Getting Started with the FXOS REST API

You can access the FXOS REST API using any REST API client. Typically REST API clients are available as browser plug-ins, but any REST API client is allowed.

Base URL

All users must access the FXOS API using HTTPS via the device's configured port. In general, the base URL for all API requests will be as follows:

```
https://<Firepower_Chassis_fqdn>[:management_port]/api/
```

Cisco recommends that the Firepower chassis fully qualified domain name (`chassis_fqdn`) be used instead of the IP address in order for the REST client to be able to authenticate the device being managed; however, the IP address can be used. The Firepower chassis will authenticate the REST client using the provided credentials. See Client Authentication for additional details.

Client Authentication

The FXOS REST API uses a session-based method of authentication, requiring an HTTP `TOKEN` header in order to authenticate each request from an API client.

All API requests except `/api/login` must include this HTTP `TOKEN` header, with the `TOKEN` value being the actual token obtained in the `/api/login` response. If the `TOKEN` is not specified in the header, an Authentication Required error code will be returned by the REST API.

To obtain an authentication token, an API client must execute a `POST /api/login` call with the following HTTP headers: `username: <name_of_user> password: <user_password>`.

Note These user credentials must already exist on the chassis, or an Authentication Failed error will be returned. Also, authentication will fail if the user password is URL-encoded.

A successful /api/login call will return an HTTP 200 code with this payload:

```
{
  "refreshPeriod": "string",
  "token": "string"
}
```

For example:

```
{
  "refreshPeriod": "0",
  "token": "a205739a4d56359730c08ee7bda559cd6e4dd36ad65bb10a17f71d4cea356028"
}
```

You must extract this token and include it in the HTTP header when submitting all other API method requests, and the header field name for the token must be TOKEN.

On authentication failure, the API will return an HTTP 400 code with this payload: { "error-code": "551", "error-description": "Authentication failed", "error-nr": "unidentified-fail" }

On authorization failure, the API will return an HTTP 400 code with the following payload when the token is invalid: { "error-code": "552", "error-description": "Authorization required", "error-nr": "service-unavailable" }

To log out, the client must submit a POST /api/logout request with this HTTP header: "TOKEN"= "<authentication_token>"

An HTTP 200 code is returned when a session was found and that session was terminated.

An HTTP 555 code is returned with the following payload when a valid session is not found for the specified token: { "error-code": "555", "error-description": "Authorization required", "error-nr": "service-unavailable" }

Supported HTTP Methods

You can use the following HTTP methods:

- **GET** – Retrieves the specified object. The query is submitted in the URL and the output is contained in the response body.
- **POST** – Creates an object. The path is submitted in the URL and the output is contained in the response body.
- **PUT** – Updates an object completely. Read-only properties are ignored and writable properties are set to their default values if not specified in the payload. Child objects are deleted if they are not specified in the request payload (except for automatically created objects).
- **PATCH** – Partially updates the object specified in the URL. Only the included properties of the specified object will be updated. Other existing properties will retain their previous values.
- **DELETE** – Deletes the object specified in the URL.

Accept Header and Content Type

All REST API clients must send an HTTP Accept Header that is set to application/json. Otherwise a 406 Not Acceptable error will be returned.

When uploading JSON objects (POST for creating objects, or PUT for updating objects), the `Content-type` HTTP header must be set to `application/json`. Otherwise, a `415 Unsupported Content Type` error will be returned by the API. When uploading Firepower Chassis infrastructure bundles or CSP binaries, the REST API client must set the `Content-type` HTTP header to `multipart/binary`.

HTTP Error Codes

When executing REST API methods, possible HTTP error codes are:

- **200** – Success with output. Method succeeded and equivalent JSON objects are returned.
- **204** – Success with empty output. Method is successful but the content is empty.
- **400** – Request failed. See the error message for more information.
- **403** – Forbidden. Permission Denied. The current user is not allowed to perform the operation.
- **404** – Object not found. The requested object was not found.
- **405** – Method not supported. The requested method is not supported by the API.
- **406** – Not acceptable. Returned when the client requests anything but `application/json`.
- **415** – Unsupported content-type. Returned when the client sends a content-type that is anything but `application/json`.
- **500** – Internal Error. The API encountered an error in serving the request.