Connecting with a Client

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

Note If connecting to the REST API for the first time, you will receive a certificate warning. You need to accept the certificate in order to use the REST API.

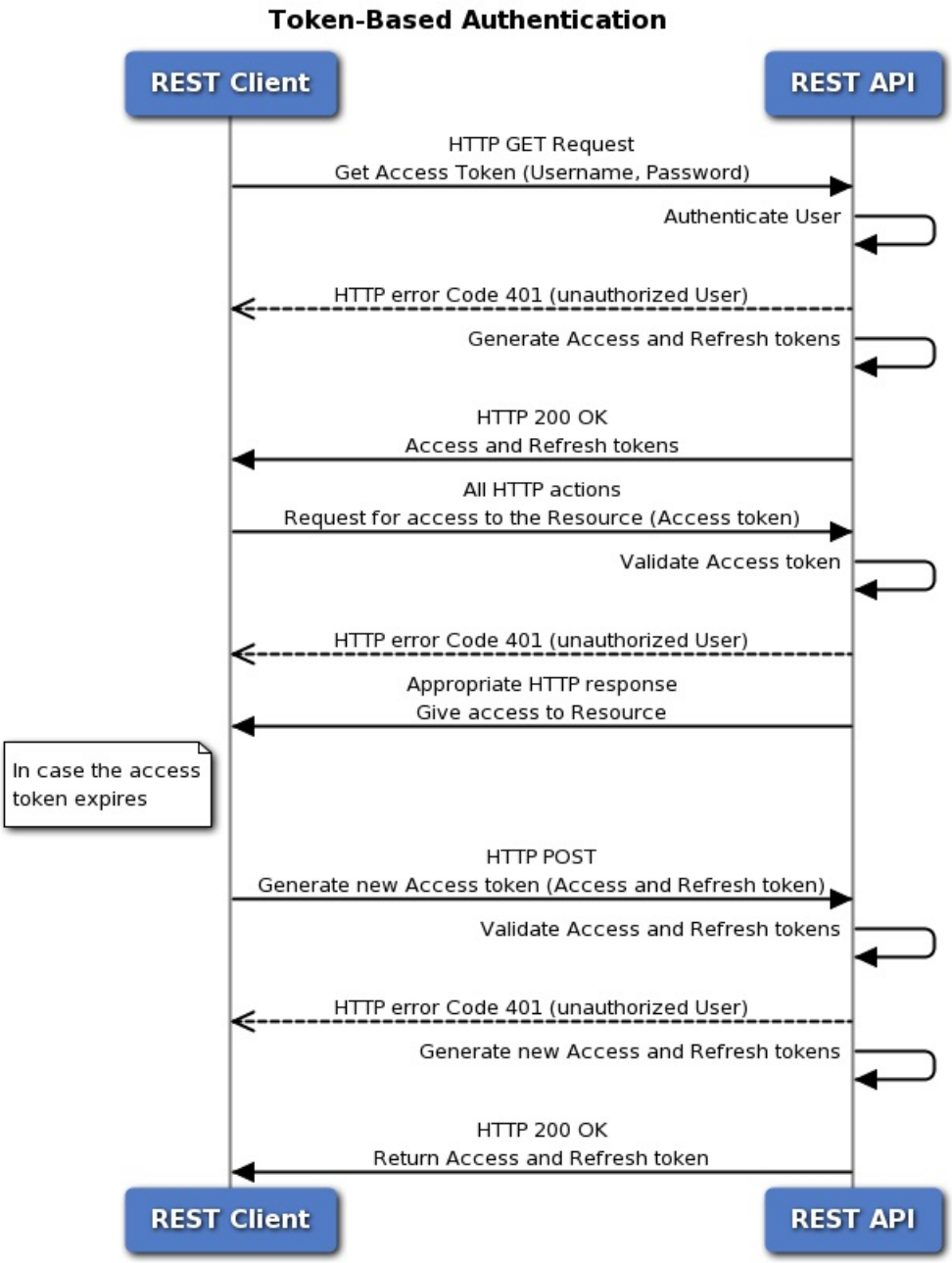
Authentication from a REST API Client

Cisco recommends that you use different accounts for interfacing with the API and the Firepower User Interface. Credentials cannot be used for both interfaces simultaneously, and will be logged out without warning if used for both.

The first time you connect to the REST API you may receive an error that the connection is not secure due to an invalid certificate. Add an exception in your browser to use the certificate and accept the connection.

With Token Based Authentication you obtain a token by providing your username and password. You use this token to access an HTTP service for a limited time period without the need for the username and password with every request. In other words, to eliminate the need for authenticating with your username and password with each request, you replace user credentials with a uniquely generated access token, which you use for accessing resources for up to 30 minutes and can refresh up to three times.

The diagram below illustrates the concept of token-based authentication:



Requesting an Authentication Token

The Token Generation Utility provides an authentication token which can be used in your REST API client.

Before you begin

You must have a configured Firepower Management Center and an account on that center with credentials to use the REST API. You must also have a REST API Client which can perform basic authentication.

Procedure

Step 1 Open your REST API Client.

Step 2 Set the client to make a POST command to the following URL: `https://<management_center_IP_or_name>/api/fmc_platform/v1/auth/generatetoken`.

Step 3 Include the username and password as a basic authentication header. The POST body should be blank.

What to do next

Add the header `X-auth-access-token:<authentication token value>` in requests to the API.

Add the headers `X-auth-access-token:<authentication token value>` and `X-auth-refresh-token:<refresh token value>` in requests to refresh the token as described in Authentication from a REST API Client, on page 1

Use the `Domain_UUID` from the authentication token in all REST requests to the server.

Refreshing an Authentication Token

Firepower Management Center REST API authentication tokens are valid for 30 minutes, and can be refreshed up to three times.

Before you begin

Obtain valid authentication and refresh tokens from the Firepower Management Center REST API. Ensure these tokens have been refreshed less than three times.

Procedure

Step 1 Open your REST API Client.

Step 2 Set the client to make a POST command to the following URL: https://<management_center_IP_or_name>/api/fmc_platform/v1/auth/refreshtoken with the headers `X-auth-access-token:<authentication token value>` and `X-auth-refresh-token:<refresh token value>`.

What to do next

Add the header `X-auth-access-token:<new authentication token value>` in requests to the API.

Add the header `X-auth-refresh-token:<new refresh token value>` in requests to refresh the token.