Throttling

The **throttle mechanism** is used to control access to the services at different levels. WSO2 ESB provides an effective and efficient way to apply the throttle mechanism to your Web services.

**Levels of throttling**

You can enable throttling at the following levels in WSO2 ESB:

- **Global level** - If it is enabled globally, restrictions are applied globally (for every message coming into the server).
- **Service level** - If it is enabled for a particular service, restrictions are applied to all the messages coming into that service.

Click on the relevant tab for instructions to add a throttling policy at the required level.

**Global level**

Follow the instructions below to define a throttle policy at a global level.

1. Enter your user name and password to log on to the ESB Management Console.
2. Go to the **Main** tab. In the **Modules** section, click **List** to open the **Deployed Modules** page.
3. In the row that displays `wso2throttle` module, click **Configure** to open the **Global Throttling Configuration** page.

4. In the **Enable Throttling** parameter, select **Yes**. The existing throttle configuration will appear in the wizard as shown in the example below.

Configure the following parameters as required to update the throttle policy.
<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Concurrent Accesses</td>
<td>The maximum number of requests served concurrently by the service at any given time.</td>
</tr>
<tr>
<td>Range</td>
<td>The range of IP addresses or the domain (based on the value selected for the Type parameter) to be restricted from accessing the service. Requests from these IP addresses/domains will be restricted based on the specified values.</td>
</tr>
<tr>
<td>Type</td>
<td>This specifies the basis on which the clients should be restricted from accessing the proxy service. Possible values are as follows.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP</strong>: This restricts access to the service based on the IP address of the client. If you select this, enter the relevant range of IP addresses in the Range parameter (e.g., <code>10.1.30-10.100.1.60</code>).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Domain</strong>: This restricts access to the service based on the domain of the client. If you select this, enter the relevant domain in the Range parameter (e.g., <code>*.wso2.com</code>).</td>
</tr>
</tbody>
</table>

It is recommended to use IP based throttling instead of domain based throttling since the performance overhead is minimal when IP based throttling is used.

Since the use of domain based throttling results in a high performance overhead, it is not provided by default with the ESB distribution. However, it can be provided as a patch if you need to use domain based throttling.

Max Request Count: This parameter specifies the maximum number of requests that should be handled within the time interval specified in the Unit Time parameter.

- This parameter is applicable only when the value selected for the Access parameter is Control.

Unit Time (ms): The time interval for which the maximum number of requests specified for the Throttle ID in the Max Request Count parameter apply.

- This parameter is applicable only when the value selected for the Access parameter is Control.
Prohibit Time Period (ms) | If the number of requests entered in the Max Request Count parameter is achieved before the time interval entered in the Unit Time (ms) parameter has elapsed, no more requests are taken by the inflow throttle handler for the time period entered in this parameter. Entering a value in this parameter alters the unit time.

For example:

Max Request Count = 50
Unit Time = 50000 ms
Prohibit Time Period = 5000 ms

If 50 requests are received within 35000 milliseconds, no requests will be taken for the next 5000 milliseconds. Thus, the time slot considered as the unit time is changed to 40000 milliseconds. If no value is entered in the Prohibit Time Period (ms) parameter, no requests will be taken until 15000 more milliseconds (i.e. the remainder of the unit time) have elapsed.

Access | This parameter is applicable only when the value selected for the Access parameter is Control.

This parameter is used to specify the extent to which the IP addresses/domains specified in the Range parameter are allowed access to the service to which the throttle policy is applied. Possible values are as follows.

- **Allow**: If this is selected, the specified IP addresses/domains are allowed to access the services to which the throttle ID is applied without any restrictions.
- **Deny**: If this is selected, specified IP addresses/domains are not allowed to access the services to which the throttle ID is applied.
- **Control**: If this is selected, the specified IP addresses/domains are allowed to access the services to which the throttle ID is applied. However, the number of times they can access the services is controlled by the Max Request Count, Unit Time (ms), and the Prohibit Time Period (ms) parameters.

Actions | Click Delete in the relevant row to delete an entry.

5. Click **Finish** to save the information.

Follow the instructions below to define a throttle policy for a service.

1. Enter your user name and password to log on to the ESB Management Console.
2. Click the **Main** tab. Under **Web Services**, click **List** to open the **Deployed Services** page.

![Deployed Services](image1)

3. Click on the service for which you want to enable throttling to open its Service Dashboard.

![Service Dashboard](image2)

4. In the **Quality of Service Configuration** panel, click **Access Throttling**. The **Throttling Configuration** page for the service will appear.

![Quality of Service Configuration](image3)

In the **Enable Throttling** parameter, select **Yes**. The existing throttle configuration will appear in the wizard as shown in the example below.

![Enable Throttling](image4)
Configure the following parameters as required to update the throttle policy.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Concurrent Accesses</td>
<td>The maximum number of requests served concurrently by the service at any given time.</td>
</tr>
<tr>
<td>Range</td>
<td>The range of IP addresses or the domain (based on the value selected for the Type parameter) to be restricted from accessing the service. Requests from these IP addresses/domains will be restricted based on the specified values.</td>
</tr>
<tr>
<td>Type</td>
<td>This specifies the basis on which the clients should be restricted from accessing the proxy service. Possible values are as follows.</td>
</tr>
<tr>
<td></td>
<td>- <strong>IP</strong>: This restricts access to the service based on the IP address of the client. If you select this, enter the relevant range of IP addresses in the Range parameter (e.g., 10.1.30–10.100.1.60).</td>
</tr>
<tr>
<td></td>
<td>- <strong>Domain</strong>: This restricts access to the service based on the domain of the client. If you select this, enter the relevant domain in the Range parameter (e.g., *.wso2.com).</td>
</tr>
<tr>
<td>Note</td>
<td>It is recommended to use IP based throttling instead of domain based throttling since the performance overhead is minimal when IP based throttling is used.</td>
</tr>
<tr>
<td></td>
<td>Since the use of domain based throttling results in a high performance overhead, it is not provided by default with the ESB distribution. However, it can be provided as a patch if you need to use domain based throttling.</td>
</tr>
<tr>
<td>Max Request Count</td>
<td>This parameter specifies the maximum number of requests that should be handled within the time interval specified in the Unit Time parameter.</td>
</tr>
<tr>
<td></td>
<td>This parameter is applicable only when the value selected for the Access parameter is Control.</td>
</tr>
<tr>
<td>Unit Time (ms)</td>
<td>The time interval for which the maximum number of requests specified for the Throttle ID in the Max Request Count parameter apply.</td>
</tr>
<tr>
<td></td>
<td>This parameter is applicable only when the value selected for the Access parameter is Control.</td>
</tr>
</tbody>
</table>
4. **Prohibit Time Period (ms)**

If the number of requests entered in the **Max Request Count** parameter is achieved before the time interval entered in the **Unit Time (ms)** parameter has elapsed, no more requests are taken by the inflow throttle handler for the time period entered in this parameter. Entering a value in this parameter alters the unit time.

For example:

Max Request Count = 50  
Unit Time = 50000 ms  
Prohibit Time Period = 5000 ms

If 50 requests are received within 35000 milliseconds, no requests will be taken for the next 5000 milliseconds. Thus, the time slot considered as the unit time is changed to 40000 milliseconds. If no value is entered in the **Prohibit Time Period (ms)** parameter, no requests will be taken until 15000 more milliseconds (i.e. the remainder of the unit time) have elapsed.

This parameter is applicable only when the value selected for the **Access** parameter is **Control**.

5. **Access**

This parameter is used to specify the extent to which the IP addresses/domains specified in the **Range** parameter are allowed access to the service to which the throttle policy is applied. Possible values are as follows.

- **Allow**: If this is selected, the specified IP addresses/domains are allowed to access the services to which the throttle ID is applied without any restrictions.
- **Deny**: If this is selected, specified IP addresses/domains are not allowed to access the services to which the throttle ID is applied.
- **Control**: If this is selected, the specified IP addresses/domains are allowed to access the services to which the throttle ID is applied. However, the number of times they can access the services is controlled by the **Max Request Count**, **Unit Time (ms)**, **Prohibit Time Period (ms)** parameters.

5. **Actions**

Click **Delete** in the relevant row to delete an entry.

You can create as many entries as required by clicking **Add New Entry**.

5. Click **Finish** to save the information.

You can also specify the throttle policy within a proxy service configuration as a key by saving the policy in the *registry* or by saving it as a local entry. However, when you are not using the Management Console, you are required to manually create an entry in the `<ESB_HOME/repository/deployment/server/servicemetafiles/<Service_Name>.xml` file to enable throttling as shown in the example below.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<serviceGroup name="ThrottleProxy" successfullyAdded="true">
  <service name="ThrottleProxy" exposedAllTransports="false" serviceDeployedTime="1431430083400" successfullyAdded="true">
    <operation name="mediate">
      <module name="addressing" version="4.2.0" type="engagedModules"/>
      <module name="POXSecurityModule" version="4.2.2" type="engagedModules"/>
      <module name="wso2statistics" version="4.2.2" type="engagedModules"/>
      <module name="ServerAdminModule" version="4.2.0" type="engagedModules"/>
    </operation>
  </service>
</serviceGroup>
```
<module name="pagination" version="4.2.0" type="engagedModules"/>
</operation>
</bindings>

<binding name="ThrottleProxySoap12Binding">
  <operation name="mediate"/>
  <operation name="GetMetadata"/>
</binding>

<binding name="ThrottleProxySoap11Binding">
  <operation name="mediate"/>
  <operation name="GetMetadata"/>
</binding>

<binding name="ThrottleProxyHttpGetBinding">
  <operation name="mediate"/>
  <operation name="GetMetadata"/>
</binding>
</bindings>

<policies>
  <policy policyType="3">
    <policyUUID>WSO2ServiceThrottlingPolicy</policyUUID>
      xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
      wsu:Id="WSO2ServiceThrottlingPolicy">
      <throttle:ServiceThrottleAssertion xmlns:throttle="http://www.wso2.org/products/wso2commons/throttle">
        <wsp:Policy>
          <throttle:ID throttle:type="IP">10.100.0.37</throttle:ID>
        </wsp:Policy>
        <throttle:Control>
          <wsp:Policy>
            <throttle:MaximumCount>5</throttle:MaximumCount>
            <throttle:UnitTime>100000</throttle:UnitTime>
            <throttle:ProhibitTimePeriod wsp:Optional="true">10000</throttle:ProhibitTimePeriod>
          </wsp:Policy>
        </throttle:Control>
      </wsp:Policy>
      <wsp:Policy>
        <throttle:ID throttle:type="DOMAIN">localhost</throttle:ID>
      </wsp:Policy>
      <throttle:Control>
        <wsp:Policy>
          <throttle:MaximumCount>1</throttle:MaximumCount>
          <throttle:UnitTime>10000</throttle:UnitTime>
          <throttle:ProhibitTimePeriod wsp:Optional="true">10000</throttle:ProhibitTimePeriod>
        </wsp:Policy>
      </w throttle:Control>
    </wsp:Policy>
  </policy>
</policies>
The proxy service configuration in this example can be as follows.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<proxy xmlns="http://ws.apache.org/ns/synapse"
    name="ThrottleProxy"
    transports="https http"
    startOnLoad="true"
    trace="disable">
    <description/>
    <target>
        <endpoint>
            <address uri="http://localhost:9000/services/SimpleStockQuoteService"/>
        </endpoint>
        <inSequence>
            <log level="full"/>
        </inSequence>
    </target>
</proxy>
```
The following is an example of a throttle policy configuration that can be saved in the registry or as a local entry.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<localEntry xmlns="http://ws.apache.org/ns/synapse" key="throttlePolicy1">
        xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
        wsu:Id="WSO2ServiceThrottlingPolicy">
        <throttle:ServiceThrottleAssertion xmlns:throttle="http://www.wso2.org/products/wso2commons/throttle">
            <wsp:Policy>
                <throttle:ID throttle:type="IP">10.100.0.37</throttle:ID>
                <wsp:Policy>
                    <throttle:Control>
                        <wsp:Policy>
                            <throttle:MaximumCount>5</throttle:MaximumCount>
                            <throttle:UnitTime>100000</throttle:UnitTime>
                            <throttle:ProhibitTimePeriod wsp:Optional="true">10000</throttle:ProhibitTimePeriod>
                        </wsp:Policy>
                    </throttle:Control>
                </wsp:Policy>
            </wsp:Policy>
            <wsp:Policy>
                <throttle:ID throttle:type="DOMAIN">localhost</throttle:ID>
                <wsp:Policy>
                    <throttle:Control>
                        <wsp:Policy>
                            <throttle:MaximumCount>5</throttle:MaximumCount>
                            <throttle:UnitTime>100000</throttle:UnitTime>
                            <throttle:ProhibitTimePeriod wsp:Optional="true">10000</throttle:ProhibitTimePeriod>
                        </wsp:Policy>
                    </throttle:Control>
                </wsp:Policy>
            </wsp:Policy>
            <wsp:Policy>
                <throttle:ID throttle:type="IP">127.0.0.1</throttle:ID>
                <wsp:Policy>
                    <throttle:Control>
                        <wsp:Policy>
                            <throttle:MaximumCount>5</throttle:MaximumCount>
                            <throttle:UnitTime>100000</throttle:UnitTime>
                            <throttle:ProhibitTimePeriod wsp:Optional="true">10000</throttle:ProhibitTimePeriod>
                        </wsp:Policy>
                    </throttle:Control>
                </wsp:Policy>
            </wsp:Policy>
        </wsp:Policy>
    </wsp:Policy>
</localEntry>
```

You need to use the same string (e.g., `throttlePolicy1`) for the throttle policy key of both the proxy service configuration, and the local entry definition, which is saved in the registry.
</wsp:Policy>
</throttle:Control>
</wsp:Policy>
</throttle:ServiceThrottleAssertion>
</wsp:Policy>
<description/>
</localEntry>