AWS Firewall Manager: Firewall Management
Copyright © 2020 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

Welcome ........................................................................................................................................... 1  
Actions ........................................................................................................................................... 2  
  AssociateAdminAccount ................................................................. 3  
  Request Syntax .................................................................................. 3  
  Request Parameters ......................................................................... 3  
  Response Elements ......................................................................... 3  
  Errors ................................................................................................. 3  
  See Also ............................................................................................ 4  
DeleteNotificationChannel ............................................................. 5  
  Response Elements ......................................................................... 5  
  Errors ................................................................................................. 5  
  See Also ............................................................................................ 5  
DeletePolicy ...................................................................................... 6  
  Request Syntax .................................................................................. 6  
  Request Parameters ......................................................................... 6  
  Response Elements ......................................................................... 7  
  Errors ................................................................................................. 7  
  See Also ............................................................................................ 7  
DisassociateAdminAccount ............................................................ 8  
  Response Elements ......................................................................... 8  
  Errors ................................................................................................. 8  
  See Also ............................................................................................ 8  
GetAdminAccount ............................................................................ 9  
  Response Syntax ................................................................................ 9  
  Response Elements ......................................................................... 9  
  Errors ................................................................................................. 9  
  See Also ............................................................................................ 10  
GetComplianceDetail ...................................................................... 11  
  Request Syntax .................................................................................. 11  
  Request Parameters ......................................................................... 11  
  Response Syntax .............................................................................. 11  
  Response Elements ......................................................................... 12  
  Errors ................................................................................................. 12  
  See Also ............................................................................................ 12  
GetNotificationChannel ................................................................. 14  
  Response Syntax .............................................................................. 14  
  Response Elements ......................................................................... 14  
  Errors ................................................................................................. 14  
  See Also ............................................................................................ 15  
GetPolicy .......................................................................................... 16  
  Request Syntax .................................................................................. 16  
  Request Parameters ......................................................................... 16  
  Response Syntax .............................................................................. 16  
  Response Elements ......................................................................... 17  
  Errors ................................................................................................. 17  
  See Also ............................................................................................ 17  
GetProtectionStatus ...................................................................... 19  
  Request Syntax .................................................................................. 19  
  Request Parameters ......................................................................... 19  
  Response Syntax .............................................................................. 19  
  Response Elements ......................................................................... 20  
  Errors ................................................................................................. 20  
  Example .............................................................................................. 22  
  See Also ............................................................................................ 22
<table>
<thead>
<tr>
<th>Function</th>
<th>Request Syntax</th>
<th>Request Parameters</th>
<th>Response Syntax</th>
<th>Response Elements</th>
<th>Errors</th>
<th>See Also</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListComplianceStatus</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>24</td>
</tr>
<tr>
<td>ListMemberAccounts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>27</td>
</tr>
<tr>
<td>ListPolicies</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>30</td>
</tr>
<tr>
<td>ListTagsForResource</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>33</td>
</tr>
<tr>
<td>PutNotificationChannel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>35</td>
</tr>
<tr>
<td>PutPolicy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>37</td>
</tr>
<tr>
<td>TagResource</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>41</td>
</tr>
<tr>
<td>UntagResource</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>43</td>
</tr>
<tr>
<td>Data Types</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>45</td>
</tr>
<tr>
<td>ComplianceViolator</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>46</td>
</tr>
</tbody>
</table>

See Also

Errors

Request Parameters

Request Syntax

Response Elements

Response Syntax

See Also

Errors

Response Elements
## AWS Firewall Manager

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EvaluationResult</td>
<td>47</td>
</tr>
<tr>
<td>Contents</td>
<td>47</td>
</tr>
<tr>
<td>See Also</td>
<td>47</td>
</tr>
<tr>
<td>Policy</td>
<td>48</td>
</tr>
<tr>
<td>Contents</td>
<td>48</td>
</tr>
<tr>
<td>See Also</td>
<td>50</td>
</tr>
<tr>
<td>PolicyComplianceDetail</td>
<td>51</td>
</tr>
<tr>
<td>Contents</td>
<td>51</td>
</tr>
<tr>
<td>See Also</td>
<td>52</td>
</tr>
<tr>
<td>PolicyComplianceStatus</td>
<td>53</td>
</tr>
<tr>
<td>Contents</td>
<td>53</td>
</tr>
<tr>
<td>See Also</td>
<td>54</td>
</tr>
<tr>
<td>PolicySummary</td>
<td>55</td>
</tr>
<tr>
<td>Contents</td>
<td>55</td>
</tr>
<tr>
<td>See Also</td>
<td>56</td>
</tr>
<tr>
<td>ResourceTag</td>
<td>57</td>
</tr>
<tr>
<td>Contents</td>
<td>57</td>
</tr>
<tr>
<td>See Also</td>
<td>57</td>
</tr>
<tr>
<td>SecurityServicePolicyData</td>
<td>58</td>
</tr>
<tr>
<td>Contents</td>
<td>58</td>
</tr>
<tr>
<td>See Also</td>
<td>59</td>
</tr>
<tr>
<td>Tag</td>
<td>60</td>
</tr>
<tr>
<td>Contents</td>
<td>60</td>
</tr>
<tr>
<td>See Also</td>
<td>60</td>
</tr>
<tr>
<td>Common Parameters</td>
<td>61</td>
</tr>
<tr>
<td>Common Errors</td>
<td>63</td>
</tr>
</tbody>
</table>
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 April 3, 2020.
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. 14)
- GetPolicy (p. 16)
- GetProtectionStatus (p. 19)
- ListComplianceStatus (p. 24)
- ListMemberAccounts (p. 27)
- ListPolicies (p. 30)
- ListTagsForResource (p. 33)
- PutNotificationChannel (p. 35)
- PutPolicy (p. 37)
- TagResource (p. 41)
- UntagResource (p. 43)
**AssociateAdminAccount**

Sets the AWS Firewall Manager administrator account. AWS Firewall Manager must be associated with the master account of 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**

```json
{
   "AdminAccount": "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.

**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


Pattern: ^[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](#).

**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 V3
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. 63).

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 V3
DeletePolicy

Permanently deletes an AWS Firewall Manager policy.

Request Syntax

```
{
    "DeleteAllPolicyResources": boolean,
    "PolicyId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 61).

The request accepts the following data in JSON format.

**DeleteAllPolicyResources (p. 6)**

If True, the request performs cleanup according to the policy type.

For AWS WAF and Shield Advanced policies, the cleanup does the following:
- Deletes rule groups created by AWS Firewall Manager
- Removes web ACLs from in-scope resources
- Deletes web ACLs that contain no rules or rule groups

For security group policies, the cleanup does the following for each security group in the policy:
- Disassociates the security group from in-scope resources
- Deletes the security group if it was created through Firewall Manager and if it's no longer associated with any resources through another policy

After the cleanup, in-scope resources are no longer protected by web ACLs in this policy. Protection of out-of-scope resources remains unchanged. Scope is determined by tags that you create and accounts that you associate with the policy. When creating the policy, if you specify that only resources in specific accounts or with specific tags are in scope of the policy, those accounts and resources are handled by the policy. All others are out of scope. If you don’t specify tags or accounts, all resources are in scope.

Type: Boolean

Required: No

**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.

Pattern: ^[a-zA-Z0-9_]*$ (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. 63).

**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 a `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 V3
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. 63).

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 V3
GetAdminAccount

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

Response Syntax

```json
{
   "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


Pattern: ^[0-9]+$

**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. 63).

**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 V3
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 noncompliant for AWS WAF and Shield Advanced policies if the specified policy has not been applied to them. Resources are considered noncompliant for security group policies if they are in scope of the policy, they violate one or more of the policy rules, and remediation is disabled or not possible.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 61).

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


Pattern: ^[0-9]+$

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.

Pattern: ^[a-zA-Z0-9-]{36}$

Required: Yes

Response Syntax

```json
{
    "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. 51) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 63).

**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 V3
GetNotificationChannel

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. 14)**

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

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

**SnsTopicArn (p. 14)**

The SNS topic that records AWS Firewall Manager activity.

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 63).

**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 V3
GetPolicy

Returns information about the specified AWS Firewall Manager policy.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 61).

The request accepts the following data in JSON format.

**PolicyId (p. 16)**

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

Type: String

Length Constraints: Fixed length of 36.

Pattern: ^[a-z0-9A-Z-]{36}$

Required: Yes

Response Syntax

```json
{
  "Policy": {
    "ExcludeMap": {
      "string": [ "string" ]
    },
    "ExcludeResourceTags": boolean,
    "IncludeMap": {
      "string": [ "string" ]
    },
    "PolicyId": "string",
    "PolicyName": "string",
    "PolicyUpdateToken": "string",
    "RemediationEnabled": boolean,
    "ResourceTags": [
      {
        "Key": "string",
        "Value": "string"
      }
    ],
    "ResourceType": "string",
    "ResourceTypeList": [ "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. 16)

Information about the specified AWS Firewall Manager policy.

Type: **Policy** (p. 48) object

**PolicyArn** (p. 16)

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

Type: String


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

Errors

For information about the errors that are common to all actions, see **Common Errors** (p. 63).

**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:
See Also

- 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 V3
GetProtectionStatus

If you created a Shield Advanced policy, returns policy-level attack summary information in the event of a potential DDoS attack. Other policy types are currently unsupported.

Request Syntax

```json
{
    "EndTime": number,
    "MaxResults": number,
    "MemberAccountId": "string",
    "NextToken": "string",
    "PolicyId": "string",
    "StartTime": number
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 61).

The request accepts the following data in JSON format.

**EndTime (p. 19)**

The end of the time period to query for the attacks. This is a timestamp type. The request syntax listing indicates a number type because the default used by AWS Firewall Manager is Unix time in seconds. However, any valid timestamp format is allowed.

Type: Timestamp

Required: No

**MaxResults (p. 19)**

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

Type: Integer

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

Required: No

**MemberAccountId (p. 19)**

The AWS account that is in scope of the policy that you want to get the details for.

Type: String


Pattern: ^[0-9]+$

Required: No

**NextToken (p. 19)**

If you specify a value for MaxResults and you have more objects than the number that you specify for MaxResults, AWS Firewall Manager returns a NextToken value in the response, which you can
use to retrieve another group of objects. For the second and subsequent GetProtectionStatus requests, specify the value of NextToken from the previous response to get information about another batch of objects.

Type: String
Pattern: ^([^\p{L}\p{Z}\p{N}\p{_.:/=+-@}]+\+\-\@]*)$
Required: No

**PolicyId (p. 19)**

The ID of the policy for which you want to get the attack information.

Type: String
Length Constraints: Fixed length of 36.
Pattern: ^[a-zA-Z0-9A-Z\-]{36}$
Required: Yes

**StartTime (p. 19)**

The start of the time period to query for the attacks. This is a timestamp type. The request syntax listing indicates a number type because the default used by AWS Firewall Manager is Unix time in seconds. However, any valid timestamp format is allowed.

Type: Timestamp
Required: No

### Response Syntax

```json
{
  "AdminAccountId": "string",
  "Data": "string",
  "NextToken": "string",
  "ServiceType": "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.

**AdminAccountId (p. 20)**

The ID of the AWS Firewall administrator account for this policy.

Type: String

Pattern: ^[0-9]+$
Data (p. 20)

Details about the attack, including the following:
- Attack type
- Account ID
- ARN of the resource attacked
- Start time of the attack
- End time of the attack (ongoing attacks will not have an end time)

The details are in JSON format.

Type: String

NextToken (p. 20)

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

AWS SDKs provide auto-pagination that identify NextToken in a response and make subsequent request calls automatically on your behalf. However, this feature is not supported by GetProtectionStatus. You must submit subsequent requests with NextToken using your own processes.

Type: String


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

ServiceType (p. 20)

The service type that is protected by the policy. Currently, this is always SHIELD_ADVANCED.

Type: String

Valid Values: WAF | WAFV2 | SHIELD_ADVANCED | SECURITY_GROUPS_COMMON | SECURITY_GROUPS_CONTENT_AUDIT | SECURITY_GROUPS_USAGE_AUDIT

Errors

For information about the errors that are common to all actions, see Common Errors (p. 63).

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

ResourceNotFoundException

The specified resource was not found.
HTTP Status Code: 400

Example

Example response

```json
[
  {
    accountId: account1
    attackSummaries:[
      {
        attackId: attackId1
        resourceARN: resource1
        attackVector: [SYC_FLOOD, UDP_REFLECTION]
        startTime: 1234567890123
        endTime: 1234567890123
      },
      {
        attackId: attackId2
        resourceARN: resource2
        attackVector: [SYC_FLOOD]
        startTime: 1234567890123
        endTime: 1234567890123
      }
    ]
  },
  {
    accountId: account2
    attackSummaries:[
      {
        attackId: attackId3
        resourceARN: resource3
        attackVector: [SYC_FLOOD, UDP_REFLECTION]
        startTime: 1234567890123
        endTime: 1234567890123
      },
      {
        attackId: attackId4
        resourceARN: resource4
        attackVector: [SYC_FLOOD]
        startTime: 1234567890123
        endTime: 1234567890123
      }
    ]
  }
]
```

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
See Also

- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3
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

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 61).

The request accepts the following data in JSON format.

MaxResults (p. 24)

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. 24)

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


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

Required: No

PolicyId (p. 24)

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

Type: String

Length Constraints: Fixed length of 36.
Response Syntax

```json
{
    "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. 25)**

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


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

**PolicyComplianceStatusList (p. 25)**

An array of `PolicyComplianceStatus` objects.

Type: Array of `PolicyComplianceStatus` (p. 53) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 63).
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 V3
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

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 61).

The request accepts the following data in JSON format.

MaxResults (p. 27)

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. 27)

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


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

Required: No

Response Syntax

```json
{
   "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. 27)**

An array of account IDs.

Type: Array of strings


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

**NextToken (p. 27)**

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


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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 63).

**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 V3
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. 61).

The request accepts the following data in JSON format.

MaxResults (p. 30)

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. 30)

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


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

Required: No

Response Syntax

```
{
   "NextToken": "string",
   "PolicyList": [
      {
         "PolicyArn": "string",
         "PolicyId": "string",
         "PolicyName": "string",
         ...
      }
   ]
}
```

API Version 2018-01-01
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. 30)

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


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

PolicyList (p. 30)

An array of PolicySummary objects.

Type: Array of PolicySummary (p. 55) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 63).

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 V3
ListTagsForResource

Retrieves the list of tags for the specified AWS resource.

Request Syntax

```
{
   "ResourceArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 61).

The request accepts the following data in JSON format.

ResourceArn (p. 33)

The Amazon Resource Name (ARN) of the resource to return tags for. The Firewall Manager policy is the only AWS resource that supports tagging, so this ARN is a policy ARN.

Type: String


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

Required: Yes

Response Syntax

```
{
   "TagList": [
      {
         "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.

TagList (p. 33)

The tags associated with the resource.

Type: Array of Tag (p. 60) 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 (p. 63).

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 V3
PutNotificationChannel

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

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 61).

The request accepts the following data in JSON format.

SnsRoleName (p. 35)

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

Type: String


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

Required: Yes

SnsTopicArn (p. 35)

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

Type: String


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 (p. 63).

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 V3
PutPolicy

Creates an AWS Firewall Manager policy.

Firewall Manager provides the following types of policies:

- A Shield Advanced policy, which applies Shield Advanced protection to specified accounts and resources
- An AWS WAF policy (type WAFV2), which defines rule groups to run first in the corresponding AWS WAF web ACL and rule groups to run last in the web ACL.
- An AWS WAF Classic policy (type WAF), which defines a rule group.
- A security group policy, which manages VPC security groups across your AWS organization.

Each policy is specific to one of the types. If you want to enforce more than one policy type across accounts, create multiple policies. You can create multiple policies for each type.

You must be subscribed to Shield Advanced to create a Shield Advanced policy. For more information about subscribing to Shield Advanced, see CreateSubscription.

Request Syntax

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

For information about the parameters that are common to all actions, see Common Parameters (p. 61).

The request accepts the following data in JSON format.

**Policy (p. 37)**

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

Type: Policy (p. 48) object

Required: Yes

**TagList (p. 37)**

The tags to add to the AWS resource.

Type: Array of Tag (p. 60) objects

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

Required: No

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",
    "ResourceTypeList": [ "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. 38)

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

Type: Policy (p. 48) object

**PolicyArn** (p. 38)

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

Type: String


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

### Errors

For information about the errors that are common to all actions, see Common Errors (p. 63).

**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 V3
TagResource

Add one or more tags to an AWS resource.

Request Syntax

```
{
    "ResourceArn": "string",
    "TagList": [
        {
            "Key": "string",
            "Value": "string"
        }
    ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 61).

The request accepts the following data in JSON format.

**ResourceArn (p. 41)**

The Amazon Resource Name (ARN) of the resource. The Firewall Manager policy is the only AWS resource that supports tagging, so this ARN is a policy ARN.

Type: String


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

Required: Yes

**TagList (p. 41)**

The tags to add to the resource.

Type: Array of Tag (p. 60) 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 (p. 63).

**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

**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 V3
UntagResource

Removes one or more tags from an AWS resource.

Request Syntax

{
    "ResourceArn": "string",
    "TagKeys": [ "string" ]
}

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 61).

The request accepts the following data in JSON format.

ResourceArn (p. 43)

The Amazon Resource Name (ARN) of the resource. The Firewall Manager policy is the only AWS resource that supports tagging, so this ARN is a policy ARN.

Type: String


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

Required: Yes

TagKeys (p. 43)

The keys of the tags to remove from the resource.

Type: Array of strings

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


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 (p. 63).

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 V3
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 (p. 46)
- EvaluationResult (p. 47)
- Policy (p. 48)
- PolicyComplianceDetail (p. 51)
- PolicyComplianceStatus (p. 53)
- PolicySummary (p. 55)
- ResourceTag (p. 57)
- SecurityServicePolicyData (p. 58)
- Tag (p. 60)
ComplianceViolator

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

Contents

ResourceId

The resource ID.

Type: String


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

Required: No

ResourceType

The resource type. This is in the format shown in the AWS Resource Types Reference. For example: AWS::ElasticLoadBalancingV2::LoadBalancer or AWS::CloudFront::Distribution.

Type: String


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

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 | RESOURCE MISSING_SHIELD_PROTECTION | RESOURCE MISSING_WEB_ACL OR_SHIELD_PROTECTION | RESOURCE MISSING_SECURITY_GROUP | RESOURCE VIOLATES_AUDIT_SECURITY_GROUP | SECURITY_GROUP UNUSED | SECURITY GROUP REDUNDANT

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 V3
EvaluationResult

Describes the compliance status for the account. An account is considered noncompliant if it includes resources that are not protected by the specified policy or that don't comply with the 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 noncompliant with the AWS Firewall Manager policy.

Type: Boolean

Required: No

ViolatorCount

The number of resources that are noncompliant with the specified policy. For AWS WAF and Shield Advanced policies, a resource is considered noncompliant if it is not associated with the policy. For security group policies, a resource is considered noncompliant if it doesn't comply with the rules of the policy and remediation is disabled or not possible.

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 V3
**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


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

Required: No

**ExcludeResourceTags**

If set to True, resources with the tags that are specified in the ResourceTag array are not in scope of the policy. If set to False, and the ResourceTag array is not null, only resources with the specified tags are in scope of 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


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

Required: No

**PolicyId**

The ID of the AWS Firewall Manager policy.

Type: String

Length Constraints: Fixed length of 36.
Pattern: ^[a-zA-Z0-9-]{36}$
Required: No

**PolicyName**

The friendly name of the AWS Firewall Manager policy.

Type: String


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


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

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

Required: No

**ResourceType**

The type of resource protected by or in scope of the policy. This is in the format shown in the AWS Resource Types Reference. For AWS WAF and Shield Advanced, examples include `AWS::ElasticLoadBalancingV2::LoadBalancer` and `AWS::CloudFront::Distribution`. For a security group common policy, valid values are `AWS::EC2::NetworkInterface` and `AWS::EC2::Instance`. For a security group content audit policy, valid values are `AWS::EC2::SecurityGroup`, `AWS::EC2::NetworkInterface`, and `AWS::EC2::Instance`. For a security group usage audit policy, the value is `AWS::EC2::SecurityGroup`.

Type: String


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

An array of ResourceType.

Type: Array of strings


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

Required: No

SecurityServicePolicyData

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

Type: SecurityServicePolicyData (p. 58) 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 V3
PolicyComplianceDetail

Describes the noncompliant 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 noncompliant, EvaluationLimitExceeded is set to True.

Contents

**EvaluationLimitExceeded**

Indicates if over 100 resources are noncompliant with the AWS Firewall Manager policy.

Type: Boolean

Required: No

**ExpiredAt**

A timestamp 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 noncompliant. 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 | AWSSHIELD_ADVANCED | AWSVPC


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

Required: No

**MemberAccount**

The AWS account ID.

Type: String


Pattern: ^[0-9]+$ 

Required: No

**PolicyId**

The ID of the AWS Firewall Manager policy.

Type: String

Length Constraints: Fixed length of 36.

Pattern: ^[a-zA-Z0-9\-]{36}$ 

Required: No

API Version 2018-01-01
PolicyOwner

The AWS account that created the AWS Firewall Manager policy.

Type: String


Pattern: ^[0-9]+$

Required: No

Violators

An array of resources that aren't protected by the AWS WAF or Shield Advanced policy or that aren't in compliance with the security group policy.

Type: Array of ComplianceViolator (p. 46) 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 V3
PolicyComplianceStatus

Indicates whether the account is compliant with the specified policy. An account is considered noncompliant if it includes resources that are not protected by the policy, for AWS WAF and Shield Advanced policies, or that are noncompliant with the policy, for security group policies.

Contents

EvaluationResults

An array of EvaluationResult objects.

Type: Array of EvaluationResult (p. 47) objects

Required: No

IssueInfoMap

Details about problems with dependent services, such as AWS WAF or AWS Config, that are causing a resource to be noncompliant. 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 | AWSSHIELD_ADVANCED | AWSVPC


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

Required: No

LastUpdated

Timestamp of the last update to the EvaluationResult objects.

Type: Timestamp

Required: No

MemberAccount

The member account ID.

Type: String


Pattern: ^[0-9]\+$

Required: No

PolicyId

The ID of the AWS Firewall Manager policy.

Type: String

Length Constraints: Fixed length of 36.

Pattern: ^[a-zA-Z0-9\-]{36}$

Required: No
PolicyName

The friendly name of the AWS Firewall Manager policy.
Type: String
Pattern: ^([\p{L}\p{Z}\p{N}_.:/=+-@]*)$
Required: No

PolicyOwner

The AWS account that created the AWS Firewall Manager policy.
Type: String
Pattern: ^[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 Go
- AWS SDK for Java
- AWS SDK for Ruby V3
PolicySummary

Details of the AWS Firewall Manager policy.

Contents

PolicyArn

The Amazon Resource Name (ARN) of the specified policy.
Type: String
Pattern: ^([\p{L}\p{Z}\p{N}_.:/=+-@]*)$
Required: No

PolicyId

The ID of the specified policy.
Type: String
Length Constraints: Fixed length of 36.
Pattern: ^[a-z0-9A-Z-]{36}$
Required: No

PolicyName

The friendly name of the specified policy.
Type: String
Pattern: ^([\p{L}\p{Z}\p{N}_.:/=+-@]*)$
Required: No

RemediationEnabled

Indicates if the policy should be automatically applied to new resources.
Type: Boolean
Required: No

ResourceType

The type of resource protected by or in scope of the policy. This is in the format shown in the AWS Resource Types Reference. For AWS WAF and Shield Advanced, examples include AWS::ElasticLoadBalancingV2::LoadBalancer and AWS::CloudFront::Distribution. For a security group common policy, valid values are AWS::EC2::NetworkInterface and AWS::EC2::Instance. For a security group content audit policy, valid values are AWS::EC2::SecurityGroup, AWS::EC2::NetworkInterface, and AWS::EC2::Instance. For a security group usage audit policy, the value is AWS::EC2::SecurityGroup.
Type: String
Pattern: ^([\p{L}\p{Z}\p{N}_.:/=+-@]*)$

Required: No

**SecurityServiceType**

The service that the policy is using to protect the resources. This specifies the type of policy that is created, either an AWS WAF policy, a Shield Advanced policy, or a security group policy.

Type: String

Valid Values: WAF | WAFV2 | SHIELD_ADVANCED | SECURITY_GROUPS_COMMON | SECURITY_GROUPS_CONTENT_AUDIT | SECURITY_GROUPS_USAGE_AUDIT

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 V3
ResourceTag

The resource tags that AWS Firewall Manager uses to determine if a particular resource should be included or excluded from 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. Firewall Manager combines the tags with "AND" so that, if you add more than one tag to a policy scope, a resource must have all the specified tags to be included or excluded. For more information, see Working with Tag Editor.

Contents

Key

The resource tag key.

Type: String


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 V3
SecurityServicePolicyData

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

Contents

ManagedServiceData

Details about the service that are specific to the service type, in JSON format. For service type SHIELD_ADVANCED, this is an empty string.

- Example: WAFV2

  "SecurityServicePolicyData": "{"type": "WAFV2","postProcessRuleGroups": [{"managedRuleGroupIdentifier": {"managedRuleGroupName": "AWSManagedRulesAdminProtectionRuleSet","vendor": "AWS" }, "ruleGroupARN": "rulegrouparn","overrideAction": {"type": "COUNT\|NONE" }, "excludedRules": [ { \"name\": \"EntityName\" } ], "type": "ManagedRuleGroup\|RuleGroup" } ], "preProcessRuleGroups": [ { "managedRuleGroupIdentifier": { "managedRuleGroupName": "AWSManagedRulesAdminProtectionRuleSet", "vendor": "AWS" }, "ruleGroupARN": "rulegrouparn","overrideAction": {"type": "COUNT\|NONE" }, "excludedRules": [ { \"name\": \"EntityName\" } ], "type": "ManagedRuleGroup\|RuleGroup" } ], "defaultAction": { "type": "BLOCK" }"

- Example: WAF Classic

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

- Example: SECURITY_GROUPS_COMMON

  "SecurityServicePolicyData": {"Type": "SECURITY_GROUPS_COMMON","ManagedServiceData":{"type \": ": SECURITY_GROUPS_COMMON",\"revertManualSecurityGroupChanges \":false,\"exclusiveResourceSecurityGroupManagement \":false, \"applyToAllEC2InstanceENIs\":false, \"securityGroups": [{\"id\": ": sg-000e55995d61a06bd \"}],\"RemediationEnabled\":false,"ResourceType":"AWS::EC2::NetworkInterface"}

- Example: SECURITY_GROUPS_CONTENT_AUDIT

  "SecurityServicePolicyData": {"Type": "SECURITY_GROUPS_CONTENT_AUDIT","ManagedServiceData": {"type \": ": SECURITY_GROUPS_CONTENT_AUDIT",\"securityGroups": [{\"id\": ": sg-000e55995d61a06bd \"}],\"securityGroupAction": {\"type\": "ALLOW \"}}},\"RemediationEnabled\":false,"ResourceType":"AWS::EC2::NetworkInterface"

The security group action for content audit can be ALLOW or DENY. For ALLOW, all in-scope security group rules must be within the allowed range of the policy's security group rules. For DENY, all in-scope security group rules must not contain a value or a range that matches a rule value or range in the policy security group.

- Example: SECURITY_GROUPS_USAGE_AUDIT

  "SecurityServicePolicyData": {"Type": "SECURITY_GROUPS_USAGE_AUDIT","ManagedServiceData": {"type \": ": SECURITY_GROUPS_USAGE_AUDIT",\"deleteUnusedSecurityGroups \":false,"ResourceType":"AWS::EC2::NetworkInterface"}

"true,"coalesceRedundantSecurityGroups
"true}},{"RemediationEnabled":false,"Resou-
rcType":"AWS::EC2::SecurityGroup"}

Type: String


Pattern: .*

Required: No

Type

The service that the policy is using to protect the resources. This specifies the type of policy that is created, either an AWS WAF policy, a Shield Advanced policy, or a security group policy. For security group policies, Firewall Manager supports one security group for each common policy and for each content audit policy. This is an adjustable limit that you can increase by contacting AWS Support.

Type: String

Valid Values: WAF | WAFV2 | SHIELD_ADVANCED | SECURITY_GROUPS_COMMON |
SECURITY_GROUPS_CONTENT_AUDIT | SECURITY_GROUPS_USAGE_AUDIT

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 V3
Tag

A collection of key:value pairs associated with an AWS resource. The key:value pair can be anything you define. Typically, the tag key represents a category (such as "environment") and the tag value represents a specific value within that category (such as "test," "development," or "production"). You can add up to 50 tags to each AWS resource.

Contents

Key

Part of the key:value pair that defines a tag. You can use a tag key to describe a category of information, such as "customer." Tag keys are case-sensitive.

Type: String


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

Required: Yes

Value

Part of the key:value pair that defines a tag. You can use a tag value to describe a specific value within a category, such as "companyA" or "companyB." Tag values are case-sensitive.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

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

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 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 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