



Opsview Inc.
185 Alewife Brook Parkway
Suite 210, Cambridge,
MA 02138

w: www.opsview.com
e: sales@opsview.com

OPSVIEW CLOUD ACCEPTABLE USE POLICY

This Policy describes acceptable use of the Opsview Cloud service and associated infrastructure. This Policy supplements and is incorporated in the Opsview Cloud Service Terms and Conditions Attachment (published at www.opsview.com/legal).

1. Granting web access to thirty parties

- a. Opsview Cloud's multi-tenant capabilities allow Customers to grant access to the web interface to their own customers or other third parties. Customers are responsible for ensuring that any user granted access to the system acts in accordance with this Acceptable Use Policy and our Terms and Conditions.

2. Secure access

- a. Users of Opsview Cloud must take appropriate steps to ensure that their user accounts can only be accessed by authorized individuals, such as:
 - i. Setting a strong password
 - ii. Minimizing privileges assigned to accounts to limit access to only what is required
 - iii. Deleting accounts that are no longer required

3. Service check intervals

- a. The service check interval allows users to set how often specific monitoring checks are executed by the system, and hence the amount of information collected and processed.
- b. Users should consider the data being collected and its rate of change to determine appropriate service check intervals. High frequency monitoring (check intervals less than one minute) should be used with care as this can significantly increase the load on the system and the amount of data that must be stored for graphing and reporting purposes.

4. Data storage

- a. Opsview Cloud allows users to set separate retention periods for both summary information and full resolution data in the Opsview Data Warehouse, with default values of 13 months and 3 months respectively. Graphing data (performance data) is retained in InfluxDB for 13 months regardless of these settings. Customers wishing to store data for longer periods should contact their Opsview Account Manager to discuss your options.

5. Opsview Cloud API

- a. Opsview Cloud offers a powerful REST API for users to perform automated configuration of the system, to trigger actions, and to extract collected monitoring data. Whilst proper use of the API is encouraged, consideration should be given to the nature and frequency of requests due to the impact that these may have on the performance of the system. For example:
 - i. Request only the data that is required by using appropriate filters
 - ii. For recurring requests such as retrieval of status data, consider the service check intervals in use and set an appropriate API request interval

- iii. Ensure scripted API requests handle failures or delays appropriately, e.g. using exponential back off
- iv. Queuing API requests and/or limiting the number of concurrent requests

6. Abuse

- a. Opsview Cloud must only be used for the purpose of monitoring and must not be used or misused in any way which would constitute abuse of the system. Prohibited uses include, but are not limited to:
 - i. Sending unsolicited email or bulk email
 - ii. Causing a denial of service attack against any third party
 - iii. Storing, sharing, or otherwise making copies of illegal or inappropriate content
 - iv. Using system resources for computational tasks such as Bitcoin mining
 - v. Interrogating and/or collecting data from any third-party system or infrastructure when you do not have permission to do so
 - vi. Use for any illegal purpose or in violation of any laws (including without limitation data, privacy, consumer protection, and export control laws).
 - vii. Violating the privacy or confidentiality of others, including by transmitting, storing, displaying, distributing or otherwise making available others' private or confidential information

7. Infringement

- a. Customers must not use Opsview Cloud in any way that would cause an infringement, dilution, misappropriation or other violation any intellectual property or proprietary rights of others, including but not limited to copyrights and rights arising from patents, trademarks and trade secrets.

If you violate this Policy, Opsview may suspend or terminate your use of Opsview Cloud. Opsview's right to suspend or terminate your use applies even if a breach is committed unintentionally or without your authorization if Opsview believes that suspension or termination is necessary to ensure compliance with laws or to protect the rights, safety, privacy, security or property of Opsview, its customers or third parties.