomes](#)
- [GetRules](#)
- [GetVariables](#)
- [ListEventPredictions](#)
- [ListTagsForResource](#)
- [PutDetector](#)
- [PutEntityType](#)
- [PutEventType](#)
- [PutExternalModel](#)
- [PutKMSEncryptionKey](#)

- [PutLabel](#)
- [PutOutcome](#)
- [SendEvent](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateDetectorVersion](#)
- [UpdateDetectorVersionMetadata](#)
- [UpdateDetectorVersionStatus](#)
- [UpdateEventLabel](#)
- [UpdateList](#)
- [UpdateModel](#)
- [UpdateModelVersion](#)
- [UpdateModelVersionStatus](#)
- [UpdateRuleMetadata](#)
- [UpdateRuleVersion](#)
- [UpdateVariable](#)

BatchCreateVariable

Creates a batch of variables.

Request Syntax

```
{
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ],
  "variableEntries": [
    {
      "dataSource": "string",
      "dataType": "string",
      "defaultValue": "string",
      "description": "string",
      "name": "string",
      "variableType": "string"
    }
  ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

tags

A collection of key and value pairs.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

variableEntries

The list of variables for the batch create variable request.

Type: Array of [VariableEntry](#) objects

Array Members: Minimum number of 1 item. Maximum number of 25 items.

Required: Yes

Response Syntax

```
{
  "errors": [
    {
      "code": number,
      "message": "string",
      "name": "string"
    }
  ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

[errors](#)

Provides the errors for the BatchCreateVariable request.

Type: Array of [BatchCreateVariableError](#) objects

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as PutExternalModel, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerErrorException

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

BatchGetVariable

Gets a batch of variables.

Request Syntax

```
{  
  "names": [ "string" ]  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

names

The list of variable names to get.

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 100 items.

Required: Yes

Response Syntax

```
{  
  "errors": [  
    {  
      "code": number,  
      "message": "string",  
      "name": "string"  
    }  
  ],  
  "variables": [  
    {  
      "arn": "string",  
      "createdTime": "string",  
      "dataSource": "string",  
    }  
  ]  
}
```

```
    "dataType": "string",
    "defaultValue": "string",
    "description": "string",
    "lastUpdatedTime": "string",
    "name": "string",
    "variableType": "string"
  }
]
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

errors

The errors from the request.

Type: Array of [BatchGetVariableError](#) objects

variables

The returned variables.

Type: Array of [Variable](#) objects

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

CancelBatchImportJob

Cancels an in-progress batch import job.

Request Syntax

```
{  
  "jobId": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

jobId

The ID of an in-progress batch import job to cancel.

Amazon Fraud Detector will throw an error if the batch import job is in FAILED, CANCELED, or COMPLETED state.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

CancelBatchPredictionJob

Cancels the specified batch prediction job.

Request Syntax

```
{  
  "jobId": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

jobId

The ID of the batch prediction job to cancel.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerErrorException

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

CreateBatchImportJob

Creates a batch import job.

Request Syntax

```
{
  "eventName": "string",
  "iamRoleArn": "string",
  "inputPath": "string",
  "jobId": "string",
  "outputPath": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

eventName

The name of the event type.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

iamRoleArn

The ARN of the IAM role created for Amazon S3 bucket that holds your data file.

The IAM role must have read permissions to your input S3 bucket and write permissions to your output S3 bucket. For more information about bucket permissions, see [User policy examples](#) in the *Amazon S3 User Guide*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:iam\:\:[0-9]{12}\:role\/[^\s]{2,64}$`

Required: Yes

inputPath

The URI that points to the Amazon S3 location of your data file.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `^s3:\:\/\/(.+)\$`

Required: Yes

jobId

The ID of the batch import job. The ID cannot be of a past job, unless the job exists in CREATE_FAILED state.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+\$`

Required: Yes

outputPath

The URI that points to the Amazon S3 location for storing your results.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `^s3:\:\/\/(.+)\$`

Required: Yes

tags

A collection of key-value pairs associated with this request.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

CreateBatchPredictionJob

Creates a batch prediction job.

Request Syntax

```
{
  "detectorName": "string",
  "detectorVersion": "string",
  "eventName": "string",
  "iamRoleArn": "string",
  "inputPath": "string",
  "jobId": "string",
  "outputPath": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

detectorName

The name of the detector.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

detectorVersion

The detector version.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 5.

Pattern: `^([1-9][0-9]*)$`

Required: No

eventTypeName

The name of the event type.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

iamRoleArn

The ARN of the IAM role to use for this job request.

The IAM Role must have read permissions to your input S3 bucket and write permissions to your output S3 bucket. For more information about bucket permissions, see [User policy examples](#) in the *Amazon S3 User Guide*.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:iam\:\:[0-9]{12}\:role\/[^\s]{2,64}$`

Required: Yes

inputPath

The Amazon S3 location of your training file.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `^s3:\/\/(.+)$`

Required: Yes

jobId

The ID of the batch prediction job.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

outputPath

The Amazon S3 location of your output file.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `^s3://(.+)$`

Required: Yes

tags

A collection of key and value pairs.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

CreateDetectorVersion

Creates a detector version. The detector version starts in a DRAFT status.

Request Syntax

```
{
  "description": "string",
  "detectorId": "string",
  "externalModelEndpoints": [ "string" ],
  "modelVersions": [
    {
      "arn": "string",
      "modelId": "string",
      "modelType": "string",
      "modelVersionNumber": "string"
    }
  ],
  "ruleExecutionMode": "string",
  "rules": [
    {
      "detectorId": "string",
      "ruleId": "string",
      "ruleVersion": "string"
    }
  ],
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

description

The description of the detector version.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

detectorId

The ID of the detector under which you want to create a new version.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

externalModelEndpoints

The Amazon Sagemaker model endpoints to include in the detector version.

Type: Array of strings

Required: No

modelVersions

The model versions to include in the detector version.

Type: Array of [ModelVersion](#) objects

Required: No

ruleExecutionMode

The rule execution mode for the rules included in the detector version.

You can define and edit the rule mode at the detector version level, when it is in draft status.

If you specify `FIRST_MATCHED`, Amazon Fraud Detector evaluates rules sequentially, first to last, stopping at the first matched rule. Amazon Fraud detector then provides the outcomes for that single rule.

If you specify `ALL_MATCHED`, Amazon Fraud Detector evaluates all rules and returns the outcomes for all matched rules.

The default behavior is `FIRST_MATCHED`.

Type: String

Valid Values: `ALL_MATCHED` | `FIRST_MATCHED`

Required: No

rules

The rules to include in the detector version.

Type: Array of [Rule](#) objects

Required: Yes

tags

A collection of key and value pairs.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

Response Syntax

```
{
  "detectorId": "string",
  "detectorVersionId": "string",
  "status": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

detectorId

The ID for the created version's parent detector.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

detectorVersionId

The ID for the created detector.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 5.

Pattern: `^([1-9][0-9]*)$`

status

The status of the detector version.

Type: String

Valid Values: DRAFT | ACTIVE | INACTIVE

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

CreateList

Creates a list.

List is a set of input data for a variable in your event dataset. You use the input data in a rule that's associated with your detector. For more information, see [Lists](#).

Request Syntax

```
{
  "description": "string",
  "elements": [ "string" ],
  "name": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ],
  "variableType": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

description

The description of the list.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

elements

The names of the elements, if providing. You can also create an empty list and add elements later using the [UpdateList](#) API.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 100000 items.

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `^\S+(\ +\S+)*$`

Required: No

name

The name of the list.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

Required: Yes

tags

A collection of the key and value pairs.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

variableType

The variable type of the list. You can only assign the variable type with String data type. For more information, see [Variable types](#).

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[A-Z_]{1,64}$`

Required: No

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)

- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

CreateModel

Creates a model using the specified model type.

Request Syntax

```
{
  "description": "string",
  "eventName": "string",
  "modelId": "string",
  "modelType": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

description

The model description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

eventName

The name of the event type.

Type: String

Required: Yes

modelId

The model ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

Required: Yes

modelType

The model type.

Type: String

Valid Values: ONLINE_FRAUD_INSIGHTS | TRANSACTION_FRAUD_INSIGHTS | ACCOUNT_TAKEOVER_INSIGHTS

Required: Yes

tags

A collection of key and value pairs.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)

- [AWS SDK for Ruby V3](#)

CreateModelVersion

Creates a version of the model using the specified model type and model id.

Request Syntax

```
{
  "externalEventsDetail": {
    "dataAccessRoleArn": "string",
    "dataLocation": "string"
  },
  "ingestedEventsDetail": {
    "ingestedEventsTimeWindow": {
      "endTime": "string",
      "startTime": "string"
    }
  },
  "modelId": "string",
  "modelType": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ],
  "trainingDataSchema": {
    "labelSchema": {
      "labelMapper": {
        "string" : [ "string" ]
      },
      "unlabeledEventsTreatment": "string"
    },
    "modelVariables": [ "string" ]
  },
  "trainingDataSource": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

externalEventsDetail

Details of the external events data used for model version training. Required if `trainingDataSource` is `EXTERNAL_EVENTS`.

Type: [ExternalEventsDetail](#) object

Required: No

ingestedEventsDetail

Details of the ingested events data used for model version training. Required if `trainingDataSource` is `INGESTED_EVENTS`.

Type: [IngestedEventsDetail](#) object

Required: No

modelId

The model ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

Required: Yes

modelType

The model type.

Type: String

Valid Values: `ONLINE_FRAUD_INSIGHTS` | `TRANSACTION_FRAUD_INSIGHTS` | `ACCOUNT_TAKEOVER_INSIGHTS`

Required: Yes

tags

A collection of key and value pairs.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

trainingDataSchema

The training data schema.

Type: [TrainingDataSchema](#) object

Required: Yes

trainingDataSource

The training data source location in Amazon S3.

Type: String

Valid Values: EXTERNAL_EVENTS | INGESTED_EVENTS

Required: Yes

Response Syntax

```
{
  "modelId": "string",
  "modelType": "string",
  "modelVersionNumber": "string",
  "status": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

modelId

The model ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

modelType

The model type.

Type: String

Valid Values: ONLINE_FRAUD_INSIGHTS | TRANSACTION_FRAUD_INSIGHTS | ACCOUNT_TAKEOVER_INSIGHTS

modelVersionNumber

The model version number of the model version created.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 7.

Pattern: `^[1-9][0-9]{0,3}\.[0-9]{1,2}$`

status

The model version status.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

CreateRule

Creates a rule for use with the specified detector.

Request Syntax

```
{
  "description": "string",
  "detectorId": "string",
  "expression": "string",
  "language": "string",
  "outcomes": [ "string" ],
  "ruleId": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

description

The rule description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

detectorId

The detector ID for the rule's parent detector.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

expression

The rule expression.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Required: Yes

language

The language of the rule.

Type: String

Valid Values: DETECTORPL

Required: Yes

outcomes

The outcome or outcomes returned when the rule expression matches.

Type: Array of strings

Array Members: Minimum number of 1 item.

Required: Yes

ruleId

The rule ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

tags

A collection of key and value pairs.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

Response Syntax

```
{
  "rule": {
    "detectorId": "string",
    "ruleId": "string",
    "ruleVersion": "string"
  }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

rule

The created rule.

Type: [Rule](#) object

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerErrorException

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

CreateVariable

Creates a variable.

Request Syntax

```
{
  "dataSource": "string",
  "dataType": "string",
  "defaultValue": "string",
  "description": "string",
  "name": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ],
  "variableType": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

dataSource

The source of the data.

Type: String

Valid Values: EVENT | MODEL_SCORE | EXTERNAL_MODEL_SCORE

Required: Yes

dataType

The data type of the variable.

Type: String

Valid Values: STRING | INTEGER | FLOAT | BOOLEAN | DATETIME

Required: Yes

defaultValue

The default value for the variable when no value is received.

Type: String

Required: Yes

description

The description.

Type: String

Required: No

name

The name of the variable.

Type: String

Required: Yes

tags

A collection of key and value pairs.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

variableType

The variable type. For more information see [Variable types](#).

Valid Values: AUTH_CODE | AVS | BILLING_ADDRESS_L1 | BILLING_ADDRESS_L2
| BILLING_CITY | BILLING_COUNTRY | BILLING_NAME | BILLING_PHONE |
BILLING_STATE | BILLING_ZIP | CARD_BIN | CATEGORICAL | CURRENCY_CODE

| EMAIL_ADDRESS | FINGERPRINT | FRAUD_LABEL | FREE_FORM_TEXT |
IP_ADDRESS | NUMERIC | ORDER_ID | PAYMENT_TYPE | PHONE_NUMBER | PRICE
| PRODUCT_CATEGORY | SHIPPING_ADDRESS_L1 | SHIPPING_ADDRESS_L2 |
SHIPPING_CITY | SHIPPING_COUNTRY | SHIPPING_NAME | SHIPPING_PHONE |
SHIPPING_STATE | SHIPPING_ZIP | USERAGENT

Type: String

Required: No

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteBatchImportJob

Deletes the specified batch import job ID record. This action does not delete the data that was batch imported.

Request Syntax

```
{  
  "jobId": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

jobId

The ID of the batch import job to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerErrorException

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteBatchPredictionJob

Deletes a batch prediction job.

Request Syntax

```
{
  "jobId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

jobId

The ID of the batch prediction job to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerErrorException

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteDetector

Deletes the detector. Before deleting a detector, you must first delete all detector versions and rule versions associated with the detector.

When you delete a detector, Amazon Fraud Detector permanently deletes the detector and the data is no longer stored in Amazon Fraud Detector.

Request Syntax

```
{
  "detectorId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

detectorId

The ID of the detector to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteDetectorVersion

Deletes the detector version. You cannot delete detector versions that are in ACTIVE status.

When you delete a detector version, Amazon Fraud Detector permanently deletes the detector and the data is no longer stored in Amazon Fraud Detector.

Request Syntax

```
{
  "detectorId": "string",
  "detectorVersionId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

detectorId

The ID of the parent detector for the detector version to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

detectorVersionId

The ID of the detector version to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 5.

Pattern: `^([1-9][0-9]*)$`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteEntityType

Deletes an entity type.

You cannot delete an entity type that is included in an event type.

When you delete an entity type, Amazon Fraud Detector permanently deletes that entity type and the data is no longer stored in Amazon Fraud Detector.

Request Syntax

```
{  
  "name": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

name

The name of the entity type to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteEvent

Deletes the specified event.

When you delete an event, Amazon Fraud Detector permanently deletes that event and the event data is no longer stored in Amazon Fraud Detector. If `deleteAuditHistory` is `True`, event data is available through search for up to 30 seconds after the delete operation is completed.

Request Syntax

```
{
  "deleteAuditHistory": boolean,
  "eventId": "string",
  "eventName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

[deleteAuditHistory](#)

Specifies whether or not to delete any predictions associated with the event. If set to `True`,

Type: Boolean

Required: No

[eventId](#)

The ID of the event to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

eventType

The name of the event type.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteEventsByEventType

Deletes all events of a particular event type.

Request Syntax

```
{  
  "eventName": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

eventName

The name of the event type.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

Response Syntax

```
{  
  "eventsDeletionStatus": "string",  
  "eventName": "string"  
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

eventsDeletionStatus

The status of the delete request.

Type: String

eventName

Name of event type for which to delete the events.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteEventType

Deletes an event type.

You cannot delete an event type that is used in a detector or a model.

When you delete an event type, Amazon Fraud Detector permanently deletes that event type and the data is no longer stored in Amazon Fraud Detector.

Request Syntax

```
{  
  "name": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

name

The name of the event type to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteExternalModel

Removes a SageMaker model from Amazon Fraud Detector.

You can remove an Amazon SageMaker model if it is not associated with a detector version. Removing a SageMaker model disconnects it from Amazon Fraud Detector, but the model remains available in SageMaker.

Request Syntax

```
{  
  "modelEndpoint": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

modelEndpoint

The endpoint of the Amazon Sagemaker model to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 63.

Pattern: `^[0-9A-Za-z_-]+$`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteLabel

Deletes a label.

You cannot delete labels that are included in an event type in Amazon Fraud Detector.

You cannot delete a label assigned to an event ID. You must first delete the relevant event ID.

When you delete a label, Amazon Fraud Detector permanently deletes that label and the data is no longer stored in Amazon Fraud Detector.

Request Syntax

```
{  
  "name": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

name

The name of the label to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerErrorException

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteList

Deletes the list, provided it is not used in a rule.

When you delete a list, Amazon Fraud Detector permanently deletes that list and the elements in the list.

Request Syntax

```
{  
  "name": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

name

The name of the list to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteModel

Deletes a model.

You can delete models and model versions in Amazon Fraud Detector, provided that they are not associated with a detector version.

When you delete a model, Amazon Fraud Detector permanently deletes that model and the data is no longer stored in Amazon Fraud Detector.

Request Syntax

```
{
  "modelId": "string",
  "modelType": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

modelId

The model ID of the model to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

Required: Yes

modelType

The model type of the model to delete.

Type: String

Valid Values: ONLINE_FRAUD_INSIGHTS | TRANSACTION_FRAUD_INSIGHTS |
ACCOUNT_TAKEOVER_INSIGHTS

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteModelVersion

Deletes a model version.

You can delete models and model versions in Amazon Fraud Detector, provided that they are not associated with a detector version.

When you delete a model version, Amazon Fraud Detector permanently deletes that model version and the data is no longer stored in Amazon Fraud Detector.

Request Syntax

```
{
  "modelId": "string",
  "modelType": "string",
  "modelVersionNumber": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

modelId

The model ID of the model version to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

Required: Yes

modelType

The model type of the model version to delete.

Type: String

Valid Values: ONLINE_FRAUD_INSIGHTS | TRANSACTION_FRAUD_INSIGHTS | ACCOUNT_TAKEOVER_INSIGHTS

Required: Yes

modelVersionNumber

The model version number of the model version to delete.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 7.

Pattern: `^[1-9][0-9]{0,3}\.[0-9]{1,2}$`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteOutcome

Deletes an outcome.

You cannot delete an outcome that is used in a rule version.

When you delete an outcome, Amazon Fraud Detector permanently deletes that outcome and the data is no longer stored in Amazon Fraud Detector.

Request Syntax

```
{  
  "name": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

name

The name of the outcome to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteRule

Deletes the rule. You cannot delete a rule if it is used by an ACTIVE or INACTIVE detector version.

When you delete a rule, Amazon Fraud Detector permanently deletes that rule and the data is no longer stored in Amazon Fraud Detector.

Request Syntax

```
{
  "rule": {
    "detectorId": "string",
    "ruleId": "string",
    "ruleVersion": "string"
  }
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

rule

A rule.

Type: [Rule](#) object

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteVariable

Deletes a variable.

You can't delete variables that are included in an event type in Amazon Fraud Detector.

Amazon Fraud Detector automatically deletes model output variables and SageMaker model output variables when you delete the model. You can't delete these variables manually.

When you delete a variable, Amazon Fraud Detector permanently deletes that variable and the data is no longer stored in Amazon Fraud Detector.

Request Syntax

```
{  
  "name": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

name

The name of the variable to delete.

Type: String

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DescribeDetector

Gets all versions for a specified detector.

Request Syntax

```
{
  "detectorId": "string",
  "maxResults": number,
  "nextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

detectorId

The detector ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

maxResults

The maximum number of results to return for the request.

Type: Integer

Valid Range: Minimum value of 1000. Maximum value of 2500.

Required: No

nextToken

The next token from the previous response.

Type: String

Required: No

Response Syntax

```
{
  "arn": "string",
  "detectorId": "string",
  "detectorVersionSummaries": [
    {
      "description": "string",
      "detectorVersionId": "string",
      "lastUpdatedTime": "string",
      "status": "string"
    }
  ],
  "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

arn

The detector ARN.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:frauddetector\:[a-z0-9-]{3,20}\:[0-9]{12}\:[^\s]{2,128}$`

detectorId

The detector ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

detectorVersionSummaries

The status and description for each detector version.

Type: Array of [DetectorVersionSummary](#) objects

nextToken

The next token to be used for subsequent requests.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DescribeModelVersions

Gets all of the model versions for the specified model type or for the specified model type and model ID. You can also get details for a single, specified model version.

Request Syntax

```
{
  "maxResults": number,
  "modelId": "string",
  "modelType": "string",
  "modelVersionNumber": "string",
  "nextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

maxResults

The maximum number of results to return.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 10.

Required: No

modelId

The model ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

Required: No

modelType

The model type.

Type: String

Valid Values: ONLINE_FRAUD_INSIGHTS | TRANSACTION_FRAUD_INSIGHTS | ACCOUNT_TAKEOVER_INSIGHTS

Required: No

modelVersionNumber

The model version number.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 7.

Pattern: `^[1-9][0-9]{0,3}\.[0-9]{1,2}$`

Required: No

nextToken

The next token from the previous results.

Type: String

Required: No

Response Syntax

```
{
  "modelVersionDetails": [
    {
      "arn": "string",
      "createdTime": "string",
      "externalEventsDetail": {
        "dataAccessRoleArn": "string",
        "dataLocation": "string"
      },
      "ingestedEventsDetail": {
        "ingestedEventsTimeWindow": {
          "endTime": "string",
```

```
    "startTime": "string"
  }
},
"lastUpdatedTime": "string",
"modelId": "string",
"modelType": "string",
"modelVersionNumber": "string",
"status": "string",
"trainingDataSchema": {
  "labelSchema": {
    "labelMapper": {
      "string" : [ "string" ]
    },
    "unlabeledEventsTreatment": "string"
  },
  "modelVariables": [ "string" ]
},
"trainingDataSource": "string",
"trainingResult": {
  "dataValidationMetrics": {
    "fieldLevelMessages": [
      {
        "content": "string",
        "fieldName": "string",
        "identifier": "string",
        "title": "string",
        "type": "string"
      }
    ],
    "fileLevelMessages": [
      {
        "content": "string",
        "title": "string",
        "type": "string"
      }
    ]
  },
  "trainingMetrics": {
    "auc": number,
    "metricDataPoints": [
      {
        "fpr": number,
        "precision": number,
        "threshold": number,
```

```
        "tpr": number
      }
    ]
  },
  "variableImportanceMetrics": {
    "logOddsMetrics": [
      {
        "variableImportance": number,
        "variableName": "string",
        "variableType": "string"
      }
    ]
  }
},
"trainingResultV2": {
  "aggregatedVariablesImportanceMetrics": {
    "logOddsMetrics": [
      {
        "aggregatedVariablesImportance": number,
        "variableNames": [ "string" ]
      }
    ]
  },
  "dataValidationMetrics": {
    "fieldLevelMessages": [
      {
        "content": "string",
        "fieldName": "string",
        "identifier": "string",
        "title": "string",
        "type": "string"
      }
    ],
    "fileLevelMessages": [
      {
        "content": "string",
        "title": "string",
        "type": "string"
      }
    ]
  },
  "trainingMetricsV2": {
    "ati": {
      "metricDataPoints": [
```

```
    {
      "adr": number,
      "atodr": number,
      "cr": number,
      "threshold": number
    }
  ],
  "modelPerformance": {
    "asi": number
  }
},
"ofi": {
  "metricDataPoints": [
    {
      "fpr": number,
      "precision": number,
      "threshold": number,
      "tpr": number
    }
  ],
  "modelPerformance": {
    "auc": number,
    "uncertaintyRange": {
      "lowerBoundValue": number,
      "upperBoundValue": number
    }
  }
},
"tfi": {
  "metricDataPoints": [
    {
      "fpr": number,
      "precision": number,
      "threshold": number,
      "tpr": number
    }
  ],
  "modelPerformance": {
    "auc": number,
    "uncertaintyRange": {
      "lowerBoundValue": number,
      "upperBoundValue": number
    }
  }
}
```

```
    }
  },
  "variableImportanceMetrics": {
    "logOddsMetrics": [
      {
        "variableImportance": number,
        "variableName": "string",
        "variableType": "string"
      }
    ]
  }
}
],
"nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

modelVersionDetails

The model version details.

Type: Array of [ModelVersionDetail](#) objects

nextToken

The next token.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerErrorException

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetBatchImportJobs

Gets all batch import jobs or a specific job of the specified ID. This is a paginated API. If you provide a null `maxResults`, this action retrieves a maximum of 50 records per page. If you provide a `maxResults`, the value must be between 1 and 50. To get the next page results, provide the pagination token from the `GetBatchImportJobsResponse` as part of your request. A null pagination token fetches the records from the beginning.

Request Syntax

```
{
  "jobId": "string",
  "maxResults": number,
  "nextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

jobId

The ID of the batch import job to get.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

maxResults

The maximum number of objects to return for request.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 50.

Required: No

nextToken

The next token from the previous request.

Type: String

Required: No

Response Syntax

```
{
  "batchImports": [
    {
      "arn": "string",
      "completionTime": "string",
      "eventName": "string",
      "failedRecordsCount": number,
      "failureReason": "string",
      "iamRoleArn": "string",
      "inputPath": "string",
      "jobId": "string",
      "outputPath": "string",
      "processedRecordsCount": number,
      "startTime": "string",
      "status": "string",
      "totalRecordsCount": number
    }
  ],
  "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

batchImports

An array containing the details of each batch import job.

Type: Array of [BatchImport](#) objects

[nextToken](#)

The next token for the subsequent request.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetBatchPredictionJobs

Gets all batch prediction jobs or a specific job if you specify a job ID. This is a paginated API. If you provide a null `maxResults`, this action retrieves a maximum of 50 records per page. If you provide a `maxResults`, the value must be between 1 and 50. To get the next page results, provide the pagination token from the `GetBatchPredictionJobsResponse` as part of your request. A null pagination token fetches the records from the beginning.

Request Syntax

```
{
  "jobId": "string",
  "maxResults": number,
  "nextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

jobId

The batch prediction job for which to get the details.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

maxResults

The maximum number of objects to return for the request.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 50.

Required: No

nextToken

The next token from the previous request.

Type: String

Required: No

Response Syntax

```
{
  "batchPredictions": [
    {
      "arn": "string",
      "completionTime": "string",
      "detectorName": "string",
      "detectorVersion": "string",
      "eventName": "string",
      "failureReason": "string",
      "iamRoleArn": "string",
      "inputPath": "string",
      "jobId": "string",
      "lastHeartbeatTime": "string",
      "outputPath": "string",
      "processedRecordsCount": number,
      "startTime": "string",
      "status": "string",
      "totalRecordsCount": number
    }
  ],
  "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

batchPredictions

An array containing the details of each batch prediction job.

Type: Array of [BatchPrediction](#) objects

[nextToken](#)

The next token for the subsequent request.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetDeleteEventsByEventTypeStatus

Retrieves the status of a DeleteEventsByEventType action.

Request Syntax

```
{  
  "eventName": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

eventName

Name of event type for which to get the deletion status.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

Response Syntax

```
{  
  "eventsDeletionStatus": "string",  
  "eventName": "string"  
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

eventsDeletionStatus

The deletion status.

Type: String

Valid Values: IN_PROGRESS_INITIALIZING | IN_PROGRESS | CANCEL_IN_PROGRESS | CANCELED | COMPLETE | FAILED

eventTypeName

The event type name.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetDetectors

Gets all detectors or a single detector if a `detectorId` is specified. This is a paginated API. If you provide a null `maxResults`, this action retrieves a maximum of 10 records per page. If you provide a `maxResults`, the value must be between 5 and 10. To get the next page results, provide the pagination token from the `GetDetectorsResponse` as part of your request. A null pagination token fetches the records from the beginning.

Request Syntax

```
{
  "detectorId": "string",
  "maxResults": number,
  "nextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

detectorId

The detector ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

maxResults

The maximum number of objects to return for the request.

Type: Integer

Valid Range: Minimum value of 5. Maximum value of 10.

Required: No

nextToken

The next token for the subsequent request.

Type: String

Required: No

Response Syntax

```
{
  "detectors": [
    {
      "arn": "string",
      "createdTime": "string",
      "description": "string",
      "detectorId": "string",
      "eventName": "string",
      "lastUpdatedTime": "string"
    }
  ],
  "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

detectors

The detectors.

Type: Array of [Detector](#) objects

nextToken

The next page token.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)

- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetDetectorVersion

Gets a particular detector version.

Request Syntax

```
{
  "detectorId": "string",
  "detectorVersionId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

detectorId

The detector ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

detectorVersionId

The detector version ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 5.

Pattern: `^([1-9][0-9]*)$`

Required: Yes

Response Syntax

```
{
  "arn": "string",
  "createdTime": "string",
  "description": "string",
  "detectorId": "string",
  "detectorVersionId": "string",
  "externalModelEndpoints": [ "string" ],
  "lastUpdatedTime": "string",
  "modelVersions": [
    {
      "arn": "string",
      "modelId": "string",
      "modelType": "string",
      "modelVersionNumber": "string"
    }
  ],
  "ruleExecutionMode": "string",
  "rules": [
    {
      "detectorId": "string",
      "ruleId": "string",
      "ruleVersion": "string"
    }
  ],
  "status": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

arn

The detector version ARN.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:frauddetector\:[a-z0-9-]{3,20}\:[0-9]{12}\:[^\s]{2,128}$`

createdTime

The timestamp when the detector version was created.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

description

The detector version description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

detectorId

The detector ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

detectorVersionId

The detector version ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 5.

Pattern: `^([1-9][0-9]*)$`

externalModelEndpoints

The Amazon SageMaker model endpoints included in the detector version.

Type: Array of strings

lastUpdatedTime

The timestamp when the detector version was last updated.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

modelVersions

The model versions included in the detector version.

Type: Array of [ModelVersion](#) objects

ruleExecutionMode

The execution mode of the rule in the detector

FIRST_MATCHED indicates that Amazon Fraud Detector evaluates rules sequentially, first to last, stopping at the first matched rule. Amazon Fraud detector then provides the outcomes for that single rule.

ALL_MATCHED indicates that Amazon Fraud Detector evaluates all rules and returns the outcomes for all matched rules. You can define and edit the rule mode at the detector version level, when it is in draft status.

Type: String

Valid Values: ALL_MATCHED | FIRST_MATCHED

rules

The rules included in the detector version.

Type: Array of [Rule](#) objects

status

The status of the detector version.

Type: String

Valid Values: DRAFT | ACTIVE | INACTIVE

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerErrorException

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetEntityTypes

Gets all entity types or a specific entity type if a name is specified. This is a paginated API. If you provide a null `maxResults`, this action retrieves a maximum of 10 records per page. If you provide a `maxResults`, the value must be between 5 and 10. To get the next page results, provide the pagination token from the `GetEntityTypesResponse` as part of your request. A null pagination token fetches the records from the beginning.

Request Syntax

```
{
  "maxResults": number,
  "name": "string",
  "nextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

maxResults

The maximum number of objects to return for the request.

Type: Integer

Valid Range: Minimum value of 5. Maximum value of 10.

Required: No

name

The name.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

[nextToken](#)

The next token for the subsequent request.

Type: String

Required: No

Response Syntax

```
{
  "entityTypes": [
    {
      "arn": "string",
      "createdTime": "string",
      "description": "string",
      "lastUpdatedTime": "string",
      "name": "string"
    }
  ],
  "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

[entityTypes](#)

An array of entity types.

Type: Array of [EntityType](#) objects

[nextToken](#)

The next page token.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)

- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetEvent

Retrieves details of events stored with Amazon Fraud Detector. This action does not retrieve prediction results.

Request Syntax

```
{
  "eventId": "string",
  "eventName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

eventId

The ID of the event to retrieve.

Type: String

Required: Yes

eventName

The event type of the event to retrieve.

Type: String

Required: Yes

Response Syntax

```
{
  "event": {
    "currentLabel": "string",
    "entities": [
      {
```

```
        "entityId": "string",
        "entityType": "string"
    }
],
"eventId": "string",
"eventTimestamp": "string",
"eventName": "string",
"eventVariables": {
    "string" : "string"
},
"labelTimestamp": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

event

The details of the event.

Type: [Event](#) object

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetEventPrediction

Evaluates an event against a detector version. If a version ID is not provided, the detector's (ACTIVE) version is used.

Request Syntax

```
{
  "detectorId": "string",
  "detectorVersionId": "string",
  "entities": [
    {
      "entityId": "string",
      "entityType": "string"
    }
  ],
  "eventId": "string",
  "eventTimestamp": "string",
  "eventTypeName": "string",
  "eventVariables": {
    "string" : "string"
  },
  "externalModelEndpointDataBlobs": {
    "string" : {
      "byteBuffer": blob,
      "contentType": "string"
    }
  }
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

detectorId

The detector ID.

Type: String

Required: Yes

detectorVersionId

The detector version ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 5.

Pattern: `^[1-9][0-9]*$`

Required: No

entities

The entity type (associated with the detector's event type) and specific entity ID representing who performed the event. If an entity id is not available, use "UNKNOWN."

Type: Array of [Entity](#) objects

Required: Yes

eventId

The unique ID used to identify the event.

Type: String

Required: Yes

eventTimestamp

Timestamp that defines when the event under evaluation occurred. The timestamp must be specified using ISO 8601 standard in UTC.

Type: String

Length Constraints: Minimum length of 10. Maximum length of 30.

Required: Yes

eventName

The event type associated with the detector specified for the prediction.

Type: String

Required: Yes

eventVariables

Names of the event type's variables you defined in Amazon Fraud Detector to represent data elements and their corresponding values for the event you are sending for evaluation.

Important

You must provide at least one eventVariable

To ensure most accurate fraud prediction and to simplify your data preparation, Amazon Fraud Detector will replace all missing variables or values as follows:

For Amazon Fraud Detector trained models:

If a null value is provided explicitly for a variable or if a variable is missing, model will replace the null value or the missing variable (no variable name in the eventVariables map) with calculated default mean/medians for numeric variables and with special values for categorical variables.

For imported SageMaker models:

If a null value is provided explicitly for a variable, the model and rules will use "null" as the value. If a variable is not provided (no variable name in the eventVariables map), model and rules will use the default value that is provided for the variable.

Type: String to string map

Map Entries: Maximum number of items.

Key Length Constraints: Minimum length of 1. Maximum length of 64.

Value Length Constraints: Minimum length of 1. Maximum length of 8192.

Required: Yes

externalModelEndpointDataBlobs

The Amazon SageMaker model endpoint input data blobs.

Type: String to [ModelEndpointDataBlob](#) object map

Key Length Constraints: Minimum length of 1. Maximum length of 63.

Key Pattern: $^{\wedge}[0-9A-Za-z_-]^{\$}$

Required: No

Response Syntax

```
{
  "externalModelOutputs": [
    {
      "externalModel": {
        "modelEndpoint": "string",
        "modelSource": "string"
      },
      "outputs": {
        "string" : "string"
      }
    }
  ],
  "modelScores": [
    {
      "modelVersion": {
        "arn": "string",
        "modelId": "string",
        "modelType": "string",
        "modelVersionNumber": "string"
      },
      "scores": {
        "string" : number
      }
    }
  ],
  "ruleResults": [
    {
      "outcomes": [ "string" ],
      "ruleId": "string"
    }
  ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

externalModelOutputs

The model scores for Amazon SageMaker models.

Type: Array of [ExternalModelOutputs](#) objects

modelScores

The model scores. Amazon Fraud Detector generates model scores between 0 and 1000, where 0 is low fraud risk and 1000 is high fraud risk. Model scores are directly related to the false positive rate (FPR). For example, a score of 600 corresponds to an estimated 10% false positive rate whereas a score of 900 corresponds to an estimated 2% false positive rate.

Type: Array of [ModelScores](#) objects

ruleResults

The results from the rules.

Type: Array of [RuleResult](#) objects

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerErrorException

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ResourceUnavailableException

An exception indicating that the attached customer-owned (external) model threw an exception when Amazon Fraud Detector invoked the model.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)

- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetEventPredictionMetadata

Gets details of the past fraud predictions for the specified event ID, event type, detector ID, and detector version ID that was generated in the specified time period.

Request Syntax

```
{  
  "detectorId": "string",  
  "detectorVersionId": "string",  
  "eventId": "string",  
  "eventName": "string",  
  "predictionTimestamp": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

detectorId

The detector ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

detectorVersionId

The detector version ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 5.

Pattern: `^([1-9][0-9]*)$`

Required: Yes

eventId

The event ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

eventName

The event type associated with the detector specified for the prediction.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

predictionTimestamp

The timestamp that defines when the prediction was generated. The timestamp must be specified using ISO 8601 standard in UTC.

We recommend calling [ListEventPredictions](#) first, and using the `predictionTimestamp` value in the response to provide an accurate prediction timestamp value.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: Yes

Response Syntax

```
{
  "detectorId": "string",
  "detectorVersionId": "string",
  "detectorVersionStatus": "string",
  "entityId": "string",
```

```
"entityType": "string",
"evaluatedExternalModels": [
  {
    "inputVariables": {
      "string": "string"
    },
    "modelEndpoint": "string",
    "outputVariables": {
      "string": "string"
    },
    "useEventVariables": boolean
  }
],
"evaluatedModelVersions": [
  {
    "evaluations": [
      {
        "evaluationScore": "string",
        "outputVariableName": "string",
        "predictionExplanations": {
          "aggregatedVariablesImpactExplanations": [
            {
              "eventVariableNames": [ "string" ],
              "logOddsImpact": number,
              "relativeImpact": "string"
            }
          ],
          "variableImpactExplanations": [
            {
              "eventVariableName": "string",
              "logOddsImpact": number,
              "relativeImpact": "string"
            }
          ]
        }
      }
    ],
    "modelId": "string",
    "modelType": "string",
    "modelVersion": "string"
  }
],
"eventId": "string",
"eventTimestamp": "string",
```

```
"eventName": "string",
"eventVariables": [
  {
    "name": "string",
    "source": "string",
    "value": "string"
  }
],
"outcomes": [ "string" ],
"predictionTimestamp": "string",
"ruleExecutionMode": "string",
"rules": [
  {
    "evaluated": boolean,
    "expression": "string",
    "expressionWithValues": "string",
    "matched": boolean,
    "outcomes": [ "string" ],
    "ruleId": "string",
    "ruleVersion": "string"
  }
]
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

detectorId

The detector ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

detectorVersionId

The detector version ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 5.

Pattern: $^([1-9][0-9]^*)\$$

detectorVersionStatus

The status of the detector version.

Type: String

entityId

The entity ID.

Type: String

entityType

The entity type.

Type: String

evaluatedExternalModels

External (Amazon SageMaker) models that were evaluated for generating predictions.

Type: Array of [EvaluatedExternalModel](#) objects

evaluatedModelVersions

Model versions that were evaluated for generating predictions.

Type: Array of [EvaluatedModelVersion](#) objects

eventId

The event ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: $^[0-9a-z_-]^+\$$

eventTimestamp

The timestamp for when the prediction was generated for the associated event ID.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

eventTypeName

The event type associated with the detector specified for this prediction.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

eventVariables

A list of event variables that influenced the prediction scores.

Type: Array of [EventVariableSummary](#) objects

outcomes

The outcomes of the matched rule, based on the rule execution mode.

Type: Array of strings

predictionTimestamp

The timestamp that defines when the prediction was generated.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

ruleExecutionMode

The execution mode of the rule used for evaluating variable values.

Type: String

Valid Values: ALL_MATCHED | FIRST_MATCHED

rules

List of rules associated with the detector version that were used for evaluating variable values.

Type: Array of [EvaluatedRule](#) objects

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)

- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetEventTypes

Gets all event types or a specific event type if name is provided. This is a paginated API. If you provide a null `maxResults`, this action retrieves a maximum of 10 records per page. If you provide a `maxResults`, the value must be between 5 and 10. To get the next page results, provide the pagination token from the `GetEventTypesResponse` as part of your request. A null pagination token fetches the records from the beginning.

Request Syntax

```
{
  "maxResults": number,
  "name": "string",
  "nextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

maxResults

The maximum number of objects to return for the request.

Type: Integer

Valid Range: Minimum value of 5. Maximum value of 10.

Required: No

name

The name.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

nextToken

The next token for the subsequent request.

Type: String

Required: No

Response Syntax

```
{
  "eventTypes": [
    {
      "arn": "string",
      "createdTime": "string",
      "description": "string",
      "entityTypes": [ "string" ],
      "eventIngestion": "string",
      "eventOrchestration": {
        "eventBridgeEnabled": boolean
      },
      "eventVariables": [ "string" ],
      "ingestedEventStatistics": {
        "eventDataSizeInBytes": number,
        "lastUpdatedTime": "string",
        "leastRecentEvent": "string",
        "mostRecentEvent": "string",
        "numberOfEvents": number
      },
      "labels": [ "string" ],
      "lastUpdatedTime": "string",
      "name": "string"
    }
  ],
  "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

eventTypes

An array of event types.

Type: Array of [EventType](#) objects

nextToken

The next page token.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetExternalModels

Gets the details for one or more Amazon SageMaker models that have been imported into the service. This is a paginated API. If you provide a null `maxResults`, this actions retrieves a maximum of 10 records per page. If you provide a `maxResults`, the value must be between 5 and 10. To get the next page results, provide the pagination token from the `GetExternalModelsResult` as part of your request. A null pagination token fetches the records from the beginning.

Request Syntax

```
{
  "maxResults": number,
  "modelEndpoint": "string",
  "nextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

[maxResults](#)

The maximum number of objects to return for the request.

Type: Integer

Valid Range: Minimum value of 5. Maximum value of 10.

Required: No

[modelEndpoint](#)

The Amazon SageMaker model endpoint.

Type: String

Required: No

[nextToken](#)

The next page token for the request.

Type: String

Required: No

Response Syntax

```
{
  "externalModels": [
    {
      "arn": "string",
      "createdTime": "string",
      "inputConfiguration": {
        "csvInputTemplate": "string",
        "eventName": "string",
        "format": "string",
        "jsonInputTemplate": "string",
        "useEventVariables": boolean
      },
      "invokeModelEndpointRoleArn": "string",
      "lastUpdatedTime": "string",
      "modelEndpoint": "string",
      "modelEndpointStatus": "string",
      "modelSource": "string",
      "outputConfiguration": {
        "csvIndexToVariableMap": {
          "string" : "string"
        },
        "format": "string",
        "jsonKeyToVariableMap": {
          "string" : "string"
        }
      }
    }
  ],
  "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

externalModels

Gets the Amazon SageMaker models.

Type: Array of [ExternalModel](#) objects

nextToken

The next page token to be used in subsequent requests.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetKMSEncryptionKey

Gets the encryption key if a KMS key has been specified to be used to encrypt content in Amazon Fraud Detector.

Response Syntax

```
{
  "kmsKey": {
    "kmsEncryptionKeyArn": "string"
  }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

kmsKey

The KMS encryption key.

Type: [KMSKey](#) object

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerErrorException

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetLabels

Gets all labels or a specific label if name is provided. This is a paginated API. If you provide a null `maxResults`, this action retrieves a maximum of 50 records per page. If you provide a `maxResults`, the value must be between 10 and 50. To get the next page results, provide the pagination token from the `GetLabelsResponse` as part of your request. A null pagination token fetches the records from the beginning.

Request Syntax

```
{
  "maxResults": number,
  "name": "string",
  "nextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

maxResults

The maximum number of objects to return for the request.

Type: Integer

Valid Range: Minimum value of 10. Maximum value of 50.

Required: No

name

The name of the label or labels to get.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

nextToken

The next token for the subsequent request.

Type: String

Required: No

Response Syntax

```
{
  "labels": [
    {
      "arn": "string",
      "createdTime": "string",
      "description": "string",
      "lastUpdatedTime": "string",
      "name": "string"
    }
  ],
  "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

labels

An array of labels.

Type: Array of [Label](#) objects

nextToken

The next page token.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)

- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetListElements

Gets all the elements in the specified list.

Request Syntax

```
{  
  "maxResults": number,  
  "name": "string",  
  "nextToken": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

maxResults

The maximum number of objects to return for the request.

Type: Integer

Valid Range: Minimum value of 500. Maximum value of 5000.

Required: No

name

The name of the list.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

Required: Yes

nextToken

The next token for the subsequent request.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 8192.

Pattern: .*

Required: No

Response Syntax

```
{  
  "elements": [ "string" ],  
  "nextToken": "string"  
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

elements

The list elements.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 100000 items.

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: ^\S+(+\S+)*\$

nextToken

The next page token.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 8192.

Pattern: .*

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)

- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetListsMetadata

Gets the metadata of either all the lists under the account or the specified list.

Request Syntax

```
{  
  "maxResults": number,  
  "name": "string",  
  "nextToken": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

maxResults

The maximum number of objects to return for the request.

Type: Integer

Valid Range: Minimum value of 5. Maximum value of 50.

Required: No

name

The name of the list.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

Required: No

nextToken

The next token for the subsequent request.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 8192.

Pattern: .*

Required: No

Response Syntax

```
{
  "lists": [
    {
      "arn": "string",
      "createdTime": "string",
      "description": "string",
      "name": "string",
      "updatedTime": "string",
      "variableType": "string"
    }
  ],
  "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

lists

The metadata of the specified list or all lists under the account.

Type: Array of [AllowDenyList](#) objects

nextToken

The next page token.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 8192.

Pattern: .*

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)

- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetModels

Gets one or more models. Gets all models for the AWS account if no model type and no model id provided. Gets all models for the AWS account and model type, if the model type is specified but model id is not provided. Gets a specific model if (model type, model id) tuple is specified.

This is a paginated API. If you provide a null `maxResults`, this action retrieves a maximum of 10 records per page. If you provide a `maxResults`, the value must be between 1 and 10. To get the next page results, provide the pagination token from the response as part of your request. A null pagination token fetches the records from the beginning.

Request Syntax

```
{
  "maxResults": number,
  "modelId": "string",
  "modelType": "string",
  "nextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

maxResults

The maximum number of objects to return for the request.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 10.

Required: No

modelId

The model ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

Required: No

modelType

The model type.

Type: String

Valid Values: ONLINE_FRAUD_INSIGHTS | TRANSACTION_FRAUD_INSIGHTS | ACCOUNT_TAKEOVER_INSIGHTS

Required: No

nextToken

The next token for the subsequent request.

Type: String

Required: No

Response Syntax

```
{
  "models": [
    {
      "arn": "string",
      "createdTime": "string",
      "description": "string",
      "eventTypeName": "string",
      "lastUpdatedTime": "string",
      "modelId": "string",
      "modelType": "string"
    }
  ],
  "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

models

The array of models.

Type: Array of [Model](#) objects

nextToken

The next page token to be used in subsequent requests.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetModelVersion

Gets the details of the specified model version.

Request Syntax

```
{  
  "modelId": "string",  
  "modelType": "string",  
  "modelVersionNumber": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

modelId

The model ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

Required: Yes

modelType

The model type.

Type: String

Valid Values: ONLINE_FRAUD_INSIGHTS | TRANSACTION_FRAUD_INSIGHTS | ACCOUNT_TAKEOVER_INSIGHTS

Required: Yes

modelVersionNumber

The model version number.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 7.

Pattern: `^[1-9][0-9]{0,3}\.[0-9]{1,2}$`

Required: Yes

Response Syntax

```
{
  "arn": "string",
  "externalEventsDetail": {
    "dataAccessRoleArn": "string",
    "dataLocation": "string"
  },
  "ingestedEventsDetail": {
    "ingestedEventsTimeWindow": {
      "endTime": "string",
      "startTime": "string"
    }
  },
  "modelId": "string",
  "modelType": "string",
  "modelVersionNumber": "string",
  "status": "string",
  "trainingDataSchema": {
    "labelSchema": {
      "labelMapper": {
        "string": [ "string" ]
      },
      "unlabeledEventsTreatment": "string"
    },
    "modelVariables": [ "string" ]
  },
  "trainingDataSource": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

arn

The model version ARN.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:frauddetector\:[a-z0-9-]{3,20}\:[0-9]{12}\:[^\s]{2,128}$`

externalEventsDetail

The details of the external events data used for training the model version. This will be populated if the `trainingDataSource` is `EXTERNAL_EVENTS`

Type: [ExternalEventsDetail](#) object

ingestedEventsDetail

The details of the ingested events data used for training the model version. This will be populated if the `trainingDataSource` is `INGESTED_EVENTS`.

Type: [IngestedEventsDetail](#) object

modelId

The model ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

modelType

The model type.

Type: String

Valid Values: `ONLINE_FRAUD_INSIGHTS` | `TRANSACTION_FRAUD_INSIGHTS` | `ACCOUNT_TAKEOVER_INSIGHTS`

modelVersionNumber

The model version number.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 7.

Pattern: `^[1-9][0-9]{0,3}\.[0-9]{1,2}$`

status

The model version status.

Possible values are:

- TRAINING_IN_PROGRESS
- TRAINING_COMPLETE
- ACTIVATE_REQUESTED
- ACTIVATE_IN_PROGRESS
- ACTIVE
- INACTIVATE_REQUESTED
- INACTIVATE_IN_PROGRESS
- INACTIVE
- ERROR

Type: String

trainingDataSchema

The training data schema.

Type: [TrainingDataSchema](#) object

trainingDataSource

The training data source.

Type: String

Valid Values: EXTERNAL_EVENTS | INGESTED_EVENTS

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)

- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetOutcomes

Gets one or more outcomes. This is a paginated API. If you provide a null `maxResults`, this actions retrieves a maximum of 100 records per page. If you provide a `maxResults`, the value must be between 50 and 100. To get the next page results, provide the pagination token from the `GetOutcomesResult` as part of your request. A null pagination token fetches the records from the beginning.

Request Syntax

```
{  
  "maxResults": number,  
  "name": "string",  
  "nextToken": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

maxResults

The maximum number of objects to return for the request.

Type: Integer

Valid Range: Minimum value of 50. Maximum value of 100.

Required: No

name

The name of the outcome or outcomes to get.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

nextToken

The next page token for the request.

Type: String

Required: No

Response Syntax

```
{
  "nextToken": "string",
  "outcomes": [
    {
      "arn": "string",
      "createdTime": "string",
      "description": "string",
      "lastUpdatedTime": "string",
      "name": "string"
    }
  ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

nextToken

The next page token for subsequent requests.

Type: String

outcomes

The outcomes.

Type: Array of [Outcome](#) objects

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)

- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetRules

Get all rules for a detector (paginated) if `ruleId` and `ruleVersion` are not specified. Gets all rules for the detector and the `ruleId` if present (paginated). Gets a specific rule if both the `ruleId` and the `ruleVersion` are specified.

This is a paginated API. Providing null `maxResults` results in retrieving maximum of 100 records per page. If you provide `maxResults` the value must be between 50 and 100. To get the next page result, provide a pagination token from `GetRulesResult` as part of your request. Null pagination token fetches the records from the beginning.

Request Syntax

```
{
  "detectorId": "string",
  "maxResults": number,
  "nextToken": "string",
  "ruleId": "string",
  "ruleVersion": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

detectorId

The detector ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

maxResults

The maximum number of rules to return for the request.

Type: Integer

Valid Range: Minimum value of 50. Maximum value of 100.

Required: No

nextToken

The next page token.

Type: String

Required: No

ruleId

The rule ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

ruleVersion

The rule version.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 5.

Pattern: `^([1-9][0-9]*)$`

Required: No

Response Syntax

```
{
  "nextToken": "string",
  "ruleDetails": [
    {
      "arn": "string",
```

```
    "createdTime": "string",
    "description": "string",
    "detectorId": "string",
    "expression": "string",
    "language": "string",
    "lastUpdatedTime": "string",
    "outcomes": [ "string" ],
    "ruleId": "string",
    "ruleVersion": "string"
  }
]
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

[nextToken](#)

The next page token to be used in subsequent requests.

Type: String

[ruleDetails](#)

The details of the requested rule.

Type: Array of [RuleDetail](#) objects

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerErrorException

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetVariables

Gets all of the variables or the specific variable. This is a paginated API. Providing null `maxSizePerPage` results in retrieving maximum of 100 records per page. If you provide `maxSizePerPage` the value must be between 50 and 100. To get the next page result, a provide a pagination token from `GetVariablesResult` as part of your request. Null pagination token fetches the records from the beginning.

Request Syntax

```
{  
  "maxResults": number,  
  "name": "string",  
  "nextToken": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

maxResults

The max size per page determined for the get variable request.

Type: Integer

Valid Range: Minimum value of 50. Maximum value of 100.

Required: No

name

The name of the variable.

Type: String

Required: No

nextToken

The next page token of the get variable request.

Type: String

Required: No

Response Syntax

```
{
  "nextToken": "string",
  "variables": [
    {
      "arn": "string",
      "createdTime": "string",
      "dataSource": "string",
      "dataType": "string",
      "defaultValue": "string",
      "description": "string",
      "lastUpdatedTime": "string",
      "name": "string",
      "variableType": "string"
    }
  ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

nextToken

The next page token to be used in subsequent requests.

Type: String

variables

The names of the variables returned.

Type: Array of [Variable](#) objects

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)

- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

ListEventPredictions

Gets a list of past predictions. The list can be filtered by detector ID, detector version ID, event ID, event type, or by specifying a time period. If filter is not specified, the most recent prediction is returned.

For example, the following filter lists all past predictions for xyz event type - { "eventType": { "value": "xyz" } }

This is a paginated API. If you provide a null `maxResults`, this action will retrieve a maximum of 10 records per page. If you provide a `maxResults`, the value must be between 50 and 100. To get the next page results, provide the `nextToken` from the response as part of your request. A null `nextToken` fetches the records from the beginning.

Request Syntax

```
{
  "detectorId": {
    "value": "string"
  },
  "detectorVersionId": {
    "value": "string"
  },
  "eventId": {
    "value": "string"
  },
  "eventType": {
    "value": "string"
  },
  "maxResults": number,
  "nextToken": "string",
  "predictionTimeRange": {
    "endTime": "string",
    "startTime": "string"
  }
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

detectorId

The detector ID.

Type: [FilterCondition](#) object

Required: No

detectorVersionId

The detector version ID.

Type: [FilterCondition](#) object

Required: No

eventId

The event ID.

Type: [FilterCondition](#) object

Required: No

eventType

The event type associated with the detector.

Type: [FilterCondition](#) object

Required: No

maxResults

The maximum number of predictions to return for the request.

Type: Integer

Valid Range: Minimum value of 50. Maximum value of 100.

Required: No

nextToken

Identifies the next page of results to return. Use the token to make the call again to retrieve the next page. Keep all other arguments unchanged. Each pagination token expires after 24 hours.

Type: String

Required: No

predictionTimeRange

The time period for when the predictions were generated.

Type: [PredictionTimeRange](#) object

Required: No

Response Syntax

```
{
  "eventPredictionSummaries": [
    {
      "detectorId": "string",
      "detectorVersionId": "string",
      "eventId": "string",
      "eventTimestamp": "string",
      "eventTypeName": "string",
      "predictionTimestamp": "string"
    }
  ],
  "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

eventPredictionSummaries

The summary of the past predictions.

Type: Array of [EventPredictionSummary](#) objects

nextToken

Identifies the next page of results to return. Use the token to make the call again to retrieve the next page. Keep all other arguments unchanged. Each pagination token expires after 24 hours.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

ListTagsForResource

Lists all tags associated with the resource. This is a paginated API. To get the next page results, provide the pagination token from the response as part of your request. A null pagination token fetches the records from the beginning.

Request Syntax

```
{  
  "maxResults": number,  
  "nextToken": "string",  
  "resourceARN": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

[maxResults](#)

The maximum number of objects to return for the request.

Type: Integer

Valid Range: Fixed value of 50.

Required: No

[nextToken](#)

The next token from the previous results.

Type: String

Required: No

[resourceARN](#)

The ARN that specifies the resource whose tags you want to list.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:frauddetector\:[a-z0-9-]{3,20}\:[0-9]{12}\:[^\s]{2,128}$`

Required: Yes

Response Syntax

```
{
  "nextToken": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

nextToken

The next token for subsequent requests.

Type: String

tags

A collection of key and value pairs.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)

- [AWS SDK for Ruby V3](#)

PutDetector

Creates or updates a detector.

Request Syntax

```
{
  "description": "string",
  "detectorId": "string",
  "eventTypeName": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

description

The description of the detector.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

detectorId

The detector ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

eventName

The name of the event type.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

tags

A collection of key and value pairs.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerErrorException

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

PutEntityType

Creates or updates an entity type. An entity represents who is performing the event. As part of a fraud prediction, you pass the entity ID to indicate the specific entity who performed the event. An entity type classifies the entity. Example classifications include customer, merchant, or account.

Request Syntax

```
{
  "description": "string",
  "name": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

description

The description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

name

The name of the entity type.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

[tags](#)

A collection of key and value pairs.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

PutEventType

Creates or updates an event type. An event is a business activity that is evaluated for fraud risk. With Amazon Fraud Detector, you generate fraud predictions for events. An event type defines the structure for an event sent to Amazon Fraud Detector. This includes the variables sent as part of the event, the entity performing the event (such as a customer), and the labels that classify the event. Example event types include online payment transactions, account registrations, and authentications.

Request Syntax

```
{
  "description": "string",
  "entityTypes": [ "string" ],
  "eventIngestion": "string",
  "eventOrchestration": {
    "eventBridgeEnabled": boolean
  },
  "eventVariables": [ "string" ],
  "labels": [ "string" ],
  "name": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

description

The description of the event type.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

entityTypes

The entity type for the event type. Example entity types: customer, merchant, account.

Type: Array of strings

Array Members: Minimum number of 1 item.

Required: Yes

eventIngestion

Specifies if ingestion is enabled or disabled.

Type: String

Valid Values: ENABLED | DISABLED

Required: No

eventOrchestration

Enables or disables event orchestration. If enabled, you can send event predictions to select AWS services for downstream processing of the events.

Type: [EventOrchestration](#) object

Required: No

eventVariables

The event type variables.

Type: Array of strings

Array Members: Minimum number of 1 item.

Required: Yes

labels

The event type labels.

Type: Array of strings

Required: No

name

The name.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

tags

A collection of key and value pairs.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerErrorException

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

PutExternalModel

Creates or updates an Amazon SageMaker model endpoint. You can also use this action to update the configuration of the model endpoint, including the IAM role and/or the mapped variables.

Request Syntax

```
{
  "inputConfiguration": {
    "csvInputTemplate": "string",
    "eventName": "string",
    "format": "string",
    "jsonInputTemplate": "string",
    "useEventVariables": boolean
  },
  "invokeModelEndpointRoleArn": "string",
  "modelEndpoint": "string",
  "modelEndpointStatus": "string",
  "modelSource": "string",
  "outputConfiguration": {
    "csvIndexToVariableMap": {
      "string" : "string"
    },
    "format": "string",
    "jsonKeyToVariableMap": {
      "string" : "string"
    }
  },
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

inputConfiguration

The model endpoint input configuration.

Type: [ModelInputConfiguration](#) object

Required: Yes

invokeModelEndpointRoleArn

The IAM role used to invoke the model endpoint.

Type: String

Required: Yes

modelEndpoint

The model endpoints name.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 63.

Pattern: `^[0-9A-Za-z_-]+$`

Required: Yes

modelEndpointStatus

The model endpoint's status in Amazon Fraud Detector.

Type: String

Valid Values: ASSOCIATED | DISSOCIATED

Required: Yes

modelSource

The source of the model.

Type: String

Valid Values: SAGEMAKER

Required: Yes

outputConfiguration

The model endpoint output configuration.

Type: [ModelOutputConfiguration](#) object

Required: Yes

tags

A collection of key and value pairs.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

PutKMSEncryptionKey

Specifies the KMS key to be used to encrypt content in Amazon Fraud Detector.

Request Syntax

```
{  
  "kmsEncryptionKeyArn": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

[kmsEncryptionKeyArn](#)

The KMS encryption key ARN.

The KMS key must be single-Region key. Amazon Fraud Detector does not support multi-Region KMS key.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 90.

Pattern: ^DEFAULT|arn:[a-zA-Z0-9-]+:kms:[a-zA-Z0-9-]+:\d{12}:key\\/\w{8}-\w{4}-\w{4}-\w{4}-\w{12}\$

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)

- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

PutLabel

Creates or updates label. A label classifies an event as fraudulent or legitimate. Labels are associated with event types and used to train supervised machine learning models in Amazon Fraud Detector.

Request Syntax

```
{
  "description": "string",
  "name": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

description

The label description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

name

The label name.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

[tags](#)

A collection of key and value pairs.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

PutOutcome

Creates or updates an outcome.

Request Syntax

```
{
  "description": "string",
  "name": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

description

The outcome description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

name

The name of the outcome.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

tags

A collection of key and value pairs.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

SendEvent

Stores events in Amazon Fraud Detector without generating fraud predictions for those events. For example, you can use SendEvent to upload a historical dataset, which you can then later use to train a model.

Request Syntax

```
{
  "assignedLabel": "string",
  "entities": [
    {
      "entityId": "string",
      "entityType": "string"
    }
  ],
  "eventId": "string",
  "eventTimestamp": "string",
  "eventName": "string",
  "eventVariables": {
    "string" : "string"
  },
  "labelTimestamp": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

assignedLabel

The label to associate with the event. Required if specifying labelTimestamp.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

entities

An array of entities.

Type: Array of [Entity](#) objects

Required: Yes

eventId

The event ID to upload.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

eventTimestamp

The timestamp that defines when the event under evaluation occurred. The timestamp must be specified using ISO 8601 standard in UTC.

Type: String

Length Constraints: Minimum length of 10. Maximum length of 30.

Required: Yes

eventTypeName

The event type name of the event.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

eventVariables

Names of the event type's variables you defined in Amazon Fraud Detector to represent data elements and their corresponding values for the event you are sending for evaluation.

Type: String to string map

Map Entries: Maximum number of items.

Key Length Constraints: Minimum length of 1. Maximum length of 64.

Value Length Constraints: Minimum length of 1. Maximum length of 8192.

Required: Yes

labelTimestamp

The timestamp associated with the label. Required if specifying assignedLabel.

Type: String

Length Constraints: Minimum length of 10. Maximum length of 30.

Required: No

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

TagResource

Assigns tags to a resource.

Request Syntax

```
{
  "resourceARN": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

resourceARN

The resource ARN.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:frauddetector\:[a-z0-9-]{3,20}\:[0-9]{12}\:[^\s]{2,128}$`

Required: Yes

tags

The tags to assign to the resource.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)

- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UntagResource

Removes tags from a resource.

Request Syntax

```
{  
  "resourceARN": "string",  
  "tagKeys": [ "string" ]  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

resourceARN

The ARN of the resource from which to remove the tag.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:frauddetector\:[a-z0-9-]{3,20}\:[0-9]{12}\:[^\s]{2,128}$`

Required: Yes

tagKeys

The resource ARN.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^(([\p{L}\p{Z}\p{N}_ . :/=+\-@]*)$`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)

- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UpdateDetectorVersion

Updates a detector version. The detector version attributes that you can update include models, external model endpoints, rules, rule execution mode, and description. You can only update a DRAFT detector version.

Request Syntax

```
{
  "description": "string",
  "detectorId": "string",
  "detectorVersionId": "string",
  "externalModelEndpoints": [ "string" ],
  "modelVersions": [
    {
      "arn": "string",
      "modelId": "string",
      "modelType": "string",
      "modelVersionNumber": "string"
    }
  ],
  "ruleExecutionMode": "string",
  "rules": [
    {
      "detectorId": "string",
      "ruleId": "string",
      "ruleVersion": "string"
    }
  ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

description

The detector version description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

detectorId

The parent detector ID for the detector version you want to update.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

detectorVersionId

The detector version ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 5.

Pattern: `^([1-9][0-9]*)$`

Required: Yes

externalModelEndpoints

The Amazon SageMaker model endpoints to include in the detector version.

Type: Array of strings

Required: Yes

modelVersions

The model versions to include in the detector version.

Type: Array of [ModelVersion](#) objects

Required: No

ruleExecutionMode

The rule execution mode to add to the detector.

If you specify `FIRST_MATCHED`, Amazon Fraud Detector evaluates rules sequentially, first to last, stopping at the first matched rule. Amazon Fraud detector then provides the outcomes for that single rule.

If you specify `ALL_MATCHED`, Amazon Fraud Detector evaluates all rules and returns the outcomes for all matched rules. You can define and edit the rule mode at the detector version level, when it is in draft status.

The default behavior is `FIRST_MATCHED`.

Type: String

Valid Values: `ALL_MATCHED` | `FIRST_MATCHED`

Required: No

rules

The rules to include in the detector version.

Type: Array of [Rule](#) objects

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerErrorException

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UpdateDetectorVersionMetadata

Updates the detector version's description. You can update the metadata for any detector version (DRAFT, ACTIVE, or INACTIVE).

Request Syntax

```
{  
  "description": "string",  
  "detectorId": "string",  
  "detectorVersionId": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

description

The description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: Yes

detectorId

The detector ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

detectorVersionId

The detector version ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 5.

Pattern: `^[1-9][0-9]*$`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UpdateDetectorVersionStatus

Updates the detector version's status. You can perform the following promotions or demotions using UpdateDetectorVersionStatus: DRAFT to ACTIVE, ACTIVE to INACTIVE, and INACTIVE to ACTIVE.

Request Syntax

```
{
  "detectorId": "string",
  "detectorVersionId": "string",
  "status": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

detectorId

The detector ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

detectorVersionId

The detector version ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 5.

Pattern: `^([1-9][0-9]*)$`

Required: Yes

status

The new status.

Type: String

Valid Values: ACTIVE | INACTIVE

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UpdateEventLabel

Updates the specified event with a new label.

Request Syntax

```
{
  "assignedLabel": "string",
  "eventId": "string",
  "eventName": "string",
  "labelTimestamp": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

assignedLabel

The new label to assign to the event.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

eventId

The ID of the event associated with the label to update.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

eventType

The event type of the event associated with the label to update.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

labelTimestamp

The timestamp associated with the label. The timestamp must be specified using ISO 8601 standard in UTC.

Type: String

Length Constraints: Minimum length of 10. Maximum length of 30.

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerErrorException

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UpdateList

Updates a list.

Request Syntax

```
{  
  "description": "string",  
  "elements": [ "string" ],  
  "name": "string",  
  "updateMode": "string",  
  "variableType": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

description

The new description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

elements

One or more list elements to add or replace. If you are providing the elements, make sure to specify the updateMode to use.

If you are deleting all elements from the list, use REPLACE for the updateMode and provide an empty list (0 elements).

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 100000 items.

Length Constraints: Minimum length of 1. Maximum length of 320.

Pattern: `^\S+(\S+)*$`

Required: No

name

The name of the list to update.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

Required: Yes

updateMode

The update mode (type).

- Use APPEND if you are adding elements to the list.
- Use REPLACE if you replacing existing elements in the list.
- Use REMOVE if you are removing elements from the list.

Type: String

Valid Values: REPLACE | APPEND | REMOVE

Required: No

variableType

The variable type you want to assign to the list.

Note

You cannot update a variable type of a list that already has a variable type assigned to it. You can assign a variable type to a list only if the list does not already have a variable type.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[A-Z_]{1,64}$`

Required: No

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UpdateModel

Updates model description.

Request Syntax

```
{  
  "description": "string",  
  "modelId": "string",  
  "modelType": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

description

The new model description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

modelId

The model ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

Required: Yes

modelType

The model type.

Type: String

Valid Values: ONLINE_FRAUD_INSIGHTS | TRANSACTION_FRAUD_INSIGHTS | ACCOUNT_TAKEOVER_INSIGHTS

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UpdateModelVersion

Updates a model version. Updating a model version retrains an existing model version using updated training data and produces a new minor version of the model. You can update the training data set location and data access role attributes using this action. This action creates and trains a new minor version of the model, for example version 1.01, 1.02, 1.03.

Request Syntax

```
{
  "externalEventsDetail": {
    "dataAccessRoleArn": "string",
    "dataLocation": "string"
  },
  "ingestedEventsDetail": {
    "ingestedEventsTimeWindow": {
      "endTime": "string",
      "startTime": "string"
    }
  },
  "majorVersionNumber": "string",
  "modelId": "string",
  "modelType": "string",
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

externalEventsDetail

The details of the external events data used for training the model version. Required if `trainingDataSource` is `EXTERNAL_EVENTS`.

Type: [ExternalEventsDetail](#) object

Required: No

[ingestedEventsDetail](#)

The details of the ingested event used for training the model version. Required if your `trainingDataSource` is `INGESTED_EVENTS`.

Type: [IngestedEventsDetail](#) object

Required: No

[majorVersionNumber](#)

The major version number.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 5.

Pattern: `^([1-9][0-9]*)$`

Required: Yes

[modelId](#)

The model ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

Required: Yes

[modelType](#)

The model type.

Type: String

Valid Values: `ONLINE_FRAUD_INSIGHTS` | `TRANSACTION_FRAUD_INSIGHTS` | `ACCOUNT_TAKEOVER_INSIGHTS`

Required: Yes

tags

A collection of key and value pairs.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

Response Syntax

```
{
  "modelId": "string",
  "modelType": "string",
  "modelVersionNumber": "string",
  "status": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

modelId

The model ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

modelType

The model type.

Type: String

Valid Values: ONLINE_FRAUD_INSIGHTS | TRANSACTION_FRAUD_INSIGHTS | ACCOUNT_TAKEOVER_INSIGHTS

modelVersionNumber

The model version number of the model version updated.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 7.

Pattern: `^[1-9][0-9]{0,3}\.[0-9]{1,2}$`

status

The status of the updated model version.

Type: String

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UpdateModelVersionStatus

Updates the status of a model version.

You can perform the following status updates:

1. Change the TRAINING_IN_PROGRESS status to TRAINING_CANCELLED.
2. Change the TRAINING_COMPLETE status to ACTIVE.
3. Change ACTIVE to INACTIVE.

Request Syntax

```
{  
  "modelId": "string",  
  "modelType": "string",  
  "modelVersionNumber": "string",  
  "status": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

modelId

The model ID of the model version to update.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

Required: Yes

modelType

The model type.

Type: String

Valid Values: ONLINE_FRAUD_INSIGHTS | TRANSACTION_FRAUD_INSIGHTS | ACCOUNT_TAKEOVER_INSIGHTS

Required: Yes

modelVersionNumber

The model version number.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 7.

Pattern: `^[1-9][0-9]{0,3}\.[0-9]{1,2}$`

Required: Yes

status

The model version status.

Type: String

Valid Values: ACTIVE | INACTIVE | TRAINING_CANCELLED

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerErrorException

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)

- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UpdateRuleMetadata

Updates a rule's metadata. The description attribute can be updated.

Request Syntax

```
{
  "description": "string",
  "rule": {
    "detectorId": "string",
    "ruleId": "string",
    "ruleVersion": "string"
  }
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

description

The rule description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: Yes

rule

The rule to update.

Type: [Rule](#) object

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UpdateRuleVersion

Updates a rule version resulting in a new rule version. Updates a rule version resulting in a new rule version (version 1, 2, 3 ...).

Request Syntax

```
{
  "description": "string",
  "expression": "string",
  "language": "string",
  "outcomes": [ "string" ],
  "rule": {
    "detectorId": "string",
    "ruleId": "string",
    "ruleVersion": "string"
  },
  "tags": [
    {
      "key": "string",
      "value": "string"
    }
  ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

description

The description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

expression

The rule expression.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Required: Yes

language

The language.

Type: String

Valid Values: DETECTORPL

Required: Yes

outcomes

The outcomes.

Type: Array of strings

Array Members: Minimum number of 1 item.

Required: Yes

rule

The rule to update.

Type: [Rule](#) object

Required: Yes

tags

The tags to assign to the rule version.

Type: Array of [Tag](#) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

Response Syntax

```
{
```

```
"rule": {  
  "detectorId": "string",  
  "ruleId": "string",  
  "ruleVersion": "string"  
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

rule

The new rule version that was created.

Type: [Rule](#) object

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UpdateVariable

Updates a variable.

Request Syntax

```
{  
  "defaultValue": "string",  
  "description": "string",  
  "name": "string",  
  "variableType": "string"  
}
```

Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

defaultValue

The new default value of the variable.

Type: String

Required: No

description

The new description.

Type: String

Required: No

name

The name of the variable.

Type: String

Required: Yes

variableType

The variable type. For more information see [Variable types](#).

Type: String

Required: No

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

AccessDeniedException

An exception indicating Amazon Fraud Detector does not have the needed permissions. This can occur if you submit a request, such as `PutExternalModel`, that specifies a role that is not in your account.

HTTP Status Code: 400

ConflictException

An exception indicating there was a conflict during a delete operation.

HTTP Status Code: 400

InternalServerError

An exception indicating an internal server error.

HTTP Status Code: 500

ResourceNotFoundException

An exception indicating the specified resource was not found.

HTTP Status Code: 400

ThrottlingException

An exception indicating a throttling error.

HTTP Status Code: 400

ValidationException

An exception indicating a specified value is not allowed.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET V4](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Data Types

The Amazon Fraud Detector API contains several data types that various actions use. This section describes each data type in detail.

Note

The order of each element in a data type structure is not guaranteed. Applications should not assume a particular order.

The following data types are supported:

- [AggregatedLogOddsMetric](#)
- [AggregatedVariablesImpactExplanation](#)
- [AggregatedVariablesImportanceMetrics](#)
- [AllowDenyList](#)
- [ATIMetricDataPoint](#)
- [ATIModelPerformance](#)
- [ATITrainingMetricsValue](#)
- [BatchCreateVariableError](#)
- [BatchGetVariableError](#)
- [BatchImport](#)
- [BatchPrediction](#)
- [DataValidationMetrics](#)
- [Detector](#)
- [DetectorVersionSummary](#)
- [Entity](#)
- [EntityType](#)
- [EvaluatedExternalModel](#)
- [EvaluatedModelVersion](#)
- [EvaluatedRule](#)
- [Event](#)

- [EventOrchestration](#)
- [EventPredictionSummary](#)
- [EventType](#)
- [EventVariableSummary](#)
- [ExternalEventsDetail](#)
- [ExternalModel](#)
- [ExternalModelOutputs](#)
- [ExternalModelSummary](#)
- [FieldValidationMessage](#)
- [FileValidationMessage](#)
- [FilterCondition](#)
- [IngestedEventsDetail](#)
- [IngestedEventStatistics](#)
- [IngestedEventsTimeWindow](#)
- [KMSKey](#)
- [Label](#)
- [LabelSchema](#)
- [LogOddsMetric](#)
- [MetricDataPoint](#)
- [Model](#)
- [ModelEndpointDataBlob](#)
- [ModelInputConfiguration](#)
- [ModelOutputConfiguration](#)
- [ModelScores](#)
- [ModelVersion](#)
- [ModelVersionDetail](#)
- [ModelVersionEvaluation](#)
- [OFIMetricDataPoint](#)
- [OFIModelPerformance](#)
- [OFITrainingMetricsValue](#)

- [Outcome](#)
- [PredictionExplanations](#)
- [PredictionTimeRange](#)
- [Rule](#)
- [RuleDetail](#)
- [RuleResult](#)
- [Tag](#)
- [TFIMetricDataPoint](#)
- [TFIModelPerformance](#)
- [TFITrainingMetricsValue](#)
- [TrainingDataSchema](#)
- [TrainingMetrics](#)
- [TrainingMetricsV2](#)
- [TrainingResult](#)
- [TrainingResultV2](#)
- [UncertaintyRange](#)
- [Variable](#)
- [VariableEntry](#)
- [VariableImpactExplanation](#)
- [VariableImportanceMetrics](#)

AggregatedLogOddsMetric

The log odds metric details.

Account Takeover Insights (ATI) model uses event variables from the login data you provide to continuously calculate a set of variables (aggregated variables) based on historical events. For example, your ATI model might calculate the number of times an user has logged in using the same IP address. In this case, event variables used to derive the aggregated variables are `IP address` and `user`.

Contents

`aggregatedVariablesImportance`

The relative importance of the variables in the list to the other event variable.

Type: Float

Required: Yes

`variableNames`

The names of all the variables.

Type: Array of strings

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

AggregatedVariablesImpactExplanation

The details of the impact of aggregated variables on the prediction score.

Account Takeover Insights (ATI) model uses the login data you provide to continuously calculate a set of variables (aggregated variables) based on historical events. For example, the model might calculate the number of times an user has logged in using the same IP address. In this case, event variables used to derive the aggregated variables are IP address and user.

Contents

eventVariableNames

The names of all the event variables that were used to derive the aggregated variables.

Type: Array of strings

Required: No

logOddsImpact

The raw, uninterpreted value represented as log-odds of the fraud. These values are usually between -10 to +10, but range from -infinity to +infinity.

- A positive value indicates that the variables drove the risk score up.
- A negative value indicates that the variables drove the risk score down.

Type: Float

Required: No

relativeImpact

The relative impact of the aggregated variables in terms of magnitude on the prediction scores.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

AggregatedVariablesImportanceMetrics

The details of the relative importance of the aggregated variables.

Account Takeover Insights (ATI) model uses event variables from the login data you provide to continuously calculate a set of variables (aggregated variables) based on historical events. For example, your ATI model might calculate the number of times an user has logged in using the same IP address. In this case, event variables used to derive the aggregated variables are IP address and user.

Contents

logOddsMetrics

List of variables' metrics.

Type: Array of [AggregatedLogOddsMetric](#) objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

AllowDenyList

The metadata of a list.

Contents

name

The name of the list.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

Required: Yes

arn

The ARN of the list.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:frauddetector\:[a-z0-9-]{3,20}\:[0-9]{12}\:[^\s]{2,128}$`

Required: No

createdTime

The time the list was created.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

description

The description of the list.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

updatedTime

The time the list was last updated.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

variableType

The variable type of the list.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[A-Z_]{1,64}$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ATIMetricDataPoint

The Account Takeover Insights (ATI) model performance metrics data points.

Contents

adr

The anomaly discovery rate. This metric quantifies the percentage of anomalies that can be detected by the model at the selected score threshold. A lower score threshold increases the percentage of anomalies captured by the model, but would also require challenging a larger percentage of login events, leading to a higher customer friction.

Type: Float

Required: No

atodr

The account takeover discovery rate. This metric quantifies the percentage of account compromise events that can be detected by the model at the selected score threshold. This metric is only available if 50 or more entities with at-least one labeled account takeover event is present in the ingested dataset.

Type: Float

Required: No

cr

The challenge rate. This indicates the percentage of login events that the model recommends to challenge such as one-time password, multi-factor authentication, and investigations.

Type: Float

Required: No

threshold

The model's threshold that specifies an acceptable fraud capture rate. For example, a threshold of 500 means any model score 500 or above is labeled as fraud.

Type: Float

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ATIModelPerformance

The Account Takeover Insights (ATI) model performance score.

Contents

asi

The anomaly separation index (ASI) score. This metric summarizes the overall ability of the model to separate anomalous activities from the normal behavior. Depending on the business, a large fraction of these anomalous activities can be malicious and correspond to the account takeover attacks. A model with no separability power will have the lowest possible ASI score of 0.5, whereas the a model with a high separability power will have the highest possible ASI score of 1.0

Type: Float

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ATITrainingMetricsValue

The Account Takeover Insights (ATI) model training metric details.

Contents

metricDataPoints

The model's performance metrics data points.

Type: Array of [ATIMetricDataPoint](#) objects

Required: No

modelPerformance

The model's overall performance scores.

Type: [ATIModelPerformance](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

BatchCreateVariableError

Provides the error of the batch create variable API.

Contents

code

The error code.

Type: Integer

Required: No

message

The error message.

Type: String

Required: No

name

The name.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

BatchGetVariableError

Provides the error of the batch get variable API.

Contents

code

The error code.

Type: Integer

Required: No

message

The error message.

Type: String

Required: No

name

The error name.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

BatchImport

The batch import job details.

Contents

arn

The ARN of the batch import job.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:frauddetector\:[a-z0-9-]{3,20}\:[0-9]{12}\:[^\s]{2,128}$`

Required: No

completionTime

Timestamp of when batch import job completed.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

eventName

The name of the event type.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

failedRecordsCount

The number of records that failed to import.

Type: Integer

Required: No

failureReason

The reason batch import job failed.

Type: String

Required: No

iamRoleArn

The ARN of the IAM role to use for this job request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:iam\:\:[0-9]{12}\:role\/[^\s]{2,64}$`

Required: No

inputPath

The Amazon S3 location of your data file for batch import.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `^s3:\:\/\/(.+)\$`

Required: No

jobId

The ID of the batch import job.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+\$`

Required: No

outputPath

The Amazon S3 location of your output file.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `^s3:\V\(.+)\$`

Required: No

processedRecordsCount

The number of records processed by batch import job.

Type: Integer

Required: No

startTime

Timestamp of when the batch import job started.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

status

The status of the batch import job.

Type: String

Valid Values: `IN_PROGRESS_INITIALIZING | IN_PROGRESS | CANCEL_IN_PROGRESS | CANCELED | COMPLETE | FAILED`

Required: No

totalRecordsCount

The total number of records in the batch import job.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

BatchPrediction

The batch prediction details.

Contents

arn

The ARN of batch prediction job.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:frauddetector\[a-z0-9-]{3,20}\:[0-9]{12}\:[^\s]{2,128}$`

Required: No

completionTime

Timestamp of when the batch prediction job completed.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

detectorName

The name of the detector.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

detectorVersion

The detector version.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 7.

Pattern: `^[1-9][0-9]{0,3}\.[0-9]{1,2}$`

Required: No

eventTypeName

The name of the event type.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

failureReason

The reason a batch prediction job failed.

Type: String

Required: No

iamRoleArn

The ARN of the IAM role to use for this job request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:iam\:\:[0-9]{12}\:role\/[^\s]{2,64}$`

Required: No

inputPath

The Amazon S3 location of your training file.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `^s3:\V\(.+)\$`

Required: No

jobId

The job ID for the batch prediction.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+\$`

Required: No

lastHeartbeatTime

Timestamp of most recent heartbeat indicating the batch prediction job was making progress.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

outputPath

The Amazon S3 location of your output file.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `^s3:\V\(.+)\$`

Required: No

processedRecordsCount

The number of records processed by the batch prediction job.

Type: Integer

Required: No

startTime

Timestamp of when the batch prediction job started.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

status

The batch prediction status.

Type: String

Valid Values: IN_PROGRESS_INITIALIZING | IN_PROGRESS | CANCEL_IN_PROGRESS | CANCELED | COMPLETE | FAILED

Required: No

totalRecordsCount

The total number of records in the batch prediction job.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

DataValidationMetrics

The model training data validation metrics.

Contents

fieldLevelMessages

The field-specific model training validation messages.

Type: Array of [FieldValidationMessage](#) objects

Required: No

fileLevelMessages

The file-specific model training data validation messages.

Type: Array of [FileValidationMessage](#) objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Detector

The detector.

Contents

arn

The detector ARN.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:frauddetector\[a-z0-9-]{3,20}\:[0-9]{12}\:[^\s]{2,128}$`

Required: No

createdTime

Timestamp of when the detector was created.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

description

The detector description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

detectorId

The detector ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

eventName

The name of the event type.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

lastUpdatedTime

Timestamp of when the detector was last updated.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

DetectorVersionSummary

The summary of the detector version.

Contents

description

The detector version description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

detectorVersionId

The detector version ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 5.

Pattern: `^[1-9][0-9]*$`

Required: No

lastUpdatedTime

Timestamp of when the detector version was last updated.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

status

The detector version status.

Type: String

Valid Values: DRAFT | ACTIVE | INACTIVE

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Entity

The entity details.

Contents

entityId

The entity ID. If you do not know the `entityId`, you can pass `unknown`, which is a reserved string literal.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^[0-9A-Za-z_@+-]+$`

Required: Yes

entityType

The entity type.

Type: String

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

EntityType

The entity type details.

Contents

arn

The entity type ARN.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:frauddetector\:[a-z0-9-]{3,20}\:[0-9]{12}\:[^\s]{2,128}$`

Required: No

createdTime

Timestamp of when the entity type was created.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

description

The entity type description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

lastUpdatedTime

Timestamp of when the entity type was last updated.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

name

The entity type name.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

EvaluatedExternalModel

The details of the external (Amazon Sagemaker) model evaluated for generating predictions.

Contents

inputVariables

Input variables use for generating predictions.

Type: String to string map

Required: No

modelEndpoint

The endpoint of the external (Amazon Sagemaker) model.

Type: String

Required: No

outputVariables

Output variables.

Type: String to string map

Required: No

useEventVariables

Indicates whether event variables were used to generate predictions.

Type: Boolean

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

EvaluatedModelVersion

The model version evaluated for generating prediction.

Contents

evaluations

Evaluations generated for the model version.

Type: Array of [ModelVersionEvaluation](#) objects

Required: No

modelId

The model ID.

Type: String

Required: No

modelType

The model type.

Valid values: ONLINE_FRAUD_INSIGHTS | TRANSACTION_FRAUD_INSIGHTS

Type: String

Required: No

modelVersion

The model version.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

EvaluatedRule

The details of the rule used for evaluating variable values.

Contents

evaluated

Indicates whether the rule was evaluated.

Type: Boolean

Required: No

expression

The rule expression.

Type: String

Required: No

expressionWithValues

The rule expression value.

Type: String

Required: No

matched

Indicates whether the rule matched.

Type: Boolean

Required: No

outcomes

The rule outcome.

Type: Array of strings

Required: No

ruleId

The rule ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

ruleVersion

The rule version.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 5.

Pattern: `^[1-9][0-9]*$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Event

The event details.

Contents

currentLabel

The label associated with the event.

Type: String

Required: No

entities

The event entities.

Type: Array of [Entity](#) objects

Required: No

eventId

The event ID.

Type: String

Required: No

eventTimestamp

The timestamp that defines when the event under evaluation occurred. The timestamp must be specified using ISO 8601 standard in UTC.

Type: String

Required: No

eventName

The event type.

Type: String

Required: No

eventVariables

Names of the event type's variables you defined in Amazon Fraud Detector to represent data elements and their corresponding values for the event you are sending for evaluation.

Type: String to string map

Key Length Constraints: Minimum length of 1. Maximum length of 64.

Value Length Constraints: Minimum length of 1. Maximum length of 256.

Required: No

labelTimestamp

The timestamp associated with the label to update. The timestamp must be specified using ISO 8601 standard in UTC.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

EventOrchestration

The event orchestration status.

Contents

eventBridgeEnabled

Specifies if event orchestration is enabled through Amazon EventBridge.

Type: Boolean

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

EventPredictionSummary

Information about the summary of an event prediction.

Contents

detectorId

The detector ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

detectorVersionId

The detector version ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 5.

Pattern: `^([1-9][0-9]*)$`

Required: No

eventId

The event ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

eventTimestamp

The timestamp of the event.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

eventName

The event type.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

predictionTimestamp

The timestamp when the prediction was generated.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

EventType

The event type details.

Contents

arn

The entity type ARN.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:frauddetector\[a-z0-9-]{3,20}\:[0-9]{12}\:[^\s]{2,128}$`

Required: No

createdTime

Timestamp of when the event type was created.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

description

The event type description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

entityTypes

The event type entity types.

Type: Array of strings

Array Members: Minimum number of 1 item.

Required: No

eventIngestion

If Enabled, Amazon Fraud Detector stores event data when you generate a prediction and uses that data to update calculated variables in near real-time. Amazon Fraud Detector uses this data, known as `INGESTED_EVENTS`, to train your model and improve fraud predictions.

Type: String

Valid Values: ENABLED | DISABLED

Required: No

eventOrchestration

The event orchestration status.

Type: [EventOrchestration](#) object

Required: No

eventVariables

The event type event variables.

Type: Array of strings

Required: No

ingestedEventStatistics

Data about the stored events.

Type: [IngestedEventStatistics](#) object

Required: No

labels

The event type labels.

Type: Array of strings

Required: No

lastUpdatedTime

Timestamp of when the event type was last updated.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

name

The event type name.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

EventVariableSummary

Information about the summary of an event variable that was evaluated for generating prediction.

Contents

name

The event variable name.

Type: String

Required: No

source

The event variable source.

Type: String

Required: No

value

The value of the event variable.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ExternalEventsDetail

Details for the external events data used for model version training.

Contents

dataAccessRoleArn

The ARN of the role that provides Amazon Fraud Detector access to the data location.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:iam\:\:[0-9]{12}\:role\/[^\s]{2,64}$`

Required: Yes

dataLocation

The Amazon S3 bucket location for the data.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 512.

Pattern: `^s3:\/\/(.\+)$`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ExternalModel

The Amazon SageMaker model.

Contents

arn

The model ARN.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:frauddetector\:[a-z0-9-]{3,20}\:[0-9]{12}\:[^\s]{2,128}$`

Required: No

createdTime

Timestamp of when the model was last created.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

inputConfiguration

The input configuration.

Type: [ModelInputConfiguration](#) object

Required: No

invokeModelEndpointRoleArn

The role used to invoke the model.

Type: String

Required: No

lastUpdatedTime

Timestamp of when the model was last updated.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

modelEndpoint

The Amazon SageMaker model endpoints.

Type: String

Required: No

modelEndpointStatus

The Amazon Fraud Detector status for the external model endpoint

Type: String

Valid Values: ASSOCIATED | DISSOCIATED

Required: No

modelSource

The source of the model.

Type: String

Valid Values: SAGEMAKER

Required: No

outputConfiguration

The output configuration.

Type: [ModelOutputConfiguration](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ExternalModelOutputs

The fraud prediction scores from Amazon SageMaker model.

Contents

externalModel

The Amazon SageMaker model.

Type: [ExternalModelSummary](#) object

Required: No

outputs

The fraud prediction scores from Amazon SageMaker model.

Type: String to string map

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ExternalModelSummary

The Amazon SageMaker model.

Contents

modelEndpoint

The endpoint of the Amazon SageMaker model.

Type: String

Required: No

modelSource

The source of the model.

Type: String

Valid Values: SAGEMAKER

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

FieldValidationMessage

The message details.

Contents

content

The message content.

Type: String

Required: No

fieldName

The field name.

Type: String

Required: No

identifier

The message ID.

Type: String

Required: No

title

The message title.

Type: String

Required: No

type

The message type.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

FileValidationMessage

The message details.

Contents

content

The message content.

Type: String

Required: No

title

The message title.

Type: String

Required: No

type

The message type.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

FilterCondition

A conditional statement for filtering a list of past predictions.

Contents

value

A statement containing a resource property and a value to specify filter condition.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^[0-9A-Za-z_-]+$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

IngestedEventsDetail

The details of the ingested event.

Contents

ingestedEventsTimeWindow

The start and stop time of the ingested events.

Type: [IngestedEventsTimeWindow](#) object

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

IngestedEventStatistics

Data about the stored events.

Contents

eventDataSizeInBytes

The total size of the stored events.

Type: Long

Required: No

lastUpdatedTime

Timestamp of when the stored event was last updated.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

leastRecentEvent

The oldest stored event.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

mostRecentEvent

The newest stored event.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

numberOfEvents

The number of stored events.

Type: Long

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

IngestedEventsTimeWindow

The start and stop time of the ingested events.

Contents

endTime

Timestamp of the final ingested event.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: Yes

startTime

Timestamp of the first ingested event.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

KMSKey

The KMS key details.

Contents

kmsEncryptionKeyArn

The encryption key ARN.

Type: String

Length Constraints: Minimum length of 7. Maximum length of 90.

Pattern: `^DEFAULT|arn:[a-zA-Z0-9-]+:kms:[a-zA-Z0-9-]+:\d{12}:key\w{8}-\w{4}-\w{4}-\w{4}-\w{12}$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Label

The label details.

Contents

arn

The label ARN.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:frauddetector\:[a-z0-9-]{3,20}\:[0-9]{12}\:[^\s]{2,128}$`

Required: No

createdTime

Timestamp of when the event type was created.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

description

The label description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

lastUpdatedTime

Timestamp of when the label was last updated.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

name

The label name.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

LabelSchema

The label schema.

Contents

labelMapper

The label mapper maps the Amazon Fraud Detector supported model classification labels (FRAUD, LEGIT) to the appropriate event type labels. For example, if "FRAUD" and "LEGIT" are Amazon Fraud Detector supported labels, this mapper could be: {"FRAUD" => ["0"], "LEGIT" => ["1"]} or {"FRAUD" => ["false"], "LEGIT" => ["true"]} or {"FRAUD" => ["fraud", "abuse"], "LEGIT" => ["legit", "safe"]}. The value part of the mapper is a list, because you may have multiple label variants from your event type for a single Amazon Fraud Detector label.

Type: String to array of strings map

Required: No

unlabeledEventsTreatment

The action to take for unlabeled events.

- Use IGNORE if you want the unlabeled events to be ignored. This is recommended when the majority of the events in the dataset are labeled.
- Use FRAUD if you want to categorize all unlabeled events as "Fraud". This is recommended when most of the events in your dataset are fraudulent.
- Use LEGIT if you want to categorize all unlabeled events as "Legit". This is recommended when most of the events in your dataset are legitimate.
- Use AUTO if you want Amazon Fraud Detector to decide how to use the unlabeled data. This is recommended when there is significant unlabeled events in the dataset.

By default, Amazon Fraud Detector ignores the unlabeled data.

Type: String

Valid Values: IGNORE | FRAUD | LEGIT | AUTO

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

LogOddsMetric

The log odds metric details.

Contents

variableImportance

The relative importance of the variable. For more information, see [Model variable importance](#).

Type: Float

Required: Yes

variableName

The name of the variable.

Type: String

Required: Yes

variableType

The type of variable.

Type: String

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

MetricDataPoint

Model performance metrics data points.

Contents

fpr

The false positive rate. This is the percentage of total legitimate events that are incorrectly predicted as fraud.

Type: Float

Required: No

precision

The percentage of fraud events correctly predicted as fraudulent as compared to all events predicted as fraudulent.

Type: Float

Required: No

threshold

The model threshold that specifies an acceptable fraud capture rate. For example, a threshold of 500 means any model score 500 or above is labeled as fraud.

Type: Float

Required: No

tpr

The true positive rate. This is the percentage of total fraud the model detects. Also known as capture rate.

Type: Float

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Model

The model.

Contents

arn

The ARN of the model.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:frauddetector\:[a-z0-9-]{3,20}\:[0-9]{12}\:[^\s]{2,128}$`

Required: No

createdTime

Timestamp of when the model was created.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

description

The model description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

eventName

The name of the event type.

Type: String

Required: No

lastUpdatedTime

Timestamp of last time the model was updated.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

modelId

The model ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

Required: No

modelType

The model type.

Type: String

Valid Values: ONLINE_FRAUD_INSIGHTS | TRANSACTION_FRAUD_INSIGHTS | ACCOUNT_TAKEOVER_INSIGHTS

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ModelEndpointDataBlob

A pre-formed Amazon SageMaker model input you can include if your detector version includes an imported Amazon SageMaker model endpoint with pass-through input configuration.

Contents

byteBuffer

The byte buffer of the Amazon SageMaker model endpoint input data blob.

Type: Base64-encoded binary data object

Required: No

contentType

The content type of the Amazon SageMaker model endpoint input data blob.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ModelInputConfiguration

The Amazon SageMaker model input configuration.

Contents

useEventVariables

The event variables.

Type: Boolean

Required: Yes

csvInputTemplate

Template for constructing the CSV input-data sent to SageMaker. At event-evaluation, the placeholders for variable-names in the template will be replaced with the variable values before being sent to SageMaker.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2000.

Required: No

eventTypeName

The event type name.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

format

The format of the model input configuration. The format differs depending on if it is passed through to SageMaker or constructed by Amazon Fraud Detector.

Type: String

Valid Values: TEXT_CSV | APPLICATION_JSON

Required: No

jsonInputTemplate

Template for constructing the JSON input-data sent to SageMaker. At event-evaluation, the placeholders for variable names in the template will be replaced with the variable values before being sent to SageMaker.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2000.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ModelOutputConfiguration

Provides the Amazon SageMaker model output configuration.

Contents

format

The format of the model output configuration.

Type: String

Valid Values: TEXT_CSV | APPLICATION_JSONLINES

Required: Yes

csvIndexToVariableMap

A map of CSV index values in the SageMaker response to the Amazon Fraud Detector variables.

Type: String to string map

Required: No

jsonKeyToVariableMap

A map of JSON keys in response from SageMaker to the Amazon Fraud Detector variables.

Type: String to string map

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ModelScores

The fraud prediction scores.

Contents

modelVersion

The model version.

Type: [ModelVersion](#) object

Required: No

scores

The model's fraud prediction scores.

Type: String to float map

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ModelVersion

The model version.

Contents

modelId

The model ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

Required: Yes

modelType

The model type.

Type: String

Valid Values: ONLINE_FRAUD_INSIGHTS | TRANSACTION_FRAUD_INSIGHTS | ACCOUNT_TAKEOVER_INSIGHTS

Required: Yes

modelVersionNumber

The model version number.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 7.

Pattern: `^[1-9][0-9]{0,3}\.[0-9]{1,2}$`

Required: Yes

arn

The model version ARN.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:frauddetector\:[a-z0-9-]{3,20}\:[0-9]{12}\:[^\s]{2,128}$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ModelVersionDetail

The details of the model version.

Contents

arn

The model version ARN.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:frauddetector\:[a-z0-9-]{3,20}\:[0-9]{12}\:[^\s]{2,128}$`

Required: No

createdTime

The timestamp when the model was created.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

externalEventsDetail

The external events data details. This will be populated if the `trainingDataSource` for the model version is specified as `EXTERNAL_EVENTS`.

Type: [ExternalEventsDetail](#) object

Required: No

ingestedEventsDetail

The ingested events data details. This will be populated if the `trainingDataSource` for the model version is specified as `INGESTED_EVENTS`.

Type: [IngestedEventsDetail](#) object

Required: No

lastUpdatedTime

The timestamp when the model was last updated.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

modelId

The model ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_]+$`

Required: No

modelType

The model type.

Type: String

Valid Values: ONLINE_FRAUD_INSIGHTS | TRANSACTION_FRAUD_INSIGHTS | ACCOUNT_TAKEOVER_INSIGHTS

Required: No

modelVersionNumber

The model version number.

Type: String

Length Constraints: Minimum length of 3. Maximum length of 7.

Pattern: `^[1-9][0-9]{0,3}\.[0-9]{1,2}$`

Required: No

status

The status of the model version.

Type: String

Required: No

trainingDataSchema

The training data schema.

Type: [TrainingDataSchema](#) object

Required: No

trainingDataSource

The model version training data source.

Type: String

Valid Values: EXTERNAL_EVENTS | INGESTED_EVENTS

Required: No

trainingResult

The training results.

Type: [TrainingResult](#) object

Required: No

trainingResultV2

The training result details. The details include the relative importance of the variables.

Type: [TrainingResultV2](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ModelVersionEvaluation

The model version evaluations.

Contents

evaluationScore

The evaluation score generated for the model version.

Type: String

Required: No

outputVariableName

The output variable name.

Type: String

Required: No

predictionExplanations

The prediction explanations generated for the model version.

Type: [PredictionExplanations](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

OFIMetricDataPoint

The Online Fraud Insights (OFI) model performance metrics data points.

Contents

fpr

The false positive rate. This is the percentage of total legitimate events that are incorrectly predicted as fraud.

Type: Float

Required: No

precision

The percentage of fraud events correctly predicted as fraudulent as compared to all events predicted as fraudulent.

Type: Float

Required: No

threshold

The model threshold that specifies an acceptable fraud capture rate. For example, a threshold of 500 means any model score 500 or above is labeled as fraud.

Type: Float

Required: No

tpr

The true positive rate. This is the percentage of total fraud the model detects. Also known as capture rate.

Type: Float

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

OFIModelPerformance

The Online Fraud Insights (OFI) model performance score.

Contents

auc

The area under the curve (auc). This summarizes the total positive rate (tpr) and false positive rate (FPR) across all possible model score thresholds.

Type: Float

Required: No

uncertaintyRange

Indicates the range of area under curve (auc) expected from the OFI model. A range greater than 0.1 indicates higher model uncertainty.

Type: [UncertaintyRange](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

OFITrainingMetricsValue

The Online Fraud Insights (OFI) model training metric details.

Contents

metricDataPoints

The model's performance metrics data points.

Type: Array of [OFIMetricDataPoint](#) objects

Required: No

modelPerformance

The model's overall performance score.

Type: [OFIModelPerformance](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Outcome

The outcome.

Contents

arn

The outcome ARN.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:frauddetector\[a-z0-9-]{3,20}\:[0-9]{12}\:[^\s]{2,128}$`

Required: No

createdTime

The timestamp when the outcome was created.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

description

The outcome description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

lastUpdatedTime

The timestamp when the outcome was last updated.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

name

The outcome name.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

PredictionExplanations

The prediction explanations that provide insight into how each event variable impacted the model version's fraud prediction score.

Contents

aggregatedVariablesImpactExplanations

The details of the aggregated variables impact on the prediction score.

Account Takeover Insights (ATI) model uses event variables from the login data you provide to continuously calculate a set of variables (aggregated variables) based on historical events. For example, your ATI model might calculate the number of times an user has logged in using the same IP address. In this case, event variables used to derive the aggregated variables are IP address and user.

Type: Array of [AggregatedVariablesImpactExplanation](#) objects

Required: No

variableImpactExplanations

The details of the event variable's impact on the prediction score.

Type: Array of [VariableImpactExplanation](#) objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

PredictionTimeRange

The time period for when the predictions were generated.

Contents

endTime

The end time of the time period for when the predictions were generated.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: Yes

startTime

The start time of the time period for when the predictions were generated.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Rule

A rule.

Contents

detectorId

The detector for which the rule is associated.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

ruleId

The rule ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: Yes

ruleVersion

The rule version.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 5.

Pattern: `^([1-9][0-9]*)$`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

RuleDetail

The details of the rule.

Contents

arn

The rule ARN.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:frauddetector\[a-z0-9-]{3,20}\:[0-9]{12}\:[^\s]{2,128}$`

Required: No

createdTime

The timestamp of when the rule was created.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

description

The rule description.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Required: No

detectorId

The detector for which the rule is associated.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

expression

The rule expression.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Required: No

language

The rule language.

Type: String

Valid Values: DETECTORPL

Required: No

lastUpdatedTime

Timestamp of the last time the rule was updated.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

outcomes

The rule outcomes.

Type: Array of strings

Array Members: Minimum number of 1 item.

Required: No

ruleId

The rule ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `^[0-9a-z_-]+$`

Required: No

ruleVersion

The rule version.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 5.

Pattern: `^[1-9][0-9]*$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

RuleResult

The rule results.

Contents

outcomes

The outcomes of the matched rule, based on the rule execution mode.

Type: Array of strings

Required: No

ruleId

The rule ID that was matched, based on the rule execution mode.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Tag

A key and value pair.

Contents

key

A tag key.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^([\p{L}\p{Z}\p{N}_ . :/=+\-@]*)$`

Required: Yes

value

A value assigned to a tag key.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TFIMetricDataPoint

The performance metrics data points for Transaction Fraud Insights (TFI) model.

Contents

fpr

The false positive rate. This is the percentage of total legitimate events that are incorrectly predicted as fraud.

Type: Float

Required: No

precision

The percentage of fraud events correctly predicted as fraudulent as compared to all events predicted as fraudulent.

Type: Float

Required: No

threshold

The model threshold that specifies an acceptable fraud capture rate. For example, a threshold of 500 means any model score 500 or above is labeled as fraud.

Type: Float

Required: No

tpr

The true positive rate. This is the percentage of total fraud the model detects. Also known as capture rate.

Type: Float

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TFIModelPerformance

The Transaction Fraud Insights (TFI) model performance score.

Contents

auc

The area under the curve (auc). This summarizes the total positive rate (tpr) and false positive rate (FPR) across all possible model score thresholds.

Type: Float

Required: No

uncertaintyRange

Indicates the range of area under curve (auc) expected from the TFI model. A range greater than 0.1 indicates higher model uncertainty.

Type: [UncertaintyRange](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TFITrainingMetricsValue

The Transaction Fraud Insights (TFI) model training metric details.

Contents

metricDataPoints

The model's performance metrics data points.

Type: Array of [TFIMetricDataPoint](#) objects

Required: No

modelPerformance

The model performance score.

Type: [TFIModelPerformance](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TrainingDataSchema

The training data schema.

Contents

modelVariables

The training data schema variables.

Type: Array of strings

Required: Yes

labelSchema

The label schema.

Type: [LabelSchema](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TrainingMetrics

The training metric details.

Contents

auc

The area under the curve. This summarizes true positive rate (TPR) and false positive rate (FPR) across all possible model score thresholds. A model with no predictive power has an AUC of 0.5, whereas a perfect model has a score of 1.0.

Type: Float

Required: No

metricDataPoints

The data points details.

Type: Array of [MetricDataPoint](#) objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TrainingMetricsV2

The training metrics details.

Contents

ati

The Account Takeover Insights (ATI) model training metric details.

Type: [ATITrainingMetricsValue](#) object

Required: No

ofi

The Online Fraud Insights (OFI) model training metric details.

Type: [OFITrainingMetricsValue](#) object

Required: No

tfi

The Transaction Fraud Insights (TFI) model training metric details.

Type: [TFITrainingMetricsValue](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TrainingResult

The training result details.

Contents

dataValidationMetrics

The validation metrics.

Type: [DataValidationMetrics](#) object

Required: No

trainingMetrics

The training metric details.

Type: [TrainingMetrics](#) object

Required: No

variableImportanceMetrics

The variable importance metrics.

Type: [VariableImportanceMetrics](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

TrainingResultV2

The training result details.

Contents

aggregatedVariablesImportanceMetrics

The variable importance metrics of the aggregated variables.

Account Takeover Insights (ATI) model uses event variables from the login data you provide to continuously calculate a set of variables (aggregated variables) based on historical events. For example, your ATI model might calculate the number of times an user has logged in using the same IP address. In this case, event variables used to derive the aggregated variables are IP address and user.

Type: [AggregatedVariablesImportanceMetrics](#) object

Required: No

dataValidationMetrics

The model training data validation metrics.

Type: [DataValidationMetrics](#) object

Required: No

trainingMetricsV2

The training metric details.

Type: [TrainingMetricsV2](#) object

Required: No

variableImportanceMetrics

The variable importance metrics details.

Type: [VariableImportanceMetrics](#) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

UncertaintyRange

Range of area under curve (auc) expected from the model. A range greater than 0.1 indicates higher model uncertainty. A range is the difference between upper and lower bound of auc.

Contents

lowerBoundValue

The lower bound value of the area under curve (auc).

Type: Float

Required: Yes

upperBoundValue

The upper bound value of the area under curve (auc).

Type: Float

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Variable

The variable.

Contents

arn

The ARN of the variable.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn\:aws[a-z-]{0,15}\:frauddetector\:[a-z0-9-]{3,20}\:[0-9]{12}\:[^\s]{2,128}$`

Required: No

createdTime

The time when the variable was created.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

dataSource

The data source of the variable.

Type: String

Valid Values: EVENT | MODEL_SCORE | EXTERNAL_MODEL_SCORE

Required: No

dataType

The data type of the variable. For more information see [Variable types](#).

Type: String

Valid Values: STRING | INTEGER | FLOAT | BOOLEAN | DATETIME

Required: No

defaultValue

The default value of the variable.

Type: String

Required: No

description

The description of the variable.

Type: String

Required: No

lastUpdatedTime

The time when variable was last updated.

Type: String

Length Constraints: Minimum length of 11. Maximum length of 30.

Required: No

name

The name of the variable.

Type: String

Required: No

variableType

The variable type of the variable.

Valid Values: AUTH_CODE | AVS | BILLING_ADDRESS_L1 | BILLING_ADDRESS_L2
| BILLING_CITY | BILLING_COUNTRY | BILLING_NAME | BILLING_PHONE |
BILLING_STATE | BILLING_ZIP | CARD_BIN | CATEGORICAL | CURRENCY_CODE
| EMAIL_ADDRESS | FINGERPRINT | FRAUD_LABEL | FREE_FORM_TEXT |

IP_ADDRESS | NUMERIC | ORDER_ID | PAYMENT_TYPE | PHONE_NUMBER | PRICE
| PRODUCT_CATEGORY | SHIPPING_ADDRESS_L1 | SHIPPING_ADDRESS_L2 |
SHIPPING_CITY | SHIPPING_COUNTRY | SHIPPING_NAME | SHIPPING_PHONE |
SHIPPING_STATE | SHIPPING_ZIP | USERAGENT

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

VariableEntry

A variable in the list of variables for the batch create variable request.

Contents

dataSource

The data source of the variable.

Type: String

Required: No

dataType

The data type of the variable.

Type: String

Required: No

defaultValue

The default value of the variable.

Type: String

Required: No

description

The description of the variable.

Type: String

Required: No

name

The name of the variable.

Type: String

Required: No

variableType

The type of the variable. For more information see [Variable types](#).

Valid Values: AUTH_CODE | AVS | BILLING_ADDRESS_L1 | BILLING_ADDRESS_L2 | BILLING_CITY | BILLING_COUNTRY | BILLING_NAME | BILLING_PHONE | BILLING_STATE | BILLING_ZIP | CARD_BIN | CATEGORICAL | CURRENCY_CODE | EMAIL_ADDRESS | FINGERPRINT | FRAUD_LABEL | FREE_FORM_TEXT | IP_ADDRESS | NUMERIC | ORDER_ID | PAYMENT_TYPE | PHONE_NUMBER | PRICE | PRODUCT_CATEGORY | SHIPPING_ADDRESS_L1 | SHIPPING_ADDRESS_L2 | SHIPPING_CITY | SHIPPING_COUNTRY | SHIPPING_NAME | SHIPPING_PHONE | SHIPPING_STATE | SHIPPING_ZIP | USERAGENT

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

VariableImpactExplanation

The details of the event variable's impact on the prediction score.

Contents

eventVariableName

The event variable name.

Type: String

Required: No

logOddsImpact

The raw, uninterpreted value represented as log-odds of the fraud. These values are usually between -10 to +10, but range from - infinity to + infinity.

- A positive value indicates that the variable drove the risk score up.
- A negative value indicates that the variable drove the risk score down.

Type: Float

Required: No

relativeImpact

The event variable's relative impact in terms of magnitude on the prediction scores. The relative impact values consist of a numerical rating (0-5, 5 being the highest) and direction (increased/decreased) impact of the fraud risk.

Type: String

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

VariableImportanceMetrics

The variable importance metrics details.

Contents

logOddsMetrics

List of variable metrics.

Type: Array of [LogOddsMetric](#) objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Common Parameters

The following list contains the parameters that all actions use for signing Signature Version 4 requests with a query string. Any action-specific parameters are listed in the topic for that action. For more information about Signature Version 4, see [Signing AWS API requests](#) in the *IAM User Guide*.

Action

The action to be performed.

Type: string

Required: Yes

Version

The API version that the request is written for, expressed in the format YYYY-MM-DD.

Type: string

Required: Yes

X-Amz-Algorithm

The hash algorithm that you used to create the request signature.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Valid Values: AWS4-HMAC-SHA256

Required: Conditional

X-Amz-Credential

The credential scope value, which is a string that includes your access key, the date, the region you are targeting, the service you are requesting, and a termination string ("aws4_request"). The value is expressed in the following format: *access_key/YYYYMMDD/region/service/aws4_request*.

For more information, see [Create a signed AWS API request](#) in the *IAM User Guide*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-Date

The date that is used to create the signature. The format must be ISO 8601 basic format (YYYYMMDD'T'HHMMSS'Z'). For example, the following date time is a valid X-Amz-Date value: 20120325T120000Z.

Condition: X-Amz-Date is optional for all requests; it can be used to override the date used for signing requests. If the Date header is specified in the ISO 8601 basic format, X-Amz-Date is not required. When X-Amz-Date is used, it always overrides the value of the Date header. For more information, see [Elements of an AWS API request signature](#) in the *IAM User Guide*.

Type: string

Required: Conditional

X-Amz-Security-Token

The temporary security token that was obtained through a call to AWS Security Token Service (AWS STS). For a list of services that support temporary security credentials from AWS STS, see [AWS services that work with IAM](#) in the *IAM User Guide*.

Condition: If you're using temporary security credentials from AWS STS, you must include the security token.

Type: string

Required: Conditional

X-Amz-Signature

Specifies the hex-encoded signature that was calculated from the string to sign and the derived signing key.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-SignedHeaders

Specifies all the HTTP headers that were included as part of the canonical request. For more information about specifying signed headers, see [Create a signed AWS API request](#) in the *IAM User Guide*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

Common Errors

This section lists the errors common to the API actions of all AWS services. For errors specific to an API action for this service, see the topic for that API action.

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 400

IncompleteSignature

The request signature does not conform to AWS standards.

HTTP Status Code: 400

InternalFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

InvalidAction

The action or operation requested is invalid. Verify that the action is typed correctly.

HTTP Status Code: 400

InvalidClientTokenId

The X.509 certificate or AWS access key ID provided does not exist in our records.

HTTP Status Code: 403

NotAuthorized

You do not have permission to perform this action.

HTTP Status Code: 400

OptInRequired

The AWS access key ID needs a subscription for the service.

HTTP Status Code: 403

RequestExpired

The request reached the service more than 15 minutes after the date stamp on the request or more than 15 minutes after the request expiration date (such as for pre-signed URLs), or the date stamp on the request is more than 15 minutes in the future.

HTTP Status Code: 400

ServiceUnavailable

The request has failed due to a temporary failure of the server.

HTTP Status Code: 503

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 400

ValidationError

The input fails to satisfy the constraints specified by an AWS service.

HTTP Status Code: 400