AWS Firewall Manager

Firewall Management

API Version 2018-01-01

AWS Firewall Manager: Firewall Management

Table of Contents

Welcome

This is the *AWS Firewall Manager API Reference*. This guide is for developers who need detailed information about the AWS Firewall Manager API actions, data types, and errors. For detailed information about AWS Firewall Manager features, see the AWS Firewall Manager Developer Guide.

This document was last published on November 19, 2018.

Actions

The following actions are supported:

- AssociateAdminAccount (p. 3)
- DeleteNotificationChannel (p. 5)
- DeletePolicy (p. 6)
- DisassociateAdminAccount (p. 8)
- GetAdminAccount (p. 9)
- GetComplianceDetail (p. 11)
- GetNotificationChannel (p. 13)
- GetPolicy (p. 15)
- ListComplianceStatus (p. 18)
- ListMemberAccounts (p. 21)
- ListPolicies (p. 24)
- PutNotificationChannel (p. 27)
- PutPolicy (p. 29)

AssociateAdminAccount

Sets the AWS Firewall Manager administrator account. AWS Firewall Manager must be associated with the master account your AWS organization or associated with a member account that has the appropriate permissions. If the account ID that you submit is not an AWS Organizations master account, AWS Firewall Manager will set the appropriate permissions for the given member account.

The account that you associate with AWS Firewall Manager is called the AWS Firewall Manager administrator account.

Request Syntax

```
{
   "AdminAccount": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 46).

The request accepts the following data in JSON format.

AdminAccount (p. 3)

The AWS account ID to associate with AWS Firewall Manager as the AWS Firewall Manager administrator account. This can be an AWS Organizations master account or a member account. For more information about AWS Organizations and master accounts, see Managing the AWS Accounts in Your Organization.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

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 (p. 48).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidInputException

The parameters of the request were invalid.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do. For example, you might have submitted an `AssociateAdminAccount` request, but the account ID that you submitted was already set as the AWS Firewall Manager administrator.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

DeleteNotificationChannel

Deletes an AWS Firewall Manager association with the IAM role and the Amazon Simple Notification Service (SNS) topic that is used to record AWS Firewall Manager SNS logs.

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 (p. 48).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do. For example, you might have submitted an `AssociateAdminAccount` request, but the account ID that you submitted was already set as the AWS Firewall Manager administrator.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

DeletePolicy

Permanently deletes an AWS Firewall Manager policy.

Request Syntax

```
{
   "PolicyId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 46).

The request accepts the following data in JSON format.

PolicyId (p. 6)

> The ID of the policy that you want to delete. `PolicyId` is returned by `PutPolicy` and by `ListPolicies`.
>
> Type: String
>
> Length Constraints: Fixed length of 36.
>
> 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 (p. 48).

InternalErrorException

> The operation failed because of a system problem, even though the request was valid. Retry your request.
>
> HTTP Status Code: 400

InvalidOperationException

> The operation failed because there was nothing to do. For example, you might have submitted an `AssociateAdminAccount` request, but the account ID that you submitted was already set as the AWS Firewall Manager administrator.
>
> HTTP Status Code: 400

ResourceNotFoundException

> The specified resource was not found.
>
> 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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

DisassociateAdminAccount

Disassociates the account that has been set as the AWS Firewall Manager administrator account. To set a different account as the administrator account, you must submit an `AssociateAdminAccount` request .

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 (p. 48).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do. For example, you might have submitted an `AssociateAdminAccount` request, but the account ID that you submitted was already set as the AWS Firewall Manager administrator.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

GetAdminAccount

Returns the AWS Organizations master account that is associated with AWS Firewall Manager as the AWS Firewall Manager administrator.

Response Syntax

```
{
   "AdminAccount": "string",
   "RoleStatus": "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.

AdminAccount (p. 9)

The AWS account that is set as the AWS Firewall Manager administrator.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

RoleStatus (p. 9)

The status of the AWS account that you set as the AWS Firewall Manager administrator.

Type: String

Valid Values: `READY | CREATING | PENDING_DELETION | DELETING | DELETED`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 48).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do. For example, you might have submitted an `AssociateAdminAccount` request, but the account ID that you submitted was already set as the AWS Firewall Manager administrator.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

GetComplianceDetail

Returns detailed compliance information about the specified member account. Details include resources that are in and out of compliance with the specified policy. Resources are considered non-compliant if the specified policy has not been applied to them.

Request Syntax

```
{
   "MemberAccount": "string",
   "PolicyId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 46).

The request accepts the following data in JSON format.

MemberAccount (p. 11)

The AWS account that owns the resources that you want to get the details for.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: Yes

PolicyId (p. 11)

The ID of the policy that you want to get the details for. `PolicyId` is returned by `PutPolicy` and by `ListPolicies`.

Type: String

Length Constraints: Fixed length of 36.

Required: Yes

Response Syntax

```
{
   "PolicyComplianceDetail": {
      "EvaluationLimitExceeded": boolean,
      "ExpiredAt": number,
      "IssueInfoMap": {
         "string" : "string"
      },
      "MemberAccount": "string",
      "PolicyId": "string",
      "PolicyOwner": "string",
      "Violators": [
         {
            "ResourceId": "string",
            "ResourceType": "string",
            "ViolationReason": "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.

PolicyComplianceDetail (p. 11)

Information about the resources and the policy that you specified in the `GetComplianceDetail` request.

Type: PolicyComplianceDetail (p. 38) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 48).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

GetNotificationChannel

Returns information about the Amazon Simple Notification Service (SNS) topic that is used to record AWS Firewall Manager SNS logs.

Response Syntax

```
{
   "SnsRoleName": "string",
   "SnsTopicArn": "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.

SnsRoleName (p. 13)

The IAM role that is used by AWS Firewall Manager to record activity to SNS.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

SnsTopicArn (p. 13)

The SNS topic that records AWS Firewall Manager activity.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 48).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do. For example, you might have submitted an `AssociateAdminAccount` request, but the account ID that you submitted was already set as the AWS Firewall Manager administrator.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

GetPolicy

Returns information about the specified AWS Firewall Manager policy.

Request Syntax

```
{
   "PolicyId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 46).

The request accepts the following data in JSON format.

PolicyId (p. 15)

The ID of the AWS Firewall Manager policy that you want the details for.

Type: String

Length Constraints: Fixed length of 36.

Required: Yes

Response Syntax

```
{
   "Policy": {
      "ExcludeMap": {
         "string" : [ "string" ]
      },
      "ExcludeResourceTags": boolean,
      "IncludeMap": {
         "string" : [ "string" ]
      },
      "PolicyId": "string",
      "PolicyName": "string",
      "PolicyUpdateToken": "string",
      "RemediationEnabled": boolean,
      "ResourceTags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "ResourceType": "string",
      "SecurityServicePolicyData": {
         "ManagedServiceData": "string",
         "Type": "string"
      }
   },
   "PolicyArn": "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.

Policy (p. 15)

Information about the specified AWS Firewall Manager policy.

Type: Policy (p. 35) object

PolicyArn (p. 15)

The Amazon Resource Name (ARN) of the specified policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 48).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do. For example, you might have submitted an `AssociateAdminAccount` request, but the account ID that you submitted was already set as the AWS Firewall Manager administrator.

HTTP Status Code: 400

InvalidTypeException

The value of the `Type` parameter is invalid.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go

- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

ListComplianceStatus

Returns an array of `PolicyComplianceStatus` objects in the response. Use `PolicyComplianceStatus` to get a summary of which member accounts are protected by the specified policy.

Request Syntax

```
{
   "MaxResults": number,
   "NextToken": "string",
   "PolicyId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 46).

The request accepts the following data in JSON format.

MaxResults (p. 18)

Specifies the number of `PolicyComplianceStatus` objects that you want AWS Firewall Manager to return for this request. If you have more `PolicyComplianceStatus` objects than the number that you specify for `MaxResults`, the response includes a `NextToken` value that you can use to get another batch of `PolicyComplianceStatus` objects.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

NextToken (p. 18)

If you specify a value for `MaxResults` and you have more `PolicyComplianceStatus` objects than the number that you specify for `MaxResults`, AWS Firewall Manager returns a `NextToken` value in the response that allows you to list another group of `PolicyComplianceStatus` objects. For the second and subsequent `ListComplianceStatus` requests, specify the value of `NextToken` from the previous response to get information about another batch of `PolicyComplianceStatus` objects.

Type: String

Length Constraints: Minimum length of 1.

Required: No

PolicyId (p. 18)

The ID of the AWS Firewall Manager policy that you want the details for.

Type: String

Length Constraints: Fixed length of 36.

Required: Yes

Response Syntax

```
{
   "NextToken": "string",
   "PolicyComplianceStatusList": [
      {
         "EvaluationResults": [
            {
               "ComplianceStatus": "string",
               "EvaluationLimitExceeded": boolean,
               "ViolatorCount": number
            }
         ],
         "IssueInfoMap": {
            "string" : "string"
         },
         "LastUpdated": number,
         "MemberAccount": "string",
         "PolicyId": "string",
         "PolicyName": "string",
         "PolicyOwner": "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 (p. 19)

If you have more `PolicyComplianceStatus` objects than the number that you specified for `MaxResults` in the request, the response includes a `NextToken` value. To list more `PolicyComplianceStatus` objects, submit another `ListComplianceStatus` request, and specify the `NextToken` value from the response in the `NextToken` value in the next request.

Type: String

Length Constraints: Minimum length of 1.

PolicyComplianceStatusList (p. 19)

An array of `PolicyComplianceStatus` objects.

Type: Array of PolicyComplianceStatus (p. 40) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 48).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

ListMemberAccounts

Returns a `MemberAccounts` object that lists the member accounts in the administrator's AWS organization.

The `ListMemberAccounts` must be submitted by the account that is set as the AWS Firewall Manager administrator.

Request Syntax

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 46).

The request accepts the following data in JSON format.

MaxResults (p. 21)

Specifies the number of member account IDs that you want AWS Firewall Manager to return for this request. If you have more IDs than the number that you specify for `MaxResults`, the response includes a `NextToken` value that you can use to get another batch of member account IDs.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

NextToken (p. 21)

If you specify a value for `MaxResults` and you have more account IDs than the number that you specify for `MaxResults`, AWS Firewall Manager returns a `NextToken` value in the response that allows you to list another group of IDs. For the second and subsequent `ListMemberAccountsRequest` requests, specify the value of `NextToken` from the previous response to get information about another batch of member account IDs.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "MemberAccounts": [ "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.

MemberAccounts (p. 21)

An array of account IDs.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 1024.

NextToken (p. 21)

If you have more member account IDs than the number that you specified for `MaxResults` in the request, the response includes a `NextToken` value. To list more IDs, submit another `ListMemberAccounts` request, and specify the `NextToken` value from the response in the `NextToken` value in the next request.

Type: String

Length Constraints: Minimum length of 1.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 48).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

ListPolicies

Returns an array of `PolicySummary` objects in the response.

Request Syntax

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 46).

The request accepts the following data in JSON format.

MaxResults (p. 24)

Specifies the number of `PolicySummary` objects that you want AWS Firewall Manager to return for this request. If you have more `PolicySummary` objects than the number that you specify for `MaxResults`, the response includes a `NextToken` value that you can use to get another batch of `PolicySummary` objects.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

NextToken (p. 24)

If you specify a value for `MaxResults` and you have more `PolicySummary` objects than the number that you specify for `MaxResults`, AWS Firewall Manager returns a `NextToken` value in the response that allows you to list another group of `PolicySummary` objects. For the second and subsequent `ListPolicies` requests, specify the value of `NextToken` from the previous response to get information about another batch of `PolicySummary` objects.

Type: String

Length Constraints: Minimum length of 1.

Required: No

Response Syntax

```
{
   "NextToken": "string",
   "PolicyList": [
      {
         "PolicyArn": "string",
         "PolicyId": "string",
         "PolicyName": "string",
         "RemediationEnabled": boolean,
         "ResourceType": "string",
         "SecurityServiceType": "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 (p. 24)

If you have more `PolicySummary` objects than the number that you specified for `MaxResults` in the request, the response includes a `NextToken` value. To list more `PolicySummary` objects, submit another `ListPolicies` request, and specify the `NextToken` value from the response in the `NextToken` value in the next request.

Type: String

Length Constraints: Minimum length of 1.

PolicyList (p. 24)

An array of `PolicySummary` objects.

Type: Array of PolicySummary (p. 42) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 48).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do. For example, you might have submitted an `AssociateAdminAccount` request, but the account ID that you submitted was already set as the AWS Firewall Manager administrator.

HTTP Status Code: 400

LimitExceededException

The operation exceeds a resource limit, for example, the maximum number of `policy` objects that you can create for an AWS account. For more information, see Firewall Manager Limits in the *AWS WAF Developer Guide*.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

PutNotificationChannel

Designates the IAM role and Amazon Simple Notification Service (SNS) topic that AWS Firewall Manager uses to record SNS logs.

Request Syntax

```
{
   "SnsRoleName": "string",
   "SnsTopicArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 46).

The request accepts the following data in JSON format.

SnsRoleName (p. 27)

The Amazon Resource Name (ARN) of the IAM role that allows Amazon SNS to record AWS Firewall Manager activity.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: Yes

SnsTopicArn (p. 27)

The Amazon Resource Name (ARN) of the SNS topic that collects notifications from AWS Firewall Manager.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

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 (p. 48).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do. For example, you might have submitted an `AssociateAdminAccount` request, but the account ID that you submitted was already set as the AWS Firewall Manager administrator.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

PutPolicy

Creates an AWS Firewall Manager policy.

Request Syntax

```
{
   "Policy": {
      "ExcludeMap": {
         "string" : [ "string" ]
      },
      "ExcludeResourceTags": boolean,
      "IncludeMap": {
         "string" : [ "string" ]
      },
      "PolicyId": "string",
      "PolicyName": "string",
      "PolicyUpdateToken": "string",
      "RemediationEnabled": boolean,
      "ResourceTags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "ResourceType": "string",
      "SecurityServicePolicyData": {
         "ManagedServiceData": "string",
         "Type": "string"
      }
   }
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 46).

The request accepts the following data in JSON format.

Policy (p. 29)

The details of the AWS Firewall Manager policy to be created.

Type: Policy (p. 35) object

Required: Yes

Response Syntax

```
{
   "Policy": {
      "ExcludeMap": {
         "string" : [ "string" ]
      },
      "ExcludeResourceTags": boolean,
      "IncludeMap": {
         "string" : [ "string" ]
      },
      "PolicyId": "string",
      "PolicyName": "string",
      "PolicyUpdateToken": "string",
      "RemediationEnabled": boolean,
      "ResourceTags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "ResourceType": "string",
      "SecurityServicePolicyData": {
         "ManagedServiceData": "string",
         "Type": "string"
      }
   },
   "PolicyArn": "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.

Policy (p. 29)

The details of the AWS Firewall Manager policy that was created.

Type: Policy (p. 35) object

PolicyArn (p. 29)

The Amazon Resource Name (ARN) of the policy that was created.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 48).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidInputException

The parameters of the request were invalid.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do. For example, you might have submitted an `AssociateAdminAccount` request, but the account ID that you submitted was already set as the AWS Firewall Manager administrator.

HTTP Status Code: 400

InvalidTypeException

The value of the `Type` parameter is invalid.

HTTP Status Code: 400

LimitExceededException

The operation exceeds a resource limit, for example, the maximum number of `policy` objects that you can create for an AWS account. For more information, see Firewall Manager Limits in the *AWS WAF Developer Guide*.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

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
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V2

Data Types

The Firewall Management Service 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:

ComplianceViolator

Details of the resource that is not protected by the policy.

Contents

ResourceId

The resource ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: No

ResourceType

The resource type. This is in the format shown in AWS Resource Types Reference. Valid values are `AWS::ElasticLoadBalancingV2::LoadBalancer` or `AWS::CloudFront::Distribution`.

Type: String

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

Required: No

ViolationReason

The reason that the resource is not protected by the policy.

Type: String

Valid Values: `WEB_ACL_MISSING_RULE_GROUP | RESOURCE_MISSING_WEB_ACL | RESOURCE_INCORRECT_WEB_ACL`

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 Go
- AWS SDK for Java
- AWS SDK for Ruby V2

EvaluationResult

Describes the compliance status for the account. An account is considered non-compliant if it includes resources that are not protected by the specified policy.

Contents

ComplianceStatus

Describes an AWS account's compliance with the AWS Firewall Manager policy.

Type: String

Valid Values: `COMPLIANT | NON_COMPLIANT`

Required: No

EvaluationLimitExceeded

Indicates that over 100 resources are non-compliant with the AWS Firewall Manager policy.

Type: Boolean

Required: No

ViolatorCount

Number of resources that are non-compliant with the specified policy. A resource is considered non-compliant if it is not associated with the specified policy.

Type: Long

Valid Range: Minimum value of 0.

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 Go
- AWS SDK for Java
- AWS SDK for Ruby V2

Policy

An AWS Firewall Manager policy.

Contents

ExcludeMap

Specifies the AWS account IDs to exclude from the policy. The `IncludeMap` values are evaluated first, with all the appropriate account IDs added to the policy. Then the accounts listed in `ExcludeMap` are removed, resulting in the final list of accounts to add to the policy.

The key to the map is `ACCOUNT`. For example, a valid `ExcludeMap` would be `{“ACCOUNT” : [“accountID1”, “accountID2”]}`.

Type: String to array of strings map

Valid Keys: `ACCOUNT`

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: No

ExcludeResourceTags

If set to `True`, resources with the tags that are specified in the `ResourceTag` array are not protected by the policy. If set to `False`, and the `ResourceTag` array is not null, only resources with the specified tags are associated with the policy.

Type: Boolean

Required: Yes

IncludeMap

Specifies the AWS account IDs to include in the policy. If `IncludeMap` is null, all accounts in the organization in AWS Organizations are included in the policy. If `IncludeMap` is not null, only values listed in `IncludeMap` are included in the policy.

The key to the map is `ACCOUNT`. For example, a valid `IncludeMap` would be `{“ACCOUNT” : [“accountID1”, “accountID2”]}`.

Type: String to array of strings map

Valid Keys: `ACCOUNT`

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: No

PolicyId

The ID of the AWS Firewall Manager policy.

Type: String

Length Constraints: Fixed length of 36.

Required: No

PolicyName

The friendly name of the AWS Firewall Manager policy.

Type: String

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

Required: Yes

PolicyUpdateToken

A unique identifier for each update to the policy. When issuing a PutPolicy request, the PolicyUpdateToken in the request must match the PolicyUpdateToken of the current policy version. To get the PolicyUpdateToken of the current policy version, use a GetPolicy request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: No

RemediationEnabled

Indicates if the policy should be automatically applied to new resources.

Type: Boolean

Required: Yes

ResourceTags

An array of ResourceTag objects.

Type: Array of ResourceTag (p. 44) objects

Array Members: Minimum number of 0 items. Maximum number of 8 items.

Required: No

ResourceType

The type of resource to protect with the policy, either an Application Load Balancer or a CloudFront distribution. This is in the format shown in AWS Resource Types Reference. Valid values are AWS::ElasticLoadBalancingV2::LoadBalancer or AWS::CloudFront::Distribution.

Type: String

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

Required: Yes

SecurityServicePolicyData

Details about the security service that is being used to protect the resources.

Type: SecurityServicePolicyData (p. 45) 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 Go
- AWS SDK for Java

- AWS SDK for Ruby V2

PolicyComplianceDetail

Describes the non-compliant resources in a member account for a specific AWS Firewall Manager policy. A maximum of 100 entries are displayed. If more than 100 resources are non-compliant, `EvaluationLimitExceeded` is set to `True`.

Contents

EvaluationLimitExceeded

Indicates if over 100 resources are non-compliant with the AWS Firewall Manager policy.

Type: Boolean

Required: No

ExpiredAt

A time stamp that indicates when the returned information should be considered out-of-date.

Type: Timestamp

Required: No

IssueInfoMap

Details about problems with dependent services, such as AWS WAF or AWS Config, that are causing a resource to be non-compliant. The details include the name of the dependent service and the error message received that indicates the problem with the service.

Type: String to string map

Valid Keys: `AWSCONFIG | AWSWAF`

Value Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: No

MemberAccount

The AWS account ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: No

PolicyId

The ID of the AWS Firewall Manager policy.

Type: String

Length Constraints: Fixed length of 36.

Required: No

PolicyOwner

The AWS account that created the AWS Firewall Manager policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: No

Violators

An array of resources that are not protected by the policy.

Type: Array of ComplianceViolator (p. 33) 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 Go
- AWS SDK for Java
- AWS SDK for Ruby V2

PolicyComplianceStatus

Indicates whether the account is compliant with the specified policy. An account is considered non-compliant if it includes resources that are not protected by the policy.

Contents

EvaluationResults

An array of `EvaluationResult` objects.

Type: Array of EvaluationResult (p. 34) objects

Required: No

IssueInfoMap

Details about problems with dependent services, such as AWS WAF or AWS Config, that are causing a resource to be non-compliant. The details include the name of the dependent service and the error message received that indicates the problem with the service.

Type: String to string map

Valid Keys: `AWSCONFIG | AWSWAF`

Value Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: No

LastUpdated

Time stamp of the last update to the `EvaluationResult` objects.

Type: Timestamp

Required: No

MemberAccount

The member account ID.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: No

PolicyId

The ID of the AWS Firewall Manager policy.

Type: String

Length Constraints: Fixed length of 36.

Required: No

PolicyName

The friendly name of the AWS Firewall Manager policy.

Type: String

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

Required: No

PolicyOwner

The AWS account that created the AWS Firewall Manager policy.

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 Go
- AWS SDK for Java
- AWS SDK for Ruby V2

PolicySummary

Details of the AWS Firewall Manager policy.

Contents

PolicyArn

The Amazon Resource Name (ARN) of the specified policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: No

PolicyId

The ID of the specified policy.

Type: String

Length Constraints: Fixed length of 36.

Required: No

PolicyName

The friendly name of the specified policy.

Type: String

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

Required: No

RemediationEnabled

Indicates if the policy should be automatically applied to new resources.

Type: Boolean

Required: No

ResourceType

The type of resource to protect with the policy, either an Application Load Balancer or a CloudFront distribution. This is in the format shown in AWS Resource Types Reference. Valid values are `AWS::ElasticLoadBalancingV2::LoadBalancer` or `AWS::CloudFront::Distribution`.

Type: String

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

Required: No

SecurityServiceType

The service that the policy is using to protect the resources. This value is `WAF`.

Type: String

Valid Values: `WAF`

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 Go
- AWS SDK for Java
- AWS SDK for Ruby V2

ResourceTag

The resource tags that AWS Firewall Manager uses to determine if a particular resource should be included or excluded from protection by the AWS Firewall Manager policy. Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. Each tag consists of a key and an optional value, both of which you define. Tags are combined with an "OR." That is, if you add more than one tag, if any of the tags matches, the resource is considered a match for the include or exclude. Working with Tag Editor.

Contents

Key

The resource tag key.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

Value

The resource tag value.

Type: String

Length Constraints: Maximum length of 256.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

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 Go
- AWS SDK for Java
- AWS SDK for Ruby V2

SecurityServicePolicyData

Details about the security service that is being used to protect the resources.

Contents

ManagedServiceData

Details about the service. This contains `WAF` data in JSON format, as shown in the following example:

```
ManagedServiceData": "{\"type\": \"WAF\", \"ruleGroups\": [{\"id\":
\"12345678-1bcd-9012-efga-0987654321ab\", \"overrideAction\" : {\"type\":
\"COUNT\"}}], \"defaultAction\": {\"type\": \"BLOCK\"}}
```

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Required: No

Type

The service that the policy is using to protect the resources. This value is `WAF`.

Type: String

Valid Values: `WAF`

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 Go
- AWS SDK for Java
- AWS SDK for Ruby V2

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 Signature Version 4 Signing Process in the *Amazon Web Services General Reference*.

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 Task 2: Create a String to Sign for Signature Version 4 in the *Amazon Web Services General Reference*.

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 Handling Dates in Signature Version 4 in the *Amazon Web Services General Reference*.

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 Security Token Service, go to AWS Services That Work with IAM in the *IAM User Guide*.

Condition: If you're using temporary security credentials from the AWS Security Token Service, 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 Task 1: Create a Canonical Request For Signature Version 4 in the *Amazon Web Services General Reference*.

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

InvalidParameterCombination

Parameters that must not be used together were used together.

HTTP Status Code: 400

InvalidParameterValue

An invalid or out-of-range value was supplied for the input parameter.

HTTP Status Code: 400

InvalidQueryParameter

The AWS query string is malformed or does not adhere to AWS standards.

HTTP Status Code: 400

MalformedQueryString

The query string contains a syntax error.

HTTP Status Code: 404

MissingAction

The request is missing an action or a required parameter.

HTTP Status Code: 400

MissingAuthenticationToken

The request must contain either a valid (registered) AWS access key ID or X.509 certificate.

HTTP Status Code: 403

MissingParameter

A required parameter for the specified action is not supplied.

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