# Manage IPsec policies

## REST API reference

NetApp
February 11, 2026

This PDF was generated from https://docs.netapp.com/us-en/ontap-restapi/security_ipsec_policies_endpoint_overview.html on February 11, 2026. Always check docs.netapp.com for the latest.

# Table of Contents


Manage IPsec policies . . . 1
- Manage IPsec policies . . . 1
  - Overview . . . 1
- Retrieve IPsec policies . . . 1
  - Related ONTAP commands . . . 1
  - Parameters . . . 1
  - Response . . . 4
  - Error . . . 6
  - Definitions . . . 7
- Create an IPsec policy . . . 12
  - Related ONTAP commands . . . 12
  - Parameters . . . 12
  - Request Body . . . 12
  - Response . . . 14
  - Error . . . 17
  - Definitions . . . 19
- Delete an IPsec policy . . . 24
  - Related ONTAP commands . . . 24
  - Parameters . . . 25
  - Response . . . 25
  - Error . . . 25
  - Definitions . . . 26
- Retrieve an IPsec policy . . . 26
  - Related ONTAP commands . . . 26
  - Parameters . . . 26
  - Response . . . 27
  - Error . . . 30
  - Definitions . . . 30
- Update an IPsec policy . . . 33
  - Related ONTAP commands . . . 33
  - Parameters . . . 33
  - Request Body . . . 34
  - Response . . . 35
  - Error . . . 35
  - Definitions . . . 37

# Manage IPsec policies

## Manage IPsec policies

### Overview

The following operations are supported:

- Collection Get: GET security/ipsec/policies
- Creation Post: POST security/ipsec/policies
- Instance Get: GET security/ipsec/policies/uuid
- Instance Patch: PATCH security/ipsec/policies/uuid
- Instance Delete: DELETE security/ipsec/policies/uuid

## Retrieve IPsec policies

GET `/security/ipsec/policies`

**Introduced In:** 9.8

Retrieves the collection of IPsec policies.

### Related ONTAP commands

- `security ipsec policy show`

### Parameters

| Name | Type | In | Required | Description |
|---|---|---|---|---|
| authentication_method | string | query | False | Filter by authentication_method<br>• Introduced in: 9.10 |
| uuid | string | query | False | Filter by uuid |
| local_identity | string | query | False | Filter by local_identity |
| protocol | string | query | False | Filter by protocol |

| Name | Type | In | Required | Description |
|---|---|---|---|---|
| name | string | query | False | Filter by name<br>• maxLength: 64<br>• minLength: 1 |
| certificate_modify_keepsa | boolean | query | False | Filter by certificate_modify_keepsa<br>• Introduced in: 9.18 |
| remote_endpoint.netmask | string | query | False | Filter by remote_endpoint.netmask |
| remote_endpoint.port | string | query | False | Filter by remote_endpoint.port |
| remote_endpoint.address | string | query | False | Filter by remote_endpoint.address |
| remote_endpoint.family | string | query | False | Filter by remote_endpoint.family |
| remote_identity | string | query | False | Filter by remote_identity |
| enabled | boolean | query | False | Filter by enabled |
| certificate.name | string | query | False | Filter by certificate.name<br>• Introduced in: 9.10 |
| certificate.uuid | string | query | False | Filter by certificate.uuid<br>• Introduced in: 9.10 |

| Name | Type | In | Required | Description |
|---|---|---|---|---|
| local_endpoint.netmask | string | query | False | Filter by local_endpoint.netmask |
| local_endpoint.port | string | query | False | Filter by local_endpoint.port |
| local_endpoint.address | string | query | False | Filter by local_endpoint.address |
| local_endpoint.family | string | query | False | Filter by local_endpoint.family |
| scope | string | query | False | Filter by scope |
| ipspace.name | string | query | False | Filter by ipspace.name |
| ipspace.uuid | string | query | False | Filter by ipspace.uuid |
| svm.name | string | query | False | Filter by svm.name |
| svm.uuid | string | query | False | Filter by svm.uuid |
| ppk.identity | string | query | False | Filter by ppk.identity<br>• Introduced in: 9.17<br>• maxLength: 64<br>• minLength: 6 |
| action | string | query | False | Filter by action<br>• Introduced in: 9.15 |
| fields | array[string] | query | False | Specify the fields to return. |
| max_records | integer | query | False | Limit the number of records returned. |

| Name | Type | In | Required | Description |
|---|---|---|---|---|
| return_records | boolean | query | False | The default is true for GET calls. When set to false, only the number of records is returned.<br>• Default value: 1 |
| return_timeout | integer | query | False | The number of seconds to allow the call to execute before returning. When iterating over a collection, the default is 15 seconds. ONTAP returns earlier if either max records or the end of the collection is reached.<br>• Default value: 15<br>• Max value: 120<br>• Min value: 0 |
| order_by | array[string] | query | False | Order results by specified fields and optional [asc |

## Response

```
Status: 200, Ok
```

| Name | Type | Description |
|---|---|---|
| _links | _links | |
| error | error | |
| num_records | integer | Number of records |
| records | array[records] | |

**Example response**


```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist"
  },
  "num_records": 1,
  "records": [
    {
      "action": "string",
      "authentication_method": "string",
      "certificate": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "string",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "ipspace": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "Default",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "local_endpoint": {
        "address": "10.10.10.7",
```

```
        "family": "string",
        "netmask": "24",
        "port": "23"
      },
      "local_identity": "string",
      "name": "string",
      "ppk": {
        "identity": "string"
      },
      "protocol": "17",
      "remote_endpoint": {
        "address": "10.10.10.7",
        "family": "string",
        "netmask": "24",
        "port": "23"
      },
      "remote_identity": "string",
      "scope": "string",
      "svm": {
        "_links": {
          "self": {
            "href": "/api/resourcelink"
          }
        },
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  ]
}
```


## Error

```
Status: Default, Error
```

| Name | Type | Description |
|---|---|---|
| error | returned_error | |

**Example error**


```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```


## Definitions

**See Definitions**

href

| Name | Type | Description |
|---|---|---|
| href | string | |

_links

| Name | Type | Description |
|---|---|---|
| next | href | |
| self | href | |

error_arguments

| Name | Type | Description |
|---|---|---|
| code | string | Argument code |
| message | string | Message argument |

error

| Name | Type | Description |
|---|---|---|
| arguments | array[error_arguments] | Message arguments |
| code | string | Error code |
| message | string | Error message |

_links

| Name | Type | Description |
|---|---|---|
| self | href | |

certificate

Certificate for the IPsec policy.

| Name | Type | Description |
|---|---|---|
| _links | _links | |
| name | string | Certificate name |
| uuid | string | Certificate UUID |

ipspace

Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input.

| Name | Type | Description |
|---|---|---|
| _links | _links | |
| name | string | IPspace name |
| uuid | string | IPspace UUID |

local_endpoint

Local endpoint for the IPsec policy.

| Name | Type | Description |
|---|---|---|
| address | string | IPv4 or IPv6 address |
| family | string | IPv4 or IPv6 |
| netmask | string | Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, the default value is 64 with a valid range of 1 to 127. Output is always the netmask length. |
| port | string | Application port to be covered by the IPsec policy |

ppk

Post-quantum pre-shared key information.

| Name | Type | Description |
|---|---|---|
| identity | string | Post-quantum pre-shared key identity. |

remote_endpoint

Remote endpoint for the IPsec policy.

| Name | Type | Description |
|---|---|---|
| address | string | IPv4 or IPv6 address |
| family | string | IPv4 or IPv6 |

| Name | Type | Description |
|---|---|---|
| netmask | string | Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, the default value is 64 with a valid range of 1 to 127. Output is always the netmask length. |
| port | string | Application port to be covered by the IPsec policy |

svm

SVM, applies only to SVM-scoped objects.

| Name | Type | Description |
|---|---|---|
| _links | _links | |
| name | string | The name of the SVM. This field cannot be specified in a PATCH method. |
| uuid | string | The unique identifier of the SVM. This field cannot be specified in a PATCH method. |

records

IPsec policy object.

| Name | Type | Description |
|---|---|---|
| action | string | Action for the IPsec policy. |
| authentication_method | string | Authentication method for the IPsec policy. |
| certificate | certificate | Certificate for the IPsec policy. |
| certificate_modify_keepsa | boolean | Indicates whether old security associations are kept upon certificate modification. |
| enabled | boolean | Indicates whether or not the policy is enabled. |

| Name | Type | Description |
|---|---|---|
| ipspace | ipspace | Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input. |
| local_endpoint | local_endpoint | Local endpoint for the IPsec policy. |
| local_identity | string | Local Identity |
| name | string | IPsec policy name. |
| ppk | ppk | Post-quantum pre-shared key information. |
| protocol | string | Lower layer protocol to be covered by the IPsec policy. |
| remote_endpoint | remote_endpoint | Remote endpoint for the IPsec policy. |
| remote_identity | string | Remote Identity |
| scope | string | Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster". |
| svm | svm | SVM, applies only to SVM-scoped objects. |
| uuid | string | Unique identifier of the IPsec policy. |

returned_error

| Name | Type | Description |
|---|---|---|
| arguments | array[error_arguments] | Message arguments |
| code | string | Error code |
| message | string | Error message |
| target | string | The target parameter that caused the error. |

# Create an IPsec policy

POST `/security/ipsec/policies`

**Introduced In:** 9.8

Creates an IPsec policy.

## Related ONTAP commands

- `security ipsec policy create`

## Parameters

| Name | Type | In | Required | Description |
|---|---|---|---|---|
| return_records | boolean | query | False | The default is false. If set to true, the records are returned.<br>• Default value: |

## Request Body

| Name | Type | Description |
|---|---|---|
| action | string | Action for the IPsec policy. |
| authentication_method | string | Authentication method for the IPsec policy. |
| certificate | certificate | Certificate for the IPsec policy. |
| certificate_modify_keepsa | boolean | Indicates whether old security associations are kept upon certificate modification. |
| enabled | boolean | Indicates whether or not the policy is enabled. |
| ipspace | ipspace | Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input. |
| local_endpoint | local_endpoint | Local endpoint for the IPsec policy. |
| local_identity | string | Local Identity |

| Name | Type | Description |
| --- | --- | --- |
| name | string | IPsec policy name. |
| ppk | ppk | Post-quantum pre-shared key information. |
| protocol | string | Lower layer protocol to be covered by the IPsec policy. |
| remote_endpoint | remote_endpoint | Remote endpoint for the IPsec policy. |
| remote_identity | string | Remote Identity |
| secret_key | string | Pre-shared key for IKE negotiation. |
| svm | svm | SVM, applies only to SVM-scoped objects. |
| uuid | string | Unique identifier of the IPsec policy. |

**Example request**


```
{
  "action": "string",
  "authentication_method": "string",
  "certificate": {
    "name": "string",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "ipspace": {
    "name": "Default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "local_endpoint": {
    "address": "10.10.10.7",
    "netmask": "24",
    "port": "23"
  },
  "local_identity": "string",
  "name": "string",
  "ppk": {
    "identity": "string",
    "shared_key": "string"
  },
  "protocol": "17",
  "remote_endpoint": {
    "address": "10.10.10.7",
    "netmask": "24",
    "port": "23"
  },
  "remote_identity": "string",
  "secret_key": "string",
  "svm": {
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
```


## Response

```
Status: 201, Created
```

| Name | Type | Description |
| --- | --- | --- |
| num_records | integer | Number of records |
| records | array[records] | |

**Example response**


```
{
  "num_records": 1,
  "records": [
    {
      "action": "string",
      "authentication_method": "string",
      "certificate": {
        "name": "string",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "ipspace": {
        "name": "Default",
        "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
      },
      "local_endpoint": {
        "address": "10.10.10.7",
        "netmask": "24",
        "port": "23"
      },
      "local_identity": "string",
      "name": "string",
      "ppk": {
        "identity": "string",
        "shared_key": "string"
      },
      "protocol": "17",
      "remote_endpoint": {
        "address": "10.10.10.7",
        "netmask": "24",
        "port": "23"
      },
      "remote_identity": "string",
      "secret_key": "string",
      "svm": {
        "name": "svm1",
        "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
      },
      "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
    }
  ]
}
```

### Headers

| Name | Description | Type |
|---|---|---|
| Location | Useful for tracking the resource location | string |

## Error

```
Status: Default
```

ONTAP Error Response Codes

| Error Code | Description |
|---|---|
| 66257099 | Only one protocol can be specified. |
| 66257100 | Only one local port can be specified. |
| 66257101 | Only one remote port can be specified. |
| 66257102 | Internet Key Exchange version 1 (IKEv1) is not supported. |
| 66257104 | IPsec policy with same name already exists in this SVM. |
| 66257107 | The specified pre-shared key is not a valid hexadecimal string. |
| 66257109 | The specified pre-shared key is not a valid Base64 encoded binary string. |
| 66257110 | Failed to a create policy sequencing value. |
| 66257112 | The IPsec policy with the action specified does not provide packet protection and the authentication method provided for the policy will be ignored. |
| 66257113 | Only one local IP subnet can be specified. |
| 66257114 | Only one remote IP subnet can be specified. |
| 66257115 | Port ranges containing more than one port are not supported. |
| 66257117 | IPsec is not supported on the SVM specified in the policy, IPsec is supported on data SVMs only. |
| 66257120 | The subnet selector must be a host address (An IPv4 address with a 32-bit netmask or an IPv6 address with a 128-bit netmask). |
| 66257121 | The maximum limit of IPsec policies has been reached for the specified SVM. |
| 66257125 | The local_endpoint.address must be specified with local_endpoint.netmask. |

| Error Code | Description |
| --- | --- |
| 66257126 | The remote_endpoint.address must be specified with remote_endpoint.netmask. |
| 66257127 | The local subnet must be configured as a non-zero subnet. |
| 66257128 | Invalid ANY wildcard subnet. |
| 66257129 | A specific local or remote port number is required when the remote subnet is configured as an ANY wildcard subnet. |
| 66257130 | The maximum limit of IPsec policies has been reached for the cluster. |
| 66257131 | ESP in UDPv6 Encapsulation is not supported. |
| 66257132 | Invalid value for port field. Value should be in range <0-65535>. |
| 66257133 | A pre-shared key is needed for the PSK authentication method. Use the secret_key option to specify a key. |
| 66257134 | An end-entity certificate is needed for the PKI authentication method. Use the certificate.uuid option to specify an end-entity certificate. |
| 66257135 | The specified certificate is not found on the SVM. |
| 66257136 | A certificate is not needed for the PSK authentication method. |
| 66257137 | A pre-shared key is not needed for the PKI authentication method. |
| 66257138 | Remote identity is required when using certificate verification. |
| 66257139 | Certificate with the specified UUID was not found. |
| 66257140 | Only certificates with a client or server type are supported. |
| 66257142 | Failed to create IPsec policy because the specified SVM is being migrated. |
| 66257143 | Invalid IPsec policy provided. The subnet must be non-empty. |
| 66257144 | The IPsec policy actions ESP TRANSPORT and ESP UDP each provide packet protection and requires a secret key or certificate for authentication. |
| 66257148 | The policy name does not meet required ASCII-range characters length. |
| 66257153 | The policy requires a post-quantum pre-shared key because ppk-identity is specified for this policy. |

| Error Code | Description |
| --- | --- |
| 66257154 | The policy requires a post-quantum pre-shared identity because ppk-shared-key is specified for this policy. |
| 66257199 | Not all of the nodes in the cluster are running a version that supports the IPsec feature. |
| 66257200 | The shared key does not meet required ASCII-range characters length. |
| 66257201 | Support for the feature available with effective cluster version or later. |
| 66257202 | The specified SVM name is invalid. |
| 66257203 | The specified SVM UUID is invalid. |
| 66257204 | The specified IPspace UUID and IPspace name refer to different IPspaces. |
| 66257205 | The specified SVM must exist in the specified IPspace. |
| 66257305 | The certificate UUID does not match the provided certificate name. |
| 66257396 | IPsec is not supported for the admin SVM in a MetroCluster configuration. |

Also see the table of common errors in the Response body overview section of this documentation.

## Definitions

**See Definitions**

href

| Name | Type | Description |
|---|---|---|
| href | string | |

_links

certificate

Certificate for the IPsec policy.

| Name | Type | Description |
|---|---|---|
| name | string | Certificate name |
| uuid | string | Certificate UUID |

ipspace

Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input.

| Name | Type | Description |
|---|---|---|
| name | string | IPspace name |
| uuid | string | IPspace UUID |

local_endpoint

Local endpoint for the IPsec policy.

| Name | Type | Description |
|---|---|---|
| address | string | IPv4 or IPv6 address |
| netmask | string | Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, the default value is 64 with a valid range of 1 to 127. Output is always the netmask length. |
| port | string | Application port to be covered by the IPsec policy |

ppk

Post-quantum pre-shared key information.

| Name | Type | Description |
|---|---|---|
| identity | string | Post-quantum pre-shared key identity. |
| shared_key | string | Post-quantum pre-shared key. |

remote_endpoint

Remote endpoint for the IPsec policy.

| Name | Type | Description |
|---|---|---|
| address | string | IPv4 or IPv6 address |
| netmask | string | Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, the default value is 64 with a valid range of 1 to 127. Output is always the netmask length. |
| port | string | Application port to be covered by the IPsec policy |

svm

SVM, applies only to SVM-scoped objects.

| Name | Type | Description |
|---|---|---|
| name | string | The name of the SVM. This field cannot be specified in a PATCH method. |
| uuid | string | The unique identifier of the SVM. This field cannot be specified in a PATCH method. |

ipsec_policy

IPsec policy object.

| Name | Type | Description |
|---|---|---|
| action | string | Action for the IPsec policy. |
| authentication_method | string | Authentication method for the IPsec policy. |

| Name | Type | Description |
| --- | --- | --- |
| certificate | certificate | Certificate for the IPsec policy. |
| certificate_modify_keepsa | boolean | Indicates whether old security associations are kept upon certificate modification. |
| enabled | boolean | Indicates whether or not the policy is enabled. |
| ipspace | ipspace | Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input. |
| local_endpoint | local_endpoint | Local endpoint for the IPsec policy. |
| local_identity | string | Local Identity |
| name | string | IPsec policy name. |
| ppk | ppk | Post-quantum pre-shared key information. |
| protocol | string | Lower layer protocol to be covered by the IPsec policy. |
| remote_endpoint | remote_endpoint | Remote endpoint for the IPsec policy. |
| remote_identity | string | Remote Identity |
| secret_key | string | Pre-shared key for IKE negotiation. |
| svm | svm | SVM, applies only to SVM-scoped objects. |
| uuid | string | Unique identifier of the IPsec policy. |

error_arguments

| Name | Type | Description |
|---|---|---|
| code | string | Argument code |
| message | string | Message argument |

error

| Name | Type | Description |
|---|---|---|
| arguments | array[error_arguments] | Message arguments |
| code | string | Error code |
| message | string | Error message |

records

IPsec policy object.

| Name | Type | Description |
|---|---|---|
| action | string | Action for the IPsec policy. |
| authentication_method | string | Authentication method for the IPsec policy. |
| certificate | certificate | Certificate for the IPsec policy. |
| certificate_modify_keepsa | boolean | Indicates whether old security associations are kept upon certificate modification. |
| enabled | boolean | Indicates whether or not the policy is enabled. |
| ipspace | ipspace | Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input. |
| local_endpoint | local_endpoint | Local endpoint for the IPsec policy. |
| local_identity | string | Local Identity |
| name | string | IPsec policy name. |

| Name | Type | Description |
|---|---|---|
| ppk | ppk | Post-quantum pre-shared key information. |
| protocol | string | Lower layer protocol to be covered by the IPsec policy. |
| remote_endpoint | remote_endpoint | Remote endpoint for the IPsec policy. |
| remote_identity | string | Remote Identity |
| secret_key | string | Pre-shared key for IKE negotiation. |
| svm | svm | SVM, applies only to SVM-scoped objects. |
| uuid | string | Unique identifier of the IPsec policy. |

returned_error

| Name | Type | Description |
|---|---|---|
| arguments | array[error_arguments] | Message arguments |
| code | string | Error code |
| message | string | Error message |
| target | string | The target parameter that caused the error. |

# Delete an IPsec policy

DELETE `/security/ipsec/policies/{uuid}`

**Introduced In:** 9.8

Deletes a specific IPsec policy.

## Related ONTAP commands

- `security ipsec policy delete`

## Parameters

| Name | Type | In | Required | Description |
|---|---|---|---|---|
| uuid | string | path | True | IPsec policy UUID |

## Response

```
Status: 200, Ok
```

## Error

```
Status: Default
```

ONTAP Error Response Codes

| Error Code | Description |
|---|---|
| 66257096 | Internal error. Failed to purge connections associated with the IPsec policy. |

Also see the table of common errors in the Response body overview section of this documentation.

| Name | Type | Description |
|---|---|---|
| error | returned_error | |

**Example error**


```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```

## Definitions

### See Definitions

error_arguments

| Name | Type | Description |
|---|---|---|
| code | string | Argument code |
| message | string | Message argument |

returned_error

| Name | Type | Description |
|---|---|---|
| arguments | array[error_arguments] | Message arguments |
| code | string | Error code |
| message | string | Error message |
| target | string | The target parameter that caused the error. |

# Retrieve an IPsec policy

GET `/security/ipsec/policies/{uuid}`

**Introduced In:** 9.8

Retrieves a specific IPsec policy.

## Related ONTAP commands

- `security ipsec policy show`

## Parameters

| Name | Type | In | Required | Description |
|---|---|---|---|---|
| uuid | string | path | True | IPsec policy UUID |
| fields | array[string] | query | False | Specify the fields to return. |

## Response

```
Status: 200, Ok
```

| Name | Type | Description |
|---|---|---|
| action | string | Action for the IPsec policy. |
| authentication_method | string | Authentication method for the IPsec policy. |
| certificate | certificate | Certificate for the IPsec policy. |
| certificate_modify_keepsa | boolean | Indicates whether old security associations are kept upon certificate modification. |
| enabled | boolean | Indicates whether or not the policy is enabled. |
| ipspace | ipspace | Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input. |
| local_endpoint | local_endpoint | Local endpoint for the IPsec policy. |
| local_identity | string | Local Identity |
| name | string | IPsec policy name. |
| ppk | ppk | Post-quantum pre-shared key information. |
| protocol | string | Lower layer protocol to be covered by the IPsec policy. |
| remote_endpoint | remote_endpoint | Remote endpoint for the IPsec policy. |
| remote_identity | string | Remote Identity |
| scope | string | Set to "svm" for interfaces owned by an SVM. Otherwise, set to "cluster". |

| Name | Type | Description |
| --- | --- | --- |
| svm | svm | SVM, applies only to SVM-scoped objects. |
| uuid | string | Unique identifier of the IPsec policy. |

**Example response**


```
{
  "action": "string",
  "authentication_method": "string",
  "certificate": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "string",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "ipspace": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "name": "Default",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "local_endpoint": {
    "address": "10.10.10.7",
    "family": "string",
    "netmask": "24",
    "port": "23"
  },
  "local_identity": "string",
  "name": "string",
  "ppk": {
    "identity": "string"
  },
  "protocol": "17",
  "remote_endpoint": {
    "address": "10.10.10.7",
    "family": "string",
    "netmask": "24",
    "port": "23"
  },
  "remote_identity": "string",
  "scope": "string",
  "svm": {
    "_links": {
      "self": {
```

```
        "href": "/api/resourcelink"
      }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
  },
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
```


## Error

```
Status: Default, Error
```

| Name | Type | Description |
|---|---|---|
| error | returned_error | |

**Example error**


```
{
  "error": {
    "arguments": [
      {
        "code": "string",
        "message": "string"
      }
    ],
    "code": "4",
    "message": "entry doesn't exist",
    "target": "uuid"
  }
}
```


## Definitions

**See Definitions**

href

| Name | Type | Description |
|---|---|---|
| href | string | |

_links

| Name | Type | Description |
|---|---|---|
| self | href | |

certificate

Certificate for the IPsec policy.

| Name | Type | Description |
|---|---|---|
| _links | _links | |
| name | string | Certificate name |
| uuid | string | Certificate UUID |

ipspace

Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input.

| Name | Type | Description |
|---|---|---|
| _links | _links | |
| name | string | IPspace name |
| uuid | string | IPspace UUID |

local_endpoint

Local endpoint for the IPsec policy.

| Name | Type | Description |
|---|---|---|
| address | string | IPv4 or IPv6 address |
| family | string | IPv4 or IPv6 |

| Name | Type | Description |
|---|---|---|
| netmask | string | Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, the default value is 64 with a valid range of 1 to 127. Output is always the netmask length. |
| port | string | Application port to be covered by the IPsec policy |

ppk

Post-quantum pre-shared key information.

| Name | Type | Description |
|---|---|---|
| identity | string | Post-quantum pre-shared key identity. |

remote_endpoint

Remote endpoint for the IPsec policy.

| Name | Type | Description |
|---|---|---|
| address | string | IPv4 or IPv6 address |
| family | string | IPv4 or IPv6 |
| netmask | string | Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, the default value is 64 with a valid range of 1 to 127. Output is always the netmask length. |
| port | string | Application port to be covered by the IPsec policy |

svm

SVM, applies only to SVM-scoped objects.

| Name | Type | Description |
|---|---|---|
| _links | _links | |
| name | string | The name of the SVM. This field cannot be specified in a PATCH method. |

| Name | Type | Description |
|---|---|---|
| uuid | string | The unique identifier of the SVM. This field cannot be specified in a PATCH method. |

error_arguments

| Name | Type | Description |
|---|---|---|
| code | string | Argument code |
| message | string | Message argument |

returned_error

| Name | Type | Description |
|---|---|---|
| arguments | array[error_arguments] | Message arguments |
| code | string | Error code |
| message | string | Error message |
| target | string | The target parameter that caused the error. |

# Update an IPsec policy

PATCH `/security/ipsec/policies/{uuid}`

**Introduced In:** 9.8

Updates a specific IPsec policy.

## Related ONTAP commands

- `security ipsec policy modify`

## Parameters

| Name | Type | In | Required | Description |
|---|---|---|---|---|
| uuid | string | path | True | IPsec policy UUID |

## Request Body

| Name | Type | Description |
|---|---|---|
| certificate | certificate | Certificate for the IPsec policy. |
| certificate_modify_keepsa | boolean | Indicates whether old security associations are kept upon certificate modification. |
| enabled | boolean | Indicates whether or not the policy is enabled. |
| local_endpoint | local_endpoint | Local endpoint for the IPsec policy. |
| local_identity | string | Local Identity |
| ppk | ppk | Post-quantum pre-shared key information. |
| protocol | string | Lower layer protocol to be covered by the IPsec policy. |
| remote_endpoint | remote_endpoint | Remote endpoint for the IPsec policy. |
| remote_identity | string | Remote Identity |
| uuid | string | Unique identifier of the IPsec policy. |

**Example request**

```
{
  "certificate": {
    "name": "string",
    "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
  },
  "local_endpoint": {
    "address": "10.10.10.7",
    "netmask": "24",
    "port": "23"
  },
  "local_identity": "string",
  "ppk": {
    "identity": "string"
  },
  "protocol": "17",
  "remote_endpoint": {
    "address": "10.10.10.7",
    "netmask": "24",
    "port": "23"
  },
  "remote_identity": "string",
  "uuid": "1cd8a442-86d1-11e0-ae1c-123478563412"
}
```

## Response

```
Status: 200, Ok
```

## Error

```
Status: Default
```

ONTAP Error Response Codes

| Error Code | Description |
|---|---|
| 66257097 | Internal error. Failed to update the IPsec policy. |
| 66257099 | Only one protocol can be specified. |
| 66257100 | Only one local port can be specified. |

| Error Code | Description |
| --- | --- |
| 66257101 | Only one remote port can be specified. |
| 66257110 | Failed to create a policy sequencing value. |
| 66257113 | Only one local IP subnet can be specified. |
| 66257114 | Only one remote IP subnet can be specified. |
| 66257115 | Port ranges containing more than one port are not supported. |
| 66257120 | The subnet selector must be a host address (An IPv4 address with a 32-bit netmask or an IPv6 address with a 128-bit netmask). |
| 66257125 | The local_endpoint.address must be specified with local_endpoint.netmask. |
| 66257126 | The remote_endpoint.address must be specified with remote_endpoint.netmask. |
| 66257127 | The local subnet must be configured as a non-zero subnet. |
| 66257128 | Invalid ANY wildcard subnet. |
| 66257129 | A specific local or remote port number is required when the remote subnet is configured as an ANY wildcard subnet. |
| 66257131 | ESP in UDPv6 Encapsulation is not supported. |
| 66257135 | The specified certificate is not found on the SVM. |
| 66257136 | A certificate is not needed for the PSK authentication method. |
| 66257138 | Remote identity is required when using certificate verification. |
| 66257139 | Certificate with the specified UUID was not found. |
| 66257140 | Only certificates with a client or server type are supported. |
| 66257142 | Failed to create IPsec policy because the specified SVM is being migrated. |
| 66257143 | Invalid IPsec policy provided. The subnet must be non-empty. |
| 66257153 | The policy requires a post-quantum pre-shared key because ppk-identity is specified for this policy. |
| 66257154 | The policy requires a post-quantum pre-shared identity because ppk-shared-key is specified for this policy. |
| 66257199 | Not all of the nodes in the cluster are running a version that supports the IPsec feature. |

| Error Code | Description |
| --- | --- |
| 66257200 | The shared key does not meet required ASCII-range characters length. |
| 66257201 | Support for the feature available with effective cluster version or later. |
| 66257305 | The certificate UUID does not match the provided certificate name. |

Also see the table of common errors in the Response body overview section of this documentation.

## Definitions

**See Definitions**

href

| Name | Type | Description |
|---|---|---|
| href | string | |

_links

certificate

Certificate for the IPsec policy.

| Name | Type | Description |
|---|---|---|
| name | string | Certificate name |
| uuid | string | Certificate UUID |

ipspace

Applies to both SVM and cluster-scoped objects. Either the UUID or name may be supplied on input.

| Name | Type | Description |
|---|---|---|
| name | string | IPspace name |
| uuid | string | IPspace UUID |

local_endpoint

Local endpoint for the IPsec policy.

| Name | Type | Description |
|---|---|---|
| address | string | IPv4 or IPv6 address |
| netmask | string | Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, the default value is 64 with a valid range of 1 to 127. Output is always the netmask length. |
| port | string | Application port to be covered by the IPsec policy |

ppk

Post-quantum pre-shared key information.

| Name | Type | Description |
|---|---|---|
| identity | string | Post-quantum pre-shared key identity. |

remote_endpoint

Remote endpoint for the IPsec policy.

| Name | Type | Description |
|---|---|---|
| address | string | IPv4 or IPv6 address |
| netmask | string | Input as netmask length (16) or IPv4 mask (255.255.0.0). For IPv6, the default value is 64 with a valid range of 1 to 127. Output is always the netmask length. |
| port | string | Application port to be covered by the IPsec policy |

svm

SVM, applies only to SVM-scoped objects.

| Name | Type | Description |
|---|---|---|
| name | string | The name of the SVM. This field cannot be specified in a PATCH method. |
| uuid | string | The unique identifier of the SVM. This field cannot be specified in a PATCH method. |

ipsec_policy

IPsec policy object.

| Name | Type | Description |
|---|---|---|
| certificate | certificate | Certificate for the IPsec policy. |
| certificate_modify_keepsa | boolean | Indicates whether old security associations are kept upon certificate modification. |

| Name | Type | Description |
|---|---|---|
| enabled | boolean | Indicates whether or not the policy is enabled. |
| local_endpoint | local_endpoint | Local endpoint for the IPsec policy. |
| local_identity | string | Local Identity |
| ppk | ppk | Post-quantum pre-shared key information. |
| protocol | string | Lower layer protocol to be covered by the IPsec policy. |
| remote_endpoint | remote_endpoint | Remote endpoint for the IPsec policy. |
| remote_identity | string | Remote Identity |
| uuid | string | Unique identifier of the IPsec policy. |

error_arguments

| Name | Type | Description |
|---|---|---|
| code | string | Argument code |
| message | string | Message argument |

returned_error

| Name | Type | Description |
|---|---|---|
| arguments | array[error_arguments] | Message arguments |
| code | string | Error code |
| message | string | Error message |
| target | string | The target parameter that caused the error. |

## Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.