Cisco ACI Support for NGINX Rate Limit

Revised: June 21, 2022

New and Changed Information

This document provides procedures for configuring the NGINX rate limit feature. The following table provides an overview of the significant changes to this guide up to this current release.

Table 1: New and Changed Information In This Document

Feature	Description
Initial release of document	Initial release of document

Understanding the NGINX Rate Limit Feature

NGINX provides REST API services to clients who can read and configure the Cisco ACI fabric. Clients could be the APIC GUI or scripts that have been developed by you or by Cisco.

These services are provided to verify the authentication procedure. If a client sends multiple requests that competes with other applications, then the serviceability of NGINX would be affected for any trusted client as well. For example, if a script sends the same requests in a loop, that will result in the requests being handled in a certain sequence, which will leave other requests waiting for a long period of time where those other requests will eventually time out.

Beginning with Cisco APIC Release 4.2(3), the NGINX rate limit feature is now available to avoid this situation.

Note This procedure describes how to configure the NGINX rate limit (global throttling). For information on configuring HTTP and HTTPS AAA login throttling, see "Configuring HTTP and HTTPS Throttling Using the CLI" in the *Cisco APIC REST API Configuration Guide*.

Configuring NGINX Rate Limit Using the GUI

Procedure

Step 1 Navigate to **Fabric** > **Fabric Policies** > **Policies** > **Pod** > **Management Access**, then select the `default` management access policy.

The properties window for the default management policy is displayed.

Step 2 Determine if you want to enable global throttling for HTTP or HTTPS requests.

- If you want to enable global throttling for HTTP requests:
  - **a.** Locate the **HTTP** area in the window, then locate the **Request Throttle** field in the **HTTP** area.

    The setting for this field should be set to **Disabled** by default.
  - **b.** Click **Enabled** to enable global throttling for HTTP requests.

The **Throttle Rate** field appears.

c. Set the throttle rate for the HTTP requests:

- Enter a number between 1 and 10000 to set the global throttle rate for HTTP requests.
- Select either **Requests/Second** or **Requests/Minute** to set the global throttle unit as either the number of requests per second or the number of requests per minute.

- If you want to enable global throttling for HTTPS requests:

a. Locate the **HTTPS** area in the window, then locate the **Request Throttle** field in the **HTTPS** area.

The setting for this field should be set to **Disabled** by default.

b. Click **Enabled** to enable global throttling for HTTPS requests.

The **Throttle Rate** field appears.

c. Set the throttle rate for the HTTPS requests:

- Enter a number between 1 and 10000 to set the global throttle rate for HTTPS requests.
- Select either **Requests/Second** or **Requests/Minute** to set the global throttle unit as either the number of requests per second or the number of requests per minute.

Step 3 When you have finished setting the global throttle rate for HTTP or HTTPS requests, click **Submit** in the lower right corner of the window.

Configuring NGINX Rate Limit Using the NX-OS Style CLI

Prior to Cisco APIC Release 4.2(3), the following throttling commands were only available through the NX-OS style CLI:

- **enable-throttle**: Used to enable HTTP or HTTPS AAA login or refresh throttling.
- **throttle**: Used to set the throttle rate used for HTTP or HTTPS communication service after enabling throttling using the **enable-throttle** command.

Beginning with Cisco APIC Release 4.2(3), the following throttling command is now also available:

- **global-throttle**: Used to enable global throttling for HTTP or HTTPS requests.

Note the following behaviors, depending on which throttling command is enabled or disabled:

- When **enable-throttle** is disabled and **global-throttle** is enabled, the login or login refresh is counted as one of the requests in global rate-limiting, but is not counted as login-specific rate-limiting.
- When **enable-throttle** is enabled and **global-throttle** is disabled, only the login or login refresh is affected.

Procedure

Step 1 Navigate to the area in the CLI where you can configure the default communication policy:

Example:

```
apic1# config
apic1(config)# comm-policy default
apic1(config-comm-policy)#
```

Step 2 Determine if you want to enable global throttling for HTTP or HTTPS requests.

- If you want to enable global throttling for HTTP requests, enter `http` to configure the HTTP communication policy group:

```
apic1(config-comm-policy)# http
apic1(config-http)#
```

- If you want to enable global throttling for HTTPS requests, enter `https` to configure the HTTPS communication policy group:

```
apic1(config-comm-policy)# https
apic1(config-https)#
```

Note The commands for the remaining steps are the same, whether you are configuring an HTTP or an HTTPS communication policy group. The following steps show how to configure an HTTP communication policy group as an example.

Step 3 Enable global throttling for the HTTP or HTTPS requests.

Example:

```
apic1(config-http)# global-throttle
apic1(config-http)#
```

Step 4 Set the global throttling rate for the HTTP or HTTPS requests:

```
apic1(config-http)#  global-throttle-rate <1-10000>
```

Example:

```
apic1(config-http)# global-throttle-rate 10000
apic1(config-http)#
```

Step 5 Set the global throttling unit for the HTTP or HTTPS requests.

- To set the global throttling unit as number of requests per second:

```
apic1(config-http)# global-throttle-unit r/s
```

- To set the global throttling unit as number of requests per minute:

```
apic1(config-http)# global-throttle-unit r/m
```

Step 6 To disable global throttling for the HTTP or HTTPS requests:

Example:

```
apic1(config-http)# no global-throttle
apic1(config-http)#
```

Step 7 Exit the configuration area for the default communication policy in the CLI.

Example:

```
apic1(config-http)# exit
apic1(config-comm-policy)# exit
apic1(config)# exit
apic1#
```

Configuring NGINX Rate Limit Using the REST API

Procedure

Step 1 Configure the NGINX rate limit feature through the REST API.

The following configurable properties are added to the communication policy, where:

- `globalThrottleSt` is used to enable or disable the feature
- `globalThrottleRate` is used to set the global throttling rate
- `globalThrottleUnit` is used to set the global throttling unit

```
<type name="RateUnitType" base="string:Basic">
    <allowed name="uname" type="include" regex="[r]/[ms]"/>
</type>

<property name="globalThrottleSt"
    label="Throttle state for all clients without tag0 in header"
    type="AdminState"
    owner="management"
    mod="explicit"
    >
    <default value="disabled"/>
</property>

<property name="globalThrottleRate"
    type="scalar:Uint32"
    owner="management"
    mod="explicit"
    label="The maximum MO api calls allowed per unit time"
    >
    <default value="10000"/>
    <range min="1" max="10000"/>
</property>

<property name="globalThrottleUnit"
    type="RateUnitType"
    owner="management"
    mod="explicit"
    label="Unit of rate limit"
    >
    <default value="r/s"/>
</property>
```

Step 2 To enable the NGINX rate limit feature:

```
POST:
                 {{url}}/api/node/mo/uni/fabric/comm-default/http.xml
BODY:
                <commHttp globalThrottleSt="enabled"  dn="uni/fabric/comm-default/http"
 globalThrottleRate="1" globalThrottleUnit="r/m" ></commHttp>

 OPTIONS:
              globalThrottleSt: "enabled" or "disabled"
              globalThrottleRate: "1" to "10000"
              globalThrottleUnit="r/s" or "r/m"
```

The rate can be configured using a range of 1 to 10000, which could be rate per second or rate per minute.

Step 3 To disable the NGINX rate limit feature:

```
POST:
                 {{url}}/api/node/mo/uni/fabric/comm-default/http.xml
BODY:
                <commHttp globalThrottleSt="disabled"  dn="uni/fabric/comm-default/http"
  globalThrottleRate="1" globalThrottleUnit="r/m" ></commHttp>
```

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.