



# **Manage FPolicy configuration**

## **ONTAP 9.13.1 REST API reference**

NetApp  
May 08, 2024

This PDF was generated from [https://docs.netapp.com/us-en/ontap-restapi-9131/ontap/protocols\\_fpolicy\\_endpoint\\_overview.html](https://docs.netapp.com/us-en/ontap-restapi-9131/ontap/protocols_fpolicy_endpoint_overview.html) on May 08, 2024. Always check docs.netapp.com for the latest.

# Table of Contents

- Manage FPolicy configuration ..... 1
  - Protocols fpolicy endpoint overview ..... 1
  - Retrieve an FPolicy configuration ..... 8
  - Create an FPolicy configuration ..... 34
  - Delete the FPolicy configuration for an SVM ..... 55
  - Retrieve the FPolicy configuration for an SVM ..... 57

# Manage FPolicy configuration

## Protocols fpolicy endpoint overview

### Overview

FPolicy is an infrastructure component of ONTAP that enables partner applications to connect to ONTAP in order to monitor and set file access permissions. Every time a client accesses a file from a storage system, based on the configuration of FPolicy, the partner application is notified about file access. This enables partners to set restrictions on files that are created or accessed on the storage system. FPolicy also allows you to create file policies that specify file operation permissions according to file type. For example, you can restrict certain file types, such as .jpeg and .mp3 files, from being stored on the storage system. FPolicy can monitor file access from CIFS and NFS clients.

As part of FPolicy configuration, you can specify an FPolicy engine which defines the external FPolicy server, FPolicy events, which defines the protocol and file operations to monitor and the FPolicy policy that acts as a container for the FPolicy engine and FPolicy events. It provides a way for policy management functions, such as policy enabling and disabling.

### Examples

#### Creating an FPolicy configuration

To create an FPolicy for an SVM use the following API. Note that the *return\_records=true* query parameter is used to obtain the newly created entry in the response.

```
# The API:
POST /protocols/fpolicy/

#The call:
curl -X POST "https://<mgmt-ip>/api/protocols/fpolicy?return_records=true"
-H "accept: application/json" -H "Content-Type: application/json" -d "{
  \"engines\": [ { \"name\": \"engine1\", \"port\": 9876,
  \"primary_servers\": [ \"10.132.145.22\", \"10.140.101.109\" ],
  \"secondary_servers\": [ \"10.132.145.20\", \"10.132.145.21\" ], \"type\":
  \"synchronous\", \"format\": \"xml\" } ], \"events\": [ {
  \"file_operations\": { \"read\": true, \"write\": true }, \"filters\": {
  \"monitor_ads\": true }, \"name\": \"event_cifs\", \"protocol\": \"cifs\",
  \"volume_monitoring\": true } ], \"policies\": [ { \"engine\": { \"name\":
  \"engine1\" }, \"events\": [ { \"name\": \"event_cifs\" } ],
  \"mandatory\": true, \"name\": \"pol10\", \"priority\": 1, \"scope\": {
  \"include_volumes\": [ \"vol1\" ] } } ], \"svm\": { \"name\": \"vs1\",
  \"uuid\": \"b34f5e3d-01d0-11e9-8f63-0050568ea311\" } }]"

# The response:
{
  \"num_records\": 1,
  \"records\": [
```

```

{
  "svm": {
    "uuid": "b34f5e3d-01d0-11e9-8f63-0050568ea311",
    "name": "vs1"
  },
  "engines": [
    {
      "name": "engine1",
      "primary_servers": [
        "10.132.145.22",
        "10.140.101.109"
      ],
      "secondary_servers": [
        "10.132.145.20",
        "10.132.145.21"
      ],
      "type": "synchronous",
      "port": 9876,
      "format": "xml"
    }
  ],
  "events": [
    {
      "name": "event_cifs",
      "protocol": "cifs",
      "volume_monitoring": true,
      "file_operations": {
        "read": true,
        "write": true
      },
      "filters": {
        "monitor_ads": true
      }
    }
  ],
  "policies": [
    {
      "name": "pol0",
      "priority": 1,
      "events": [
        {
          "name": "event_cifs"
        }
      ],
      "engine": {
        "name": "engine1"
      }
    }
  ]
}

```

```

    },
    "scope": {
        "include_volumes": [
            "vol1"
        ]
    },
    "mandatory": true
}
]
}
}

```

## Retrieving the FPolicy configuration for all the SVMs in the cluster

```

# The API:
GET /protocols/fpolicy

# The call:
curl -X GET "https://<mgmt-
ip>/api/protocols/fpolicy?fields=*&return_records=true&return_timeout=15"
-H "accept: application/json"

# The response:
{
  "records": [
    {
      "svm": {
        "uuid": "b34f5e3d-01d0-11e9-8f63-0050568ea311",
        "name": "vs1"
      },
      "engines": [
        {
          "name": "engine1",
          "primary_servers": [
            "10.132.145.22",
            "10.140.101.109"
          ],
          "secondary_servers": [
            "10.132.145.20",
            "10.132.145.21"
          ]
        }
      ]
    }
  ]
}

```

```

    "type": "synchronous",
    "port": 9876,
    "format": "xml"
  }
],
"events": [
  {
    "name": "event_cifs",
    "protocol": "cifs",
    "volume_monitoring": true,
    "file_operations": {
      "close": false,
      "create": false,
      "create_dir": false,
      "delete": false,
      "delete_dir": false,
      "getattr": false,
      "link": false,
      "lookup": false,
      "open": false,
      "read": true,
      "write": true,
      "rename": false,
      "rename_dir": false,
      "setattr": false,
      "symlink": false
    },
    "filters": {
      "monitor_ads": true,
      "close_with_modification": false,
      "close_without_modification": false,
      "close_with_read": false,
      "first_read": false,
      "first_write": false,
      "offline_bit": false,
      "open_with_delete_intent": false,
      "open_with_write_intent": false,
      "write_with_size_change": false,
      "setattr_with_owner_change": false,
      "setattr_with_group_change": false,
      "setattr_with_sacl_change": false,
      "setattr_with_dacl_change": false,
      "setattr_with_modify_time_change": false,
      "setattr_with_access_time_change": false,
      "setattr_with_creation_time_change": false,
      "setattr_with_mode_change": false,

```

```

        "setattr_with_size_change": false,
        "setattr_with_allocation_size_change": false,
        "exclude_directory": false
    }
}
],
"policies": [
{
    "name": "pol0",
    "enabled": true,
    "priority": 1,
    "events": [
        {
            "name": "event_cifs"
        }
    ],
    "engine": {
        "name": "engine1"
    },
    "scope": {
        "include_volumes": [
            "vol1"
        ]
    },
    "mandatory": true,
    "passthrough_read": false,
    "allow_privileged_access": false
}
]
}
],
"num_records": 1
}

```

## Retrieving an FPolicy configuration for a particular SVM

```

# The API:
GET /protocols/fpolicy/{svm.uuid}

# The call:
curl -X GET "https://<mgmt-ip>/api/protocols/fpolicy/b34f5e3d-01d0-11e9-8f63-0050568ea311?fields=*&return_records=true&return_timeout=15" -H

```

```

"accept: application/json"

# The response:
{
  "svm": {
    "uuid": "b34f5e3d-01d0-11e9-8f63-0050568ea311",
    "name": "vs1"
  },
  "engines": [
    {
      "name": "engine1",
      "primary_servers": [
        "10.132.145.22",
        "10.140.101.109"
      ],
      "secondary_servers": [
        "10.132.145.20",
        "10.132.145.21"
      ],
      "type": "synchronous",
      "port": 9876,
      "format": "xml"
    }
  ],
  "events": [
    {
      "name": "event_cifs",
      "protocol": "cifs",
      "volume_monitoring": true,
      "file_operations": {
        "close": false,
        "create": false,
        "create_dir": false,
        "delete": false,
        "delete_dir": false,
        "getattr": false,
        "link": false,
        "lookup": false,
        "open": false,
        "read": true,
        "write": true,
        "rename": false,
        "rename_dir": false,
        "setattr": false,
        "symlink": false
      }
    },

```



```

"filters": {
  "monitor_ads": true,
  "close_with_modification": false,
  "close_without_modification": false,
  "close_with_read": false,
  "first_read": false,
  "first_write": false,
  "offline_bit": false,
  "open_with_delete_intent": false,
  "open_with_write_intent": false,
  "write_with_size_change": false,
  "setattr_with_owner_change": false,
  "setattr_with_group_change": false,
  "setattr_with_sacl_change": false,
  "setattr_with_dacl_change": false,
  "setattr_with_modify_time_change": false,
  "setattr_with_access_time_change": false,
  "setattr_with_creation_time_change": false,
  "setattr_with_mode_change": false,
  "setattr_with_size_change": false,
  "setattr_with_allocation_size_change": false,
  "exclude_directory": false
}
},
"policies": [
{
  "name": "pol0",
  "enabled": true,
  "priority": 1,
  "events": [
    {
      "name": "event_cifs"
    }
  ],
  "engine": {
    "name": "engine1"
  },
  "scope": {
    "include_volumes": [
      "vol1"
    ]
  },
  "mandatory": true,
  "passthrough_read": false,
  "allow_privileged_access": false
}
]

```

```
}  
]  
}
```

## Deleting an FPolicy configuration for a particular SVM

```
# The API:  
DELETE /protocols/fpolicy/{svm.uuid}  
  
# The call:  
curl -X DELETE "https://<mgmt-ip>/api/protocols/fpolicy/b34f5e3d-01d0-  
11e9-8f63-0050568ea311" -H "accept: application/json"
```

## Retrieve an FPolicy configuration

GET /protocols/fpolicy

**Introduced In:** 9.6

Retrieves an FPolicy configuration.

### Related ONTAP commands

- `fpolicy show`
- `fpolicy policy show`
- `fpolicy policy scope show`
- `fpolicy policy event show`
- `fpolicy policy external-engine show`

### Learn more

- [DOC /protocols/fpolicy](#)

### Parameters

Name	Type	In	Required	Description
events.file_operation s.write	boolean	query	False	Filter by events.file_operation s.write

Name	Type	In	Required	Description
events.file_operation s.access	boolean	query	False	Filter by events.file_operation s.access  • Introduced in: 9.13
events.file_operation s.rename	boolean	query	False	Filter by events.file_operation s.rename
events.file_operation s.create	boolean	query	False	Filter by events.file_operation s.create
events.file_operation s.delete	boolean	query	False	Filter by events.file_operation s.delete
events.file_operation s.symlink	boolean	query	False	Filter by events.file_operation s.symlink
events.file_operation s.lookup	boolean	query	False	Filter by events.file_operation s.lookup
events.file_operation s.rename_dir	boolean	query	False	Filter by events.file_operation s.rename_dir
events.file_operation s.open	boolean	query	False	Filter by events.file_operation s.open
events.file_operation s.create_dir	boolean	query	False	Filter by events.file_operation s.create_dir
events.file_operation s.link	boolean	query	False	Filter by events.file_operation s.link
events.file_operation s.setattr	boolean	query	False	Filter by events.file_operation s.setattr

Name	Type	In	Required	Description
events.file_operations.read	boolean	query	False	Filter by events.file_operations.read
events.file_operations.delete_dir	boolean	query	False	Filter by events.file_operations.delete_dir
events.file_operations.close	boolean	query	False	Filter by events.file_operations.close
events.file_operations.getattr	boolean	query	False	Filter by events.file_operations.getattr
events.name	string	query	False	Filter by events.name
events.filters.write_with_size_change	boolean	query	False	Filter by events.filters.write_with_size_change
events.filters.setattr_with_modify_time_change	boolean	query	False	Filter by events.filters.setattr_with_modify_time_change
events.filters.setattr_with_dacl_change	boolean	query	False	Filter by events.filters.setattr_with_dacl_change
events.filters.first_write	boolean	query	False	Filter by events.filters.first_write
events.filters.setattr_with_group_change	boolean	query	False	Filter by events.filters.setattr_with_group_change
events.filters.open_with_delete_intent	boolean	query	False	Filter by events.filters.open_with_delete_intent
events.filters.setattr_with_size_change	boolean	query	False	Filter by events.filters.setattr_with_size_change

Name	Type	In	Required	Description
events.filters.setattr_with_allocation_size_change	boolean	query	False	Filter by events.filters.setattr_with_allocation_size_change
events.filters.monitor_ads	boolean	query	False	Filter by events.filters.monitor_ads
events.filters.setattr_with_owner_change	boolean	query	False	Filter by events.filters.setattr_with_owner_change
events.filters.close_without_modification	boolean	query	False	Filter by events.filters.close_without_modification
events.filters.close_with_read	boolean	query	False	Filter by events.filters.close_with_read
events.filters.setattr_with_sacl_change	boolean	query	False	Filter by events.filters.setattr_with_sacl_change
events.filters.setattr_with_access_time_change	boolean	query	False	Filter by events.filters.setattr_with_access_time_change
events.filters.close_with_modification	boolean	query	False	Filter by events.filters.close_with_modification
events.filters.offline_bit	boolean	query	False	Filter by events.filters.offline_bit
events.filters.exclude_directory	boolean	query	False	Filter by events.filters.exclude_directory
events.filters.first_read	boolean	query	False	Filter by events.filters.first_read

Name	Type	In	Required	Description
events.filters.setattr_with_mode_change	boolean	query	False	Filter by events.filters.setattr_with_mode_change
events.filters.setattr_with_creation_time_change	boolean	query	False	Filter by events.filters.setattr_with_creation_time_change
events.filters.open_with_write_intent	boolean	query	False	Filter by events.filters.open_with_write_intent
events.volume_monitoring	boolean	query	False	Filter by events.volume_monitoring
events.monitor_fileop_failure	boolean	query	False	Filter by events.monitor_fileop_failure <ul style="list-style-type: none"> <li>• Introduced in: 9.13</li> </ul>
events.protocol	string	query	False	Filter by events.protocol
engines.type	string	query	False	Filter by engines.type
engines.buffer_size.recv_buffer	integer	query	False	Filter by engines.buffer_size.recv_buffer <ul style="list-style-type: none"> <li>• Introduced in: 9.11</li> <li>• Max value: 7895160</li> <li>• Min value: 0</li> </ul>

Name	Type	In	Required	Description
engines.buffer_size. send_buffer	integer	query	False	Filter by engines.buffer_size. send_buffer <ul style="list-style-type: none"> <li>• Introduced in: 9.11</li> <li>• Max value: 7895160</li> <li>• Min value: 0</li> </ul>
engines.request_cancel_timeout	string	query	False	Filter by engines.request_cancel_timeout <ul style="list-style-type: none"> <li>• Introduced in: 9.11</li> </ul>
engines.format	string	query	False	Filter by engines.format <ul style="list-style-type: none"> <li>• Introduced in: 9.11</li> </ul>
engines.primary_servers	string	query	False	Filter by engines.primary_servers
engines.port	integer	query	False	Filter by engines.port
engines.secondary_servers	string	query	False	Filter by engines.secondary_servers
engines.name	string	query	False	Filter by engines.name
engines.max_server_requests	integer	query	False	Filter by engines.max_server_requests <ul style="list-style-type: none"> <li>• Introduced in: 9.11</li> <li>• Max value: 10000</li> <li>• Min value: 1</li> </ul>

Name	Type	In	Required	Description
engines.status_request_interval	string	query	False	Filter by engines.status_request_interval  • Introduced in: 9.11
engines.keep_alive_interval	string	query	False	Filter by engines.keep_alive_interval  • Introduced in: 9.13
engines.ssl_option	string	query	False	Filter by engines.ssl_option  • Introduced in: 9.11
engines.server_progress_timeout	string	query	False	Filter by engines.server_progress_timeout  • Introduced in: 9.11
engines.resiliency.directory_path	string	query	False	Filter by engines.resiliency.directory_path  • Introduced in: 9.11
engines.resiliency.retention_duration	string	query	False	Filter by engines.resiliency.retention_duration  • Introduced in: 9.11
engines.resiliency.enabled	boolean	query	False	Filter by engines.resiliency.enabled  • Introduced in: 9.11



Name	Type	In	Required	Description
engines.certificate.serial_number	string	query	False	Filter by engines.certificate.serial_number  • Introduced in: 9.11
engines.certificate.ca	string	query	False	Filter by engines.certificate.ca  • Introduced in: 9.11
engines.certificate.name	string	query	False	Filter by engines.certificate.name  • Introduced in: 9.11
engines.request_abort_timeout	string	query	False	Filter by engines.request_abort_timeout  • Introduced in: 9.11
policies.engine.name	string	query	False	Filter by policies.engine.name
policies.privileged_user	string	query	False	Filter by policies.privileged_user  • Introduced in: 9.11
policies.enabled	boolean	query	False	Filter by policies.enabled
policies.passthrough_read	boolean	query	False	Filter by policies.passthrough_read  • Introduced in: 9.11

Name	Type	In	Required	Description
policies.mandatory	boolean	query	False	Filter by policies.mandatory
policies.name	string	query	False	Filter by policies.name
policies.priority	integer	query	False	Filter by policies.priority <ul style="list-style-type: none"> <li>• Max value: 10</li> <li>• Min value: 1</li> </ul>
policies.allow_privileged_access	boolean	query	False	Filter by policies.allow_privileged_access <ul style="list-style-type: none"> <li>• Introduced in: 9.13</li> </ul>
policies.scope.exclude_export_policies	string	query	False	Filter by policies.scope.exclude_export_policies
policies.scope.include_volumes	string	query	False	Filter by policies.scope.include_volumes
policies.scope.check_extensions_on_directories	boolean	query	False	Filter by policies.scope.check_extensions_on_directories <ul style="list-style-type: none"> <li>• Introduced in: 9.11</li> </ul>
policies.scope.include_export_policies	string	query	False	Filter by policies.scope.include_export_policies
policies.scope.object_monitoring_with_no_extension	boolean	query	False	Filter by policies.scope.object_monitoring_with_no_extension <ul style="list-style-type: none"> <li>• Introduced in: 9.11</li> </ul>

Name	Type	In	Required	Description
policies.scope.exclude_shares	string	query	False	Filter by policies.scope.exclude_shares
policies.scope.exclude_volumes	string	query	False	Filter by policies.scope.exclude_volumes
policies.scope.include_shares	string	query	False	Filter by policies.scope.include_shares
policies.scope.exclude_extension	string	query	False	Filter by policies.scope.exclude_extension
policies.scope.include_extension	string	query	False	Filter by policies.scope.include_extension
policies.events.name	string	query	False	Filter by policies.events.name
svm.uuid	string	query	False	Filter by svm.uuid
svm.name	string	query	False	Filter by svm.name
fields	array[string]	query	False	Specify the fields to return.
max_records	integer	query	False	Limit the number of records returned.
return_records	boolean	query	False	<p>The default is true for GET calls. When set to false, only the number of records is returned.</p> <ul style="list-style-type: none"> <li>• Default value: 1</li> </ul>

Name	Type	In	Required	Description
return_timeout	integer	query	False	<p>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.</p> <ul style="list-style-type: none"> <li>• Max value: 120</li> <li>• Min value: 0</li> <li>• Default value: 1</li> </ul>
order_by	array[string]	query	False	Order results by specified fields and optional [asc

## Response

Status: 200, Ok

Name	Type	Description
_links	<a href="#">_links</a>	
num_records	integer	Number of records
records	array[ <a href="#">fpolicy</a> ]	

## Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "engines": {
      "certificate": {
        "ca": "TASample1",
        "name": "Sample1-FPolicy-Client",
        "serial_number": "8DDE112A114D1FBC"
      },
      "format": "xml",
      "keep_alive_interval": "PT2M",
      "max_server_requests": 500,
      "name": "fp_ex_eng",
      "port": 9876,
      "primary_servers": [
        "10.132.145.20",
        "10.140.101.109"
      ],
      "request_abort_timeout": "PT40S",
      "request_cancel_timeout": "PT20S",
      "resiliency": {
        "directory_path": "/dir1",
        "retention_duration": "PT3M"
      },
      "secondary_servers": [
        "10.132.145.20",
        "10.132.145.21"
      ],
      "server_progress_timeout": "PT1M",
      "ssl_option": "no_auth",
      "status_request_interval": "PT10S",
```

```

    "type": "synchronous"
  },
  "events": {
    "name": "event_nfs_close",
    "protocol": "cifs"
  },
  "policies": {
    "engine": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      }
    }
  },
  "events": [
    "event_nfs_close",
    "event_open"
  ],
  "name": "fp_policy_1",
  "privileged_user": "mydomain\\testuser",
  "scope": {
    "exclude_export_policies": {
    },
    "exclude_extension": {
    },
    "exclude_shares": {
    },
    "exclude_volumes": [
      "vol1",
      "vol_svm1",
      "*"
    ],
    "include_export_policies": {
    },
    "include_extension": {
    },
    "include_shares": [
      "sh1",
      "share_cifs"
    ],
    "include_volumes": [
      "vol1",
      "vol_svm1"
    ]
  }
},

```

```

    "svm": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    }
  }
}

```

## Error

Status: Default, Error

Name	Type	Description
error	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	<a href="#">href</a>	
self	<a href="#">href</a>	

\_links

Name	Type	Description
self	<a href="#">href</a>	

buffer\_size

Specifies the send and receive buffer size of the connected socket for the FPolicy server.

Name	Type	Description
recv_buffer	integer	Specifies the receive buffer size of the connected socket for the FPolicy server. Default value is 256KB.
send_buffer	integer	Specifies the send buffer size of the connected socket for the FPolicy server. Default value 1MB.

certificate

Provides details about certificate used to authenticate the Fpolicy server.

Name	Type	Description
ca	string	Specifies the certificate authority (CA) name of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.



Name	Type	Description
name	string	Specifies the certificate name as a fully qualified domain name (FQDN) or custom common name. The certificate is used if SSL authentication between the SVM and the FPolicy server is configured.
serial_number	string	Specifies the serial number of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.

#### resiliency

If all primary and secondary servers are down, or if no response is received from the FPolicy servers, file access events are stored inside the storage controller under the specified resiliency-directory-path.

Name	Type	Description
directory_path	string	Specifies the directory path under the SVM namespace, where notifications are stored in the files whenever a network outage happens.
enabled	boolean	Specifies whether the resiliency feature is enabled or not. Default is false.
retention_duration	string	Specifies the ISO-8601 duration, for which the notifications are written to files inside the storage controller during a network outage. The value for this field must be between 0 and 600 seconds. Default is 180 seconds.

#### fpolicy\_engines

Defines how ONTAP makes and manages connections to external FPolicy servers.

Name	Type	Description
buffer_size	<a href="#">buffer_size</a>	Specifies the send and receive buffer size of the connected socket for the FPolicy server.

Name	Type	Description
certificate	<a href="#">certificate</a>	Provides details about certificate used to authenticate the FPolicy server.
format	string	<p>The format for the notification messages sent to the FPolicy servers. The possible values are:</p> <ul style="list-style-type: none"> <li>• xml - Notifications sent to the FPolicy server will be formatted using the XML schema.</li> <li>• protobuf - Notifications sent to the FPolicy server will be formatted using Protobuf schema, which is a binary form.</li> </ul>
keep_alive_interval	string	Specifies the ISO-8601 interval time for a storage appliance to send Keep Alive message to an FPolicy server. The allowed range is between 10 to 600 seconds.
max_server_requests	integer	Specifies the maximum number of outstanding requests for the FPolicy server. It is used to specify maximum outstanding requests that will be queued up for the FPolicy server. The value for this field must be between 1 and 10000. The default values are 500, 1000 or 2000 for Low-end(<64 GB memory), Mid-end(>=64 GB memory) and High-end(>=128 GB memory) Platforms respectively.
name	string	Specifies the name to assign to the external server configuration.
port	integer	Port number of the FPolicy server application.
primary_servers	array[string]	

Name	Type	Description
request_abort_timeout	string	Specifies the ISO-8601 timeout duration for a screen request to be aborted by a storage appliance. The allowed range is between 0 to 200 seconds.
request_cancel_timeout	string	Specifies the ISO-8601 timeout duration for a screen request to be processed by an FPolicy server. The allowed range is between 0 to 100 seconds.
resiliency	<a href="#">resiliency</a>	If all primary and secondary servers are down, or if no response is received from the FPolicy servers, file access events are stored inside the storage controller under the specified resiliency-directory-path.
secondary_servers	array[string]	
server_progress_timeout	string	Specifies the ISO-8601 timeout duration in which a throttled FPolicy server must complete at least one screen request. If no request is processed within the timeout, connection to the FPolicy server is terminated. The allowed range is between 0 to 100 seconds.

Name	Type	Description
ssl_option	string	<p>Specifies the SSL option for external communication with the FPolicy server. Possible values include the following:</p> <ul style="list-style-type: none"> <li>• no_auth When set to "no_auth", no authentication takes place.</li> <li>• server_auth When set to "server_auth", only the FPolicy server is authenticated by the SVM. With this option, before creating the FPolicy external engine, the administrator must install the public certificate of the certificate authority (CA) that signed the FPolicy server certificate.</li> <li>• mutual_auth When set to "mutual_auth", mutual authentication takes place between the SVM and the FPolicy server. This means authentication of the FPolicy server by the SVM along with authentication of the SVM by the FPolicy server. With this option, before creating the FPolicy external engine, the administrator must install the public certificate of the certificate authority (CA) that signed the FPolicy server certificate along with the public certificate and key file for authentication of the SVM.</li> </ul>
status_request_interval	string	<p>Specifies the ISO-8601 interval time for a storage appliance to query a status request from an FPolicy server. The allowed range is between 0 to 50 seconds.</p>

Name	Type	Description
type	string	<p>The notification mode determines what ONTAP does after sending notifications to FPolicy servers. The possible values are:</p> <ul style="list-style-type: none"> <li>• synchronous - After sending a notification, wait for a response from the FPolicy server.</li> <li>• asynchronous - After sending a notification, file request processing continues. <ul style="list-style-type: none"> <li>◦ Default value: 1</li> <li>◦ enum: ["synchronous", "asynchronous"]</li> <li>◦ Introduced in: 9.10</li> <li>◦ x-nullable: true</li> </ul> </li> </ul>

#### file\_operations

Specifies the file operations for the FPolicy event. You must specify a valid protocol in the protocol parameter. The event will check the operations specified from all client requests using the protocol.

Name	Type	Description
access	boolean	Access operations
close	boolean	File close operations
create	boolean	File create operations
create_dir	boolean	Directory create operations
delete	boolean	File delete operations
delete_dir	boolean	Directory delete operations
getattr	boolean	Get attribute operations
link	boolean	Link operations
lookup	boolean	Lookup operations
open	boolean	File open operations

Name	Type	Description
read	boolean	File read operations
rename	boolean	File rename operations
rename_dir	boolean	Directory rename operations
setattr	boolean	Set attribute operations
symlink	boolean	Symbolic link operations
write	boolean	File write operations

## filters

Specifies the list of filters for a given file operation for the specified protocol. When you specify the filters, you must specify the valid protocols and a valid file operations.

Name	Type	Description
close_with_modification	boolean	Filter the client request for close with modification.
close_with_read	boolean	Filter the client request for close with read.
close_without_modification	boolean	Filter the client request for close without modification.
exclude_directory	boolean	Filter the client requests for directory operations. When this filter is specified directory operations are not monitored.
first_read	boolean	Filter the client requests for the first-read.
first_write	boolean	Filter the client requests for the first-write.
monitor_ads	boolean	Filter the client request for alternate data stream.
offline_bit	boolean	Filter the client request for offline bit set. FPolicy server receives notification only when offline files are accessed.

Name	Type	Description
open_with_delete_intent	boolean	Filter the client request for open with delete intent.
open_with_write_intent	boolean	Filter the client request for open with write intent.
setattr_with_access_time_change	boolean	Filter the client setattr requests for changing the access time of a file or directory.
setattr_with_allocation_size_change	boolean	Filter the client setattr requests for changing the allocation size of a file.
setattr_with_creation_time_change	boolean	Filter the client setattr requests for changing the creation time of a file or directory.
setattr_with_dacl_change	boolean	Filter the client setattr requests for changing dacl on a file or directory.
setattr_with_group_change	boolean	Filter the client setattr requests for changing group of a file or directory.
setattr_with_mode_change	boolean	Filter the client setattr requests for changing the mode bits on a file or directory.
setattr_with_modify_time_change	boolean	Filter the client setattr requests for changing the modification time of a file or directory.
setattr_with_owner_change	boolean	Filter the client setattr requests for changing owner of a file or directory.
setattr_with_sacl_change	boolean	Filter the client setattr requests for changing sacl on a file or directory.
setattr_with_size_change	boolean	Filter the client setattr requests for changing the size of a file.
write_with_size_change	boolean	Filter the client request for write with size change.

## fpolicy\_events

The information that a FPolicy process needs to determine what file access operations to monitor and for which of the monitored events notifications should be sent to the external FPolicy server.

Name	Type	Description
file_operations	<a href="#">file_operations</a>	Specifies the file operations for the FPolicy event. You must specify a valid protocol in the protocol parameter. The event will check the operations specified from all client requests using the protocol.
filters	<a href="#">filters</a>	Specifies the list of filters for a given file operation for the specified protocol. When you specify the filters, you must specify the valid protocols and a valid file operations.
monitor_fileop_failure	boolean	Specifies whether failed file operations monitoring is required.
name	string	Specifies the name of the FPolicy event.
protocol	string	Protocol for which event is created. If you specify protocol, then you must also specify a valid value for the file operation parameters. The value of this parameter must be one of the following: <ul style="list-style-type: none"><li>• cifs - for the CIFS protocol.</li><li>• nfsv3 - for the NFSv3 protocol.</li><li>• nfsv4 - for the NFSv4 protocol.</li></ul>
volume_monitoring	boolean	Specifies whether volume operation monitoring is required.

## fpolicy\_engine\_reference

FPolicy external engine



Name	Type	Description
_links	<a href="#">_links</a>	
name	string	The name of the FPolicy external engine.

fpolicy\_event\_reference

FPolicy events

Name	Type	Description
_links	<a href="#">_links</a>	
name	string	

scope

Name	Type	Description
check_extensions_on_directories	boolean	Specifies whether the file name extension checks also apply to directory objects. If this parameter is set to true, the directory objects are subjected to the same extension checks as regular files. If this parameter is set to false, the directory names are not matched for extensions and notifications are sent for directories even if their name extensions do not match. Default is false.
exclude_export_policies	array[string]	
exclude_extension	array[string]	
exclude_shares	array[string]	
exclude_volumes	array[string]	
include_export_policies	array[string]	
include_extension	array[string]	
include_shares	array[string]	
include_volumes	array[string]	

Name	Type	Description
object_monitoring_with_no_extension	boolean	Specifies whether the extension checks also apply to objects with no extension. If this parameter is set to true, all objects with or without extensions are monitored. Default is false.

#### fpolicy\_policies

Name	Type	Description
allow_privileged_access	boolean	Specifies whether privileged access is required for FPolicy servers. Privileged access is used when the FPolicy server requires direct access to the cluster nodes. When this parameter is set to true, FPolicy servers can access files on the cluster using a separate data channel with privileged access.
enabled	boolean	Specifies if the policy is enabled on the SVM or not. If no value is mentioned for this field but priority is set, then this policy will be enabled.
engine	<a href="#">fpolicy_engine_reference</a>	FPolicy external engine
events	array[ <a href="#">fpolicy_event_reference</a> ]	
mandatory	boolean	Specifies what action to take on a file access event in a case when all primary and secondary servers are down or no response is received from the FPolicy servers within a given timeout period. When this parameter is set to true, file access events will be denied under these circumstances.
name	string	Specifies the name of the policy.

Name	Type	Description
passthrough_read	boolean	Specifies whether passthrough-read should be allowed for FPolicy servers registered for the policy. Passthrough-read is a way to read data for offline files without restoring the files to primary storage. Offline files are files that have been moved to secondary storage.
priority	integer	Specifies the priority that is assigned to this policy.
privileged_user	string	Specifies the privileged user name for accessing files on the cluster using a separate data channel with privileged access. The input for this field should be in "domain\username" format.
scope	<a href="#">scope</a>	

#### svm

Name	Type	Description
_links	<a href="#">_links</a>	
name	string	The name of the SVM.
uuid	string	The unique identifier of the SVM.

#### fpolicy

FPolicy is an infrastructure component of ONTAP that enables partner applications connected to your storage systems to monitor and set file access permissions. Every time a client accesses a file from a storage system, based on the configuration of FPolicy, the partner application is notified about file access.

Name	Type	Description
_links	<a href="#">_links</a>	
engines	array[ <a href="#">fpolicy_engines</a> ]	
events	array[ <a href="#">fpolicy_events</a> ]	
policies	array[ <a href="#">fpolicy_policies</a> ]	
svm	<a href="#">svm</a>	

#### error\_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[ <a href="#">error_arguments</a> ]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

## Create an FPolicy configuration

POST /protocols/fpolicy

**Introduced In:** 9.6

Creates an FPolicy configuration.

### Required properties

- `svm.uuid` or `svm.name` - Existing SVM in which to create the FPolicy configuration.

### Recommended optional properties

- `engines` - External server to which the notifications will be sent.
- `events` - File operations to monitor.
- `policies` - Policy configuration which acts as a container for FPolicy event and FPolicy engine.
- `scope` - Scope of the policy. Can be limited to exports, volumes, shares or file extensions.

### Default property values

If not specified in POST, the following default property values are assigned:

- `engines.type` - *synchronous*
- `policies.engine` - *native*
- `policies.mandatory` - *true*

- `events.volume_monitoring` - *false*
- `events.file_operations.*` - *false*
- `events.filters.*` - *false*
- `events.monitor_fileop_failure.*` - *false*

## Related ONTAP commands

- `fpolicy policy event create`
- `fpolicy policy external-engine create`
- `fpolicy policy create`
- `fpolicy policy scope create`
- `fpolicy enable`

## Learn more

- [DOC /protocols/fpolicy](#)

## Parameters

Name	Type	In	Required	Description
return_records	boolean	query	False	<p>The default is false. If set to true, the records are returned.</p> <ul style="list-style-type: none"> <li>• Default value:</li> </ul>

## Request Body

Name	Type	Description
_links	<a href="#">_links</a>	
engines	array[ <a href="#">fpolicy_engines</a> ]	
events	array[ <a href="#">fpolicy_events</a> ]	
policies	array[ <a href="#">fpolicy_policies</a> ]	
svm	<a href="#">svm</a>	

## Example request

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "engines": {
    "certificate": {
      "ca": "TASample1",
      "name": "Sample1-FPolicy-Client",
      "serial_number": "8DDE112A114D1FBC"
    },
    "format": "xml",
    "keep_alive_interval": "PT2M",
    "max_server_requests": 500,
    "name": "fp_ex_eng",
    "port": 9876,
    "primary_servers": [
      "10.132.145.20",
      "10.140.101.109"
    ],
    "request_abort_timeout": "PT40S",
    "request_cancel_timeout": "PT20S",
    "resiliency": {
      "directory_path": "/dir1",
      "retention_duration": "PT3M"
    },
    "secondary_servers": [
      "10.132.145.20",
      "10.132.145.21"
    ],
    "server_progress_timeout": "PT1M",
    "ssl_option": "no_auth",
    "status_request_interval": "PT10S",
    "type": "synchronous"
  },
  "events": {
    "name": "event_nfs_close",
    "protocol": "cifs"
  },
  "policies": {
    "engine": {
      "_links": {
        "self": {
```

```

        "href": "/api/resourcelink"
    }
}
},
"events": [
    "event_nfs_close",
    "event_open"
],
"name": "fp_policy_1",
"privileged_user": "mydomain\\testuser",
"scope": {
    "exclude_export_policies": {
    },
    "exclude_extension": {
    },
    "exclude_shares": {
    },
    "exclude_volumes": [
        "vol1",
        "vol_svm1",
        "*"
    ],
    "include_export_policies": {
    },
    "include_extension": {
    },
    "include_shares": [
        "sh1",
        "share_cifs"
    ],
    "include_volumes": [
        "vol1",
        "vol_svm1"
    ]
}
},
"svm": {
    "_links": {
        "self": {
            "href": "/api/resourcelink"
        }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
}
}

```

## Response

Status: 201, Created

Name	Type	Description
_links	<a href="#">_links</a>	
num_records	integer	Number of records
records	array[ <a href="#">fpolicy</a> ]	



## Example response

```
{
  "_links": {
    "next": {
      "href": "/api/resourcelink"
    },
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "num_records": 1,
  "records": {
    "_links": {
      "self": {
        "href": "/api/resourcelink"
      }
    },
    "engines": {
      "certificate": {
        "ca": "TASample1",
        "name": "Sample1-FPolicy-Client",
        "serial_number": "8DDE112A114D1FBC"
      },
      "format": "xml",
      "keep_alive_interval": "PT2M",
      "max_server_requests": 500,
      "name": "fp_ex_eng",
      "port": 9876,
      "primary_servers": [
        "10.132.145.20",
        "10.140.101.109"
      ],
      "request_abort_timeout": "PT40S",
      "request_cancel_timeout": "PT20S",
      "resiliency": {
        "directory_path": "/dir1",
        "retention_duration": "PT3M"
      },
      "secondary_servers": [
        "10.132.145.20",
        "10.132.145.21"
      ],
      "server_progress_timeout": "PT1M",
      "ssl_option": "no_auth",
      "status_request_interval": "PT10S",
```

```

    "type": "synchronous"
  },
  "events": {
    "name": "event_nfs_close",
    "protocol": "cifs"
  },
  "policies": {
    "engine": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      }
    }
  },
  "events": [
    "event_nfs_close",
    "event_open"
  ],
  "name": "fp_policy_1",
  "privileged_user": "mydomain\\testuser",
  "scope": {
    "exclude_export_policies": {
    },
    "exclude_extension": {
    },
    "exclude_shares": {
    },
    "exclude_volumes": [
      "vol1",
      "vol_svm1",
      "*"
    ],
    "include_export_policies": {
    },
    "include_extension": {
    },
    "include_shares": [
      "sh1",
      "share_cifs"
    ],
    "include_volumes": [
      "vol1",
      "vol_svm1"
    ]
  }
},

```

```

    "svm": {
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "svm1",
      "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
    }
  }
}

```

## Headers

Name	Description	Type
Location	Useful for tracking the resource location	string

## Error

Status: Default

## ONTAP Error Response Codes

Error Code	Description
9765032	The FPolicy engine, FPolicy event or FPolicy policy specified already exists
9765031	If any of the FPolicy engine, FPolicy event, or FPolicy policy creation fails due to a systematic error or hardware failure, the cause of the failure is detailed in the error message
2621706	The SVM UUID specified belongs to different SVM
2621462	The SVM name specified does not exist

Name	Type	Description
error	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	<a href="#">href</a>	

buffer\_size

Specifies the send and receive buffer size of the connected socket for the FPolicy server.

Name	Type	Description
recv_buffer	integer	Specifies the receive buffer size of the connected socket for the FPolicy server. Default value is 256KB.
send_buffer	integer	Specifies the send buffer size of the connected socket for the FPolicy server. Default value 1MB.

certificate

Provides details about certificate used to authenticate the Fpolicy server.

Name	Type	Description
ca	string	Specifies the certificate authority (CA) name of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.
name	string	Specifies the certificate name as a fully qualified domain name (FQDN) or custom common name. The certificate is used if SSL authentication between the SVM and the FPolicy server is configured.

Name	Type	Description
serial_number	string	Specifies the serial number of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.

#### resiliency

If all primary and secondary servers are down, or if no response is received from the FPolicy servers, file access events are stored inside the storage controller under the specified resiliency-directory-path.

Name	Type	Description
directory_path	string	Specifies the directory path under the SVM namespace, where notifications are stored in the files whenever a network outage happens.
enabled	boolean	Specifies whether the resiliency feature is enabled or not. Default is false.
retention_duration	string	Specifies the ISO-8601 duration, for which the notifications are written to files inside the storage controller during a network outage. The value for this field must be between 0 and 600 seconds. Default is 180 seconds.

#### fpolicy\_engines

Defines how ONTAP makes and manages connections to external FPolicy servers.

Name	Type	Description
buffer_size	<a href="#">buffer_size</a>	Specifies the send and receive buffer size of the connected socket for the FPolicy server.
certificate	<a href="#">certificate</a>	Provides details about certificate used to authenticate the Fpolicy server.

Name	Type	Description
format	string	<p>The format for the notification messages sent to the FPolicy servers. The possible values are:</p> <ul style="list-style-type: none"> <li>• xml - Notifications sent to the FPolicy server will be formatted using the XML schema.</li> <li>• protobuf - Notifications sent to the FPolicy server will be formatted using Protobuf schema, which is a binary form.</li> </ul>
keep_alive_interval	string	Specifies the ISO-8601 interval time for a storage appliance to send Keep Alive message to an FPolicy server. The allowed range is between 10 to 600 seconds.
max_server_requests	integer	Specifies the maximum number of outstanding requests for the FPolicy server. It is used to specify maximum outstanding requests that will be queued up for the FPolicy server. The value for this field must be between 1 and 10000. The default values are 500, 1000 or 2000 for Low-end(<64 GB memory), Mid-end(>=64 GB memory) and High-end(>=128 GB memory) Platforms respectively.
name	string	Specifies the name to assign to the external server configuration.
port	integer	Port number of the FPolicy server application.
primary_servers	array[string]	
request_abort_timeout	string	Specifies the ISO-8601 timeout duration for a screen request to be aborted by a storage appliance. The allowed range is between 0 to 200 seconds.

Name	Type	Description
request_cancel_timeout	string	Specifies the ISO-8601 timeout duration for a screen request to be processed by an FPolicy server. The allowed range is between 0 to 100 seconds.
resiliency	<a href="#">resiliency</a>	If all primary and secondary servers are down, or if no response is received from the FPolicy servers, file access events are stored inside the storage controller under the specified resiliency-directory-path.
secondary_servers	array[string]	
server_progress_timeout	string	Specifies the ISO-8601 timeout duration in which a throttled FPolicy server must complete at least one screen request. If no request is processed within the timeout, connection to the FPolicy server is terminated. The allowed range is between 0 to 100 seconds.



Name	Type	Description
ssl_option	string	<p>Specifies the SSL option for external communication with the FPolicy server. Possible values include the following:</p> <ul style="list-style-type: none"> <li>• no_auth When set to "no_auth", no authentication takes place.</li> <li>• server_auth When set to "server_auth", only the FPolicy server is authenticated by the SVM. With this option, before creating the FPolicy external engine, the administrator must install the public certificate of the certificate authority (CA) that signed the FPolicy server certificate.</li> <li>• mutual_auth When set to "mutual_auth", mutual authentication takes place between the SVM and the FPolicy server. This means authentication of the FPolicy server by the SVM along with authentication of the SVM by the FPolicy server. With this option, before creating the FPolicy external engine, the administrator must install the public certificate of the certificate authority (CA) that signed the FPolicy server certificate along with the public certificate and key file for authentication of the SVM.</li> </ul>
status_request_interval	string	<p>Specifies the ISO-8601 interval time for a storage appliance to query a status request from an FPolicy server. The allowed range is between 0 to 50 seconds.</p>

Name	Type	Description
type	string	<p>The notification mode determines what ONTAP does after sending notifications to FPolicy servers. The possible values are:</p> <ul style="list-style-type: none"> <li>• synchronous - After sending a notification, wait for a response from the FPolicy server.</li> <li>• asynchronous - After sending a notification, file request processing continues. <ul style="list-style-type: none"> <li>◦ Default value: 1</li> <li>◦ enum: ["synchronous", "asynchronous"]</li> <li>◦ Introduced in: 9.10</li> <li>◦ x-nullable: true</li> </ul> </li> </ul>

#### file\_operations

Specifies the file operations for the FPolicy event. You must specify a valid protocol in the protocol parameter. The event will check the operations specified from all client requests using the protocol.

Name	Type	Description
access	boolean	Access operations
close	boolean	File close operations
create	boolean	File create operations
create_dir	boolean	Directory create operations
delete	boolean	File delete operations
delete_dir	boolean	Directory delete operations
getattr	boolean	Get attribute operations
link	boolean	Link operations
lookup	boolean	Lookup operations
open	boolean	File open operations

Name	Type	Description
read	boolean	File read operations
rename	boolean	File rename operations
rename_dir	boolean	Directory rename operations
setattr	boolean	Set attribute operations
symlink	boolean	Symbolic link operations
write	boolean	File write operations

## filters

Specifies the list of filters for a given file operation for the specified protocol. When you specify the filters, you must specify the valid protocols and a valid file operations.

Name	Type	Description
close_with_modification	boolean	Filter the client request for close with modification.
close_with_read	boolean	Filter the client request for close with read.
close_without_modification	boolean	Filter the client request for close without modification.
exclude_directory	boolean	Filter the client requests for directory operations. When this filter is specified directory operations are not monitored.
first_read	boolean	Filter the client requests for the first-read.
first_write	boolean	Filter the client requests for the first-write.
monitor_ads	boolean	Filter the client request for alternate data stream.
offline_bit	boolean	Filter the client request for offline bit set. FPolicy server receives notification only when offline files are accessed.

Name	Type	Description
open_with_delete_intent	boolean	Filter the client request for open with delete intent.
open_with_write_intent	boolean	Filter the client request for open with write intent.
setattr_with_access_time_change	boolean	Filter the client setattr requests for changing the access time of a file or directory.
setattr_with_allocation_size_change	boolean	Filter the client setattr requests for changing the allocation size of a file.
setattr_with_creation_time_change	boolean	Filter the client setattr requests for changing the creation time of a file or directory.
setattr_with_dacl_change	boolean	Filter the client setattr requests for changing dacl on a file or directory.
setattr_with_group_change	boolean	Filter the client setattr requests for changing group of a file or directory.
setattr_with_mode_change	boolean	Filter the client setattr requests for changing the mode bits on a file or directory.
setattr_with_modify_time_change	boolean	Filter the client setattr requests for changing the modification time of a file or directory.
setattr_with_owner_change	boolean	Filter the client setattr requests for changing owner of a file or directory.
setattr_with_sacl_change	boolean	Filter the client setattr requests for changing sacl on a file or directory.
setattr_with_size_change	boolean	Filter the client setattr requests for changing the size of a file.
write_with_size_change	boolean	Filter the client request for write with size change.

## fpolicy\_events

The information that a FPolicy process needs to determine what file access operations to monitor and for which of the monitored events notifications should be sent to the external FPolicy server.

Name	Type	Description
file_operations	<a href="#">file_operations</a>	Specifies the file operations for the FPolicy event. You must specify a valid protocol in the protocol parameter. The event will check the operations specified from all client requests using the protocol.
filters	<a href="#">filters</a>	Specifies the list of filters for a given file operation for the specified protocol. When you specify the filters, you must specify the valid protocols and a valid file operations.
monitor_fileop_failure	boolean	Specifies whether failed file operations monitoring is required.
name	string	Specifies the name of the FPolicy event.
protocol	string	Protocol for which event is created. If you specify protocol, then you must also specify a valid value for the file operation parameters. The value of this parameter must be one of the following: <ul style="list-style-type: none"><li>• cifs - for the CIFS protocol.</li><li>• nfsv3 - for the NFSv3 protocol.</li><li>• nfsv4 - for the NFSv4 protocol.</li></ul>
volume_monitoring	boolean	Specifies whether volume operation monitoring is required.

## fpolicy\_engine\_reference

FPolicy external engine

Name	Type	Description
_links	<a href="#">_links</a>	
name	string	The name of the FPolicy external engine.

fpolicy\_event\_reference

FPolicy events

Name	Type	Description
_links	<a href="#">_links</a>	
name	string	

scope

Name	Type	Description
check_extensions_on_directories	boolean	Specifies whether the file name extension checks also apply to directory objects. If this parameter is set to true, the directory objects are subjected to the same extension checks as regular files. If this parameter is set to false, the directory names are not matched for extensions and notifications are sent for directories even if their name extensions do not match. Default is false.
exclude_export_policies	array[string]	
exclude_extension	array[string]	
exclude_shares	array[string]	
exclude_volumes	array[string]	
include_export_policies	array[string]	
include_extension	array[string]	
include_shares	array[string]	
include_volumes	array[string]	

Name	Type	Description
object_monitoring_with_no_extension	boolean	Specifies whether the extension checks also apply to objects with no extension. If this parameter is set to true, all objects with or without extensions are monitored. Default is false.

#### fpolicy\_policies

Name	Type	Description
allow_privileged_access	boolean	Specifies whether privileged access is required for FPolicy servers. Privileged access is used when the FPolicy server requires direct access to the cluster nodes. When this parameter is set to true, FPolicy servers can access files on the cluster using a separate data channel with privileged access.
enabled	boolean	Specifies if the policy is enabled on the SVM or not. If no value is mentioned for this field but priority is set, then this policy will be enabled.
engine	<a href="#">fpolicy_engine_reference</a>	FPolicy external engine
events	array[ <a href="#">fpolicy_event_reference</a> ]	
mandatory	boolean	Specifies what action to take on a file access event in a case when all primary and secondary servers are down or no response is received from the FPolicy servers within a given timeout period. When this parameter is set to true, file access events will be denied under these circumstances.
name	string	Specifies the name of the policy.

Name	Type	Description
passthrough_read	boolean	Specifies whether passthrough-read should be allowed for FPolicy servers registered for the policy. Passthrough-read is a way to read data for offline files without restoring the files to primary storage. Offline files are files that have been moved to secondary storage.
priority	integer	Specifies the priority that is assigned to this policy.
privileged_user	string	Specifies the privileged user name for accessing files on the cluster using a separate data channel with privileged access. The input for this field should be in "domain\username" format.
scope	<a href="#">scope</a>	

#### svm

Name	Type	Description
_links	<a href="#">_links</a>	
name	string	The name of the SVM.
uuid	string	The unique identifier of the SVM.

#### fpolicy

FPolicy is an infrastructure component of ONTAP that enables partner applications connected to your storage systems to monitor and set file access permissions. Every time a client accesses a file from a storage system, based on the configuration of FPolicy, the partner application is notified about file access.

Name	Type	Description
_links	<a href="#">_links</a>	
engines	array[ <a href="#">fpolicy_engines</a> ]	
events	array[ <a href="#">fpolicy_events</a> ]	
policies	array[ <a href="#">fpolicy_policies</a> ]	
svm	<a href="#">svm</a>	

[\\_links](#)



Name	Type	Description
next	<a href="#">href</a>	
self	<a href="#">href</a>	

error\_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

error

Name	Type	Description
arguments	array[ <a href="#">error_arguments</a> ]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

## Delete the FPolicy configuration for an SVM

```
DELETE /protocols/fpolicy/{svm.uuid}
```

**Introduced In:** 9.6

Deletes the FPolicy configuration for the specified SVM. Before deleting the FPolicy configuration, ensure that all policies belonging to the SVM are disabled.

### Related ONTAP commands

- `fpolicy delete`
- `fpolicy policy scope delete`
- `fpolicy policy delete`
- `fpolicy policy event delete`
- `fpolicy policy external-engine delete`

## Learn more

- [DOC /protocols/fpolicy](#)

## Parameters

Name	Type	In	Required	Description
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.

## Response

Status: 200, Ok

## Error

Status: Default

### ONTAP Error Response Codes

Error Code	Description
9765030	Cannot delete an FPolicy configuration if any of the policy is enabled
9765031	If any of the FPolicy engine, FPolicy event or FPolicy policy deletion fails due to a systemic error or hardware failure, the cause of the failure is detailed in the error message.

Name	Type	Description
error	<a href="#">error</a>	

## 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

#### error

Name	Type	Description
arguments	array[ <a href="#">error_arguments</a> ]	Message arguments
code	string	Error code
message	string	Error message
target	string	The target parameter that caused the error.

## Retrieve the FPolicy configuration for an SVM

GET /protocols/fpolicy/{svm.uuid}

Introduced In: 9.6

Retrieves an FPolicy configuration of an SVM.

## Related ONTAP commands

- `fpolicy show`
- `fpolicy policy show`
- `fpolicy policy scope show`
- `fpolicy policy event show`
- `fpolicy policy external-engine show`

## Learn more

- [DOC /protocols/fpolicy](#)

## Parameters

Name	Type	In	Required	Description
svm.uuid	string	path	True	UUID of the SVM to which this object belongs.
fields	array[string]	query	False	Specify the fields to return.

## Response

Status: 200, Ok

Name	Type	Description
_links	<a href="#">_links</a>	
engines	array[ <a href="#">fpolicy_engines</a> ]	
events	array[ <a href="#">fpolicy_events</a> ]	
policies	array[ <a href="#">fpolicy_policies</a> ]	
svm	<a href="#">svm</a>	

## Example response

```
{
  "_links": {
    "self": {
      "href": "/api/resourcelink"
    }
  },
  "engines": {
    "certificate": {
      "ca": "TASample1",
      "name": "Sample1-FPolicy-Client",
      "serial_number": "8DDE112A114D1FBC"
    },
    "format": "xml",
    "keep_alive_interval": "PT2M",
    "max_server_requests": 500,
    "name": "fp_ex_eng",
    "port": 9876,
    "primary_servers": [
      "10.132.145.20",
      "10.140.101.109"
    ],
    "request_abort_timeout": "PT40S",
    "request_cancel_timeout": "PT20S",
    "resiliency": {
      "directory_path": "/dir1",
      "retention_duration": "PT3M"
    },
    "secondary_servers": [
      "10.132.145.20",
      "10.132.145.21"
    ],
    "server_progress_timeout": "PT1M",
    "ssl_option": "no_auth",
    "status_request_interval": "PT10S",
    "type": "synchronous"
  },
  "events": {
    "name": "event_nfs_close",
    "protocol": "cifs"
  },
  "policies": {
    "engine": {
      "_links": {
        "self": {
```

```

        "href": "/api/resourcelink"
    }
}
},
"events": [
    "event_nfs_close",
    "event_open"
],
"name": "fp_policy_1",
"privileged_user": "mydomain\\testuser",
"scope": {
    "exclude_export_policies": {
    },
    "exclude_extension": {
    },
    "exclude_shares": {
    },
    "exclude_volumes": [
        "vol1",
        "vol_svm1",
        "*"
    ],
    "include_export_policies": {
    },
    "include_extension": {
    },
    "include_shares": [
        "sh1",
        "share_cifs"
    ],
    "include_volumes": [
        "vol1",
        "vol_svm1"
    ]
}
},
"svm": {
    "_links": {
        "self": {
            "href": "/api/resourcelink"
        }
    },
    "name": "svm1",
    "uuid": "02c9e252-41be-11e9-81d5-00a0986138f7"
}
}

```

## Error

Status: Default, Error

Name	Type	Description
error	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	<a href="#">href</a>	

buffer\_size

Specifies the send and receive buffer size of the connected socket for the FPolicy server.

Name	Type	Description
recv_buffer	integer	Specifies the receive buffer size of the connected socket for the FPolicy server. Default value is 256KB.
send_buffer	integer	Specifies the send buffer size of the connected socket for the FPolicy server. Default value 1MB.

certificate

Provides details about certificate used to authenticate the Fpolicy server.

Name	Type	Description
ca	string	Specifies the certificate authority (CA) name of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.
name	string	Specifies the certificate name as a fully qualified domain name (FQDN) or custom common name. The certificate is used if SSL authentication between the SVM and the FPolicy server is configured.



Name	Type	Description
serial_number	string	Specifies the serial number of the certificate used for authentication if SSL authentication between the SVM and the FPolicy server is configured.

#### resiliency

If all primary and secondary servers are down, or if no response is received from the FPolicy servers, file access events are stored inside the storage controller under the specified resiliency-directory-path.

Name	Type	Description
directory_path	string	Specifies the directory path under the SVM namespace, where notifications are stored in the files whenever a network outage happens.
enabled	boolean	Specifies whether the resiliency feature is enabled or not. Default is false.
retention_duration	string	Specifies the ISO-8601 duration, for which the notifications are written to files inside the storage controller during a network outage. The value for this field must be between 0 and 600 seconds. Default is 180 seconds.

#### fpolicy\_engines

Defines how ONTAP makes and manages connections to external FPolicy servers.

Name	Type	Description
buffer_size	<a href="#">buffer_size</a>	Specifies the send and receive buffer size of the connected socket for the FPolicy server.
certificate	<a href="#">certificate</a>	Provides details about certificate used to authenticate the Fpolicy server.

Name	Type	Description
format	string	<p>The format for the notification messages sent to the FPolicy servers. The possible values are:</p> <ul style="list-style-type: none"> <li>• xml - Notifications sent to the FPolicy server will be formatted using the XML schema.</li> <li>• protobuf - Notifications sent to the FPolicy server will be formatted using Protobuf schema, which is a binary form.</li> </ul>
keep_alive_interval	string	Specifies the ISO-8601 interval time for a storage appliance to send Keep Alive message to an FPolicy server. The allowed range is between 10 to 600 seconds.
max_server_requests	integer	Specifies the maximum number of outstanding requests for the FPolicy server. It is used to specify maximum outstanding requests that will be queued up for the FPolicy server. The value for this field must be between 1 and 10000. The default values are 500, 1000 or 2000 for Low-end(<64 GB memory), Mid-end(>=64 GB memory) and High-end(>=128 GB memory) Platforms respectively.
name	string	Specifies the name to assign to the external server configuration.
port	integer	Port number of the FPolicy server application.
primary_servers	array[string]	
request_abort_timeout	string	Specifies the ISO-8601 timeout duration for a screen request to be aborted by a storage appliance. The allowed range is between 0 to 200 seconds.

Name	Type	Description
request_cancel_timeout	string	Specifies the ISO-8601 timeout duration for a screen request to be processed by an FPolicy server. The allowed range is between 0 to 100 seconds.
resiliency	<a href="#">resiliency</a>	If all primary and secondary servers are down, or if no response is received from the FPolicy servers, file access events are stored inside the storage controller under the specified resiliency-directory-path.
secondary_servers	array[string]	
server_progress_timeout	string	Specifies the ISO-8601 timeout duration in which a throttled FPolicy server must complete at least one screen request. If no request is processed within the timeout, connection to the FPolicy server is terminated. The allowed range is between 0 to 100 seconds.

Name	Type	Description
ssl_option	string	<p>Specifies the SSL option for external communication with the FPolicy server. Possible values include the following:</p> <ul style="list-style-type: none"> <li>• no_auth When set to "no_auth", no authentication takes place.</li> <li>• server_auth When set to "server_auth", only the FPolicy server is authenticated by the SVM. With this option, before creating the FPolicy external engine, the administrator must install the public certificate of the certificate authority (CA) that signed the FPolicy server certificate.</li> <li>• mutual_auth When set to "mutual_auth", mutual authentication takes place between the SVM and the FPolicy server. This means authentication of the FPolicy server by the SVM along with authentication of the SVM by the FPolicy server. With this option, before creating the FPolicy external engine, the administrator must install the public certificate of the certificate authority (CA) that signed the FPolicy server certificate along with the public certificate and key file for authentication of the SVM.</li> </ul>
status_request_interval	string	<p>Specifies the ISO-8601 interval time for a storage appliance to query a status request from an FPolicy server. The allowed range is between 0 to 50 seconds.</p>

Name	Type	Description
type	string	<p>The notification mode determines what ONTAP does after sending notifications to FPolicy servers. The possible values are:</p> <ul style="list-style-type: none"> <li>• synchronous - After sending a notification, wait for a response from the FPolicy server.</li> <li>• asynchronous - After sending a notification, file request processing continues. <ul style="list-style-type: none"> <li>◦ Default value: 1</li> <li>◦ enum: ["synchronous", "asynchronous"]</li> <li>◦ Introduced in: 9.10</li> <li>◦ x-nullable: true</li> </ul> </li> </ul>

#### file\_operations

Specifies the file operations for the FPolicy event. You must specify a valid protocol in the protocol parameter. The event will check the operations specified from all client requests using the protocol.

Name	Type	Description
access	boolean	Access operations
close	boolean	File close operations
create	boolean	File create operations
create_dir	boolean	Directory create operations
delete	boolean	File delete operations
delete_dir	boolean	Directory delete operations
getattr	boolean	Get attribute operations
link	boolean	Link operations
lookup	boolean	Lookup operations
open	boolean	File open operations

Name	Type	Description
read	boolean	File read operations
rename	boolean	File rename operations
rename_dir	boolean	Directory rename operations
setattr	boolean	Set attribute operations
symlink	boolean	Symbolic link operations
write	boolean	File write operations

## filters

Specifies the list of filters for a given file operation for the specified protocol. When you specify the filters, you must specify the valid protocols and a valid file operations.

Name	Type	Description
close_with_modification	boolean	Filter the client request for close with modification.
close_with_read	boolean	Filter the client request for close with read.
close_without_modification	boolean	Filter the client request for close without modification.
exclude_directory	boolean	Filter the client requests for directory operations. When this filter is specified directory operations are not monitored.
first_read	boolean	Filter the client requests for the first-read.
first_write	boolean	Filter the client requests for the first-write.
monitor_ads	boolean	Filter the client request for alternate data stream.
offline_bit	boolean	Filter the client request for offline bit set. FPolicy server receives notification only when offline files are accessed.

Name	Type	Description
open_with_delete_intent	boolean	Filter the client request for open with delete intent.
open_with_write_intent	boolean	Filter the client request for open with write intent.
setattr_with_access_time_change	boolean	Filter the client setattr requests for changing the access time of a file or directory.
setattr_with_allocation_size_change	boolean	Filter the client setattr requests for changing the allocation size of a file.
setattr_with_creation_time_change	boolean	Filter the client setattr requests for changing the creation time of a file or directory.
setattr_with_dacl_change	boolean	Filter the client setattr requests for changing dacl on a file or directory.
setattr_with_group_change	boolean	Filter the client setattr requests for changing group of a file or directory.
setattr_with_mode_change	boolean	Filter the client setattr requests for changing the mode bits on a file or directory.
setattr_with_modify_time_change	boolean	Filter the client setattr requests for changing the modification time of a file or directory.
setattr_with_owner_change	boolean	Filter the client setattr requests for changing owner of a file or directory.
setattr_with_sacl_change	boolean	Filter the client setattr requests for changing sacl on a file or directory.
setattr_with_size_change	boolean	Filter the client setattr requests for changing the size of a file.
write_with_size_change	boolean	Filter the client request for write with size change.

## fpolicy\_events

The information that a FPolicy process needs to determine what file access operations to monitor and for which of the monitored events notifications should be sent to the external FPolicy server.

Name	Type	Description
file_operations	<a href="#">file_operations</a>	Specifies the file operations for the FPolicy event. You must specify a valid protocol in the protocol parameter. The event will check the operations specified from all client requests using the protocol.
filters	<a href="#">filters</a>	Specifies the list of filters for a given file operation for the specified protocol. When you specify the filters, you must specify the valid protocols and a valid file operations.
monitor_fileop_failure	boolean	Specifies whether failed file operations monitoring is required.
name	string	Specifies the name of the FPolicy event.
protocol	string	Protocol for which event is created. If you specify protocol, then you must also specify a valid value for the file operation parameters. The value of this parameter must be one of the following: <ul style="list-style-type: none"><li>• cifs - for the CIFS protocol.</li><li>• nfsv3 - for the NFSv3 protocol.</li><li>• nfsv4 - for the NFSv4 protocol.</li></ul>
volume_monitoring	boolean	Specifies whether volume operation monitoring is required.

## fpolicy\_engine\_reference

FPolicy external engine



Name	Type	Description
_links	<a href="#">_links</a>	
name	string	The name of the FPolicy external engine.

fpolicy\_event\_reference

FPolicy events

Name	Type	Description
_links	<a href="#">_links</a>	
name	string	

scope

Name	Type	Description
check_extensions_on_directories	boolean	Specifies whether the file name extension checks also apply to directory objects. If this parameter is set to true, the directory objects are subjected to the same extension checks as regular files. If this parameter is set to false, the directory names are not matched for extensions and notifications are sent for directories even if their name extensions do not match. Default is false.
exclude_export_policies	array[string]	
exclude_extension	array[string]	
exclude_shares	array[string]	
exclude_volumes	array[string]	
include_export_policies	array[string]	
include_extension	array[string]	
include_shares	array[string]	
include_volumes	array[string]	

Name	Type	Description
object_monitoring_with_no_extension	boolean	Specifies whether the extension checks also apply to objects with no extension. If this parameter is set to true, all objects with or without extensions are monitored. Default is false.

#### fpolicy\_policies

Name	Type	Description
allow_privileged_access	boolean	Specifies whether privileged access is required for FPolicy servers. Privileged access is used when the FPolicy server requires direct access to the cluster nodes. When this parameter is set to true, FPolicy servers can access files on the cluster using a separate data channel with privileged access.
enabled	boolean	Specifies if the policy is enabled on the SVM or not. If no value is mentioned for this field but priority is set, then this policy will be enabled.
engine	<a href="#">fpolicy_engine_reference</a>	FPolicy external engine
events	array[ <a href="#">fpolicy_event_reference</a> ]	
mandatory	boolean	Specifies what action to take on a file access event in a case when all primary and secondary servers are down or no response is received from the FPolicy servers within a given timeout period. When this parameter is set to true, file access events will be denied under these circumstances.
name	string	Specifies the name of the policy.

Name	Type	Description
passthrough_read	boolean	Specifies whether passthrough-read should be allowed for FPolicy servers registered for the policy. Passthrough-read is a way to read data for offline files without restoring the files to primary storage. Offline files are files that have been moved to secondary storage.
priority	integer	Specifies the priority that is assigned to this policy.
privileged_user	string	Specifies the privileged user name for accessing files on the cluster using a separate data channel with privileged access. The input for this field should be in "domain\username" format.
scope	<a href="#">scope</a>	

#### svm

Name	Type	Description
_links	<a href="#">_links</a>	
name	string	The name of the SVM.
uuid	string	The unique identifier of the SVM.

#### error\_arguments

Name	Type	Description
code	string	Argument code
message	string	Message argument

#### error

Name	Type	Description
arguments	array[ <a href="#">error_arguments</a> ]	Message arguments
code	string	Error code

Name	Type	Description
message	string	Error message
target	string	The target parameter that caused the error.

## Copyright information

Copyright © 2024 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.