About the Firepower Management Center REST API

The Firepower Management Center REST API provides a lightweight API to manage a Firepower Management Center.

- About the Firepower Management Center REST API, on page 1
- Enabling the REST API, on page 1
- Best Practices, on page 2

About the Firepower Management Center REST API

With the release of Cisco's Firepower Management Center REST API, you now have light-weight, easy-to-use option for managing Firepower Threat Defense and legacy Firepower devices through a Firepower Management Center.

The REST API is an application programming interface (API), based on "RESTful" principles, which you can quickly enable on any Firepower Management Center running version 6.1 or higher, and use with a REST client.

After installing a REST client, you can contact the specific Firepower Management Center's REST agent and use standard HTTP methods to access current configuration information, and issue additional configuration parameters.

Enabling the REST API

In Firepower Management Center, the REST API is enabled by default. However, if you are intending to use the REST API, you should confirm that it is enabled.

Note If you are using UCAPL mode, check that the REST API is not enabled.

Step 1 Navigate to System>Configuration>REST API Preferences>Enable REST API

Step 2 Check the "Enable REST API" checkbox.

Step 3 Click "Save". A box saying "Save Successful" will display when the REST API is enabled.

Best Practices

Cisco recommends the following best practices for optimal results with the REST API:

- Keep UI users and script users separate. Especially do not use the admin account as an API user.
- Do not give script users more privilege than needed.
- Always validate the content coming from the server.
- Validate/sanitize JSON content, as it may include embedded executable code.
- If you are using CC or UCAPL mode you should disable REST API access to the Firepower Management Center and managed devices.