Cookbook - Security access control

Overview

Security Access Control (SAC) is a utility to control access to available API. The control is focused around security concern in terms of addressing unauthorised access and DoS attacks.

Default extension

SAC service is implemented as an extension to sacFilter through **SYS.httpSecurityAccessControlService** extension point. Default implementation is ServletRequestSecurityAccessControlServiceImpl, which allows:

- IP whitelisting
- IP blacklisting
- Throttling (global and by IP)

Default extension enablement:

```
SYS.httpSecurityAccessControlService=servletRequestSecurityAccessControlSe
rvice
```

Detailed configuration is accomplished via **SYSTEM_EXTENSION_CFG_SECURITY** system attribute.

Note that all changes to SAC config will take place only after reloading system configurations from the configurations panel in Admin.

Configuration	Example	Purpose
[NodeType].HTTP.maxRequestsPerMinute	SFW.HTTP.maxRequestsPerMinute=5000	Limit overall number of requests per minute (integer) ⚠ For frontend application this would include media files and all resources fetched to render the web pages Note Type corresponds to the node type of the application i.e. ADM, API, SFW, SFG etc

[NodeType].HTTP.maxRequestsPerMinutePerIP	SWF.HTTP.maxRequestsPerMinutePerIP=300	Limit number of requests per minute per IP (integer) ⚠ For frontend application this would include media files and all resources fetched to render the web pages Note Type corresponds to the node type of the application i.e. ADM, API, SFW, SFG etc Offending IP addresses will be reported to alerts in admin app.
[NodeType].HTTP.blockIPCSV	SFW.HTTP.blockIPCSV=192.0.0.18,192.10	Comma separated list of "starts with" IP declarations to blacklist. Note that the declaration has to conform to the IP resolver (Recommended approach is to track IP addresses reported in alerts and add them). You can also blacklist networks by specifying only the beginning of the IP. This setting is mutually exclusive to "HTTP.allowIPCSV"
[NodeType].HTTP.allowIPCSV=192.0.0.18,192.10	SFW.HTTP.allowIPCSV=192.0.0.18,192.10	Comma separated list of "starts with" IP declarations to whitelist. It is recommended to use this setting for the admin app to limit access only to known networks. You can also whitelist networks by specifying only the beginning of the IP. This setting is mutually exclusive to "HTTP.blockIPCSV"

Example config

```
# Limiting Admin to access only from known IP
ADM.HTTP.maxRequestsPerMinute=1000
ADM.HTTP.allowIPCSV=192.0.0.18

# Frontend (limits should include resources)
SFG.HTTP.maxRequestsPerMinute=5000
SFG.HTTP.maxRequestsPerMinutePerIP=300
SFW.HTTP.maxRequestsPerMinute=5000
SFW.HTTP.maxRequestsPerMinutePerIP=300
# Blocking bad IPs from accessing frontend
SFW.HTTP.blockIPCSV=192.0.0.18

# REST API (only API calls)
API.HTTP.maxRequestsPerMinute=1000
API.HTTP.maxRequestsPerMinutePerIP=10
```