FIREEYE TECHNICAL DOCUMENTATION

FIREEYE
API REFERENCE
RELEASE 2020.1

FireEye API Reference

Software Release 2020.1

Revision 1

FireEye Contact Information:

Website: www.fireeye.com/company/contact-us.html

Technical Support: csportal.fireeye.com

Phone (US):

1.408.321.6300

1.877.FIREEYE

Contents

PART I: Overview

This section covers the following topics:

What's New

This reference documents version 2.0 of the Web Services API. The following changes have been made since version 1.2:

- When using the Alert Acknowledgment API, you must use the alert's UUID. The v1.2.0 version of this endpoint is unchanged and accepts either the alert infection ID or UUID.
- The YARA rules endpoints are now supported on VX Series appliances.
- The new `schema_compatibility` parameter for the Alert Acknowledgment API specifies XML and JSON content compatible with the upgraded schema. Omit this option if you are using an older schema and do not want schema compatibility.
- The Alert and Result response body of the Alert Request API has a new flag, `malicious`, that indicates if a sample is malicious or not.

Changes in 2018.02, revision 2:

- VX Series-specific URLs have been corrected.

Changes in 2018.03:

- The Submit Malware Object request has two new submission options:
  - `enable_vnc`—Enables VNC while making a submission on an Malware Analysis appliance.
  - `properties`—Provides additional context about a submission.
- The new Submission Queue Size Request gets the total number of running and queued submissions on Malware Analysis appliances.
- The Alerts endpoint no longer returns the `X-FireEye-Verdict` header. The verdict is now returned in the response body of the Submission Results endpoint.
- The new System Health Request returns detailed system health status on Network Security appliances.

Changes in 2018.05:

- The System Health request is now available on all appliances.
- The Alerts response now shows the acknowledgment status as `"ack":"`*`status`*`"`.

Changes in 2018.05, revision 2:

- Corrected a typo in the VX Series Submission Results URL.

Changes in 2018.05, revision 3:

- Corrected the `analysistype` value for `sandbox`.

Changes in 2018.05, revision 4:

- The Submit URL Request is not supported on VX Series appliances.

Changes in 2019.01:

- The new Alert Details request gets details for a single alert.
- The new System Current Health request returns the current system health status.
- The new System Health History request returns the system health status for a given time period.

Changes in 2019.02:

- The Statistics request has a new optional parameter `include_submission_stats`.
- The v2.0.0 version of the Alerts Updated with ATI Details request is deprecated.
- Admin users can now access Web service API.
- The Events request has a new option to indicate whether to include all IPS events or MVX-correlated events only.
- There are three new custom IOC endpoints:
  - List a YARA Rule
  - Download a YARA Rule File
  - Download a Custom Snort Rule File

Changes in 2019.03:

- Added Email Quarantine endpoints.
- Added a note to the Reports by Time request about using the `limit` parameter with IPS report types.

Changes in 2019.03, revision 2:

- The section on Submission Limits has been removed as it no longer applies.

Changes in 2020.1, revision 1:

- Added Network Security IPS API endpoints.
- Added Central Management IPS API endpoints.

Introduction

The Web Services Application Programming Interface (API) allows FireEye's partners to access FireEye product alert records and reports and to submit malware objects and URLs for evaluation. The Web Services API is a role-based access control (RBAC) compliant Representational State Transfer (REST) interface.

The Web Services API supports both XML and JSON output. Furthermore, the Web Services API works on top of a unified alert access system, allowing any authenticated client to request alert records based on certain criteria.

During normal operations, the Central Management appliance receives alerts and other data from the networked appliances. This data is held in the Central Management database and is used to produce reports and alerts that are then available to the system users. Use the Web Services API to access and update these reports and alerts. You can also use the Web Services API to submit suspicious objects and URLs to the Malware Analysis appliance.

The commands in this reference are available on the following appliances:

	NX	EX	FX	AX	CM	VX
Authentication	o	o	o	o	o	o
Alerts	o	o	o	o	o	
Artifacts	o	o	o	o	o	
Configuration	o	o	o	o	o	
Email Quarantine		o			o	
Feeds					o	
YARA	o	o	o	o	o	o
SNORT	o				o	
Submission				o	o	o
IPS Events	o				o	
ATI	o	o	o	o	o	
Reports	o	o	o	o	o	
Statistics	o	o				

	NX	EX	FX	AX	CM	VX
Event filters	o					
System Health	o					

Getting Started

Before you can use the FireEye Web Services API, perform the following actions:

- Ensure the FireEye appliances are networked through the Central Management appliance. For more information, see Ensuring the FireEye Appliances Are Networked below.
- Ensure the Central Management appliance is running software version 9.0.0 or higher.
- Ensure any networked appliances are running software version 9.0.0 or higher.
- Enable the Web Service API. For more information, see Enabling the Web Services API below.
- Create one or more Web Services API user accounts. For more information, see Creating a Web Services API User Account on page 17.

Ensuring the FireEye Appliances Are Networked

Appliances need to be networked to use the Web Services API only if you are using the Central Management appliance to retrieve data from another appliance. The Web Services API can also be used directly on the appliances.

To ensure all FireEye appliances are networked:

1. In a Web browser, log in to the Central Management appliance.

   The FireEye Central Management Dashboard opens.
2. Select the Appliances tab.
3. Review the appliances on the Appliances Management screen.

   If any appliances are missing, you need to add the missing appliances. For instructions on adding an appliance, see the *Central Management Administration Guide*.

Enabling the Web Services API

To enable the Web Services API on an integrated appliance:

1. In a terminal window, log in to the command-line interface (CLI) on the appliance where you will run the Web Services API.

2. Enable the CLI configuration mode:

```
hostname > enable
hostname # configure terminal
```

3. Enable the Web Services API:

```
hostname (config) # wsapi enable
```

4. Verify that the Web Services API is enabled.

   For example, if you run the `show wsapi` command on the following appliances:

   FireEye AX 8400:

```
hostname (config) # show wsapi
   Server Enabled                                 :         yes
   Current State                                  :         running
   Max Alerts                                     :         200
   Max Submission Hour Threshold                  :         667
   Max Submission Day Threshold                   :         16000
   Max Minute API (including Submission) Threshold  :       1000
   Max Day API (including Submission) Threshold     :       100000
```

   FireEye CM 4400:

```
hostname (config) # show wsapi
wsapi status:
   Server Enabled                                 :         yes
   Current State                                  :         running
   Max Alerts                                     :         200
   Max Minute Threshold                           :         1000
   Max Day Threshold                              :         1000000
   OS Changes                                     :         no
```

If the Web Services API is enabled, the `Server Enabled` status is set to **yes**.

To enable WSAPI on appliances connected to the Central Management appliance:

- Network Security appliance

  1. Enable the CLI configuration mode:

```
hostname > enable
hostname # configure terminal
```

  2. Enter the following command on the CMS:

```
hostname (config) # cmc execute group sysgroup.Web_MPS command
"wsapi enable"
```

- Email Security — Server Edition appliance

  1. Enable the CLI configuration mode:

```
hostname > enable
hostname # configure terminal
```

  2. Enter the following command on the Central Management CLI:

```
hostname (config) # cmc execute group sysgroup.Email_MPS command
"wsapi enable"
```

Creating a Web Services API User Account

To submit API requests from a remote system, you need a valid API user account on the appliance where you will run the Web Services API. Create one of the following API user accounts:

- api_analyst
- api_monitor

The admin user also has privileges. These profiles provide the remote access privileges listed in the following table.

User Profile Access Privileges

Privilege	api_analyst	api_monitor	admin
Read Alerts	Yes	Yes	Yes
Update Alerts (Central Management)	Yes	No	Yes
Read Reports	Yes	Yes	Yes
Read Stats (Central Management)	Yes	No	Yes
Submit Object	Yes	No	Yes
Submit URL (other appliances)	Yes	No	Yes

For more information about setting up user accounts, see the *Central Management Administration Guide* or the *System Administration Guide* for your appliance.

PART II: Endpoints

The following endpoints are available in the current release:

- **Authentication**—Sends POST requests to authenticate API calls. For more information, see Authentication on page 21.
- **Alerts**—Queries your appliance for alert information. Also acknowledges alerts that have been reviewed. For more information, see Alerts on page 27.
- **Alerts**—Queries the Central Management appliance for alert information. For more information, see Alerts on page 27.
- **Events**—Retrieves Multi-Vector Virtual Execution (MVX) correlated Intrusion Prevention System (IPS) event data from the Network Security appliance managed by your Central Management appliance. For more information, see Events on page 65.
- **Email Quarantine**—Lists, downloads, releases, or deletes quarantined emails. For more information, see Email Quarantine Management on page 85.
- **Reports and Statistics**—Retrieves reports from the FireEye appliances. For more information, see Reports and Statistics on page 97.
- **Submission**—Submits files and URLs for detailed analysis to an Malware Analysis appliance. The Malware Analysis appliance returns a response. For more information, see Malware Objects on page 125.
- **ATI**—Retrieves Advanced Threat Intelligence details for any alert. For more information, see Retrieving ATI Details on page 157.
- **Custom IOCs**—Adds, lists, updates, deletes, or downloads files with custom indicators of compromise (IOCs). For more information, see Custom IOCs on page 1.
- **Logging Out**—Ends the authenticated session between the remote server and your appliance. For more information, see Logging Out on page 249.

Authentication

The Web Services API uses an HTTP Basic authentication scheme to manage authentication between the remote server and your appliance. You need a valid user account on your appliance with the API Analyst or API Monitor profile. You provide the user name and password in an HTTP POST authentication request to your appliance. If the user is authenticated, your appliance provides a session token that maintains authentication for the duration of the current session.

The user account must be established on the appliance you are using to run the Web Services API before you can establish a session between the remote server and your appliance. For more information about setting up user accounts on your appliance, see the *System Administration Guide* for your appliance.

If your account requires the password to be changed when you run the authentication request, an error is returned, and you must change your password to continue using the API. To avoid an interruption in service, FireEye recommends changing passwords before they expire.

The request must be made using the HTTP POST method.

Authentication Request

To log in to your appliance from a remote server using the Web Services API, send the following HTTP POST request URL and headers:

VX Series only:

```
POST https://<address>/wsapis/common/[v1.2.0|v2.0.0]/auth/login?
```

All other appliances:

```
POST https://<address>/wsapis/[v1.2.0|v2.0.0]/auth/login?
```

This command is available on the following appliances:

- Central Management
- Malware Analysis
- Email Security — Server Edition
- File Protect
- Network Security
- VX Series

Required headers:

```
Authorization: Basic [Base64(Username:Password)]
X-FeClient-Token: [Client-Token]
```

Parameters

- address—The IP address of the appliance running the Web Services API.
- Base64 (Username:Password)—The base64-encrypted user name and password supplied by the appliance's administrator.
- Client-Token—(Optional) This client token is provided by FireEye. For more information about the client token, contact your sales representative.

Example

The following is an example of a valid authentication request:

```
POST https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/auth/login
```

Request headers:

```
Authorization: Basic dGVzdDp0ZXN0
X-FeClient-Token: BigDataInc
```

Authentication Response

After it receives the authentication request, your appliance authenticates the user account and responds with either an authentication confirmation code, along with an API-Token used to maintain the authenticated session, or an authentication invalid code.

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Response Fields

- Response Code—A standard HTML response code.
  - 200—Authentication Success
  - 401—Authentication Refused
  - 503—Web Services API server disabled
- Response Message—A standard HTML response message.
  - OK—Authentication Success
  - Unauthorized—Authentication Refused
  - Not available—Web Services API server disabled
- Date—Standard HTML date format
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- Client-Token—(Optional) This client token is provided by FireEye. For more information about the client token, contact your sales representative.

Example

The following is an example of a valid response received from an appliance.

```
HTTP/1.1 [Response Code] [Response Message]
Date: Fri, 20 Oct 2017 08:00:00
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

cURL Code Sample: Authentication

The following code sample can be copied and executed from any command-line interface that includes the cURL library.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSkH --no-progress-bar --header "Authorization: Basic dGVzdDp0ZXN0" -
D /cygdrive/c/tmp/auth.txt -F form=foo
https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/auth/login
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` configuration file will not be read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This option allows you to specify a custom header with the `--header` switch.
- `--no-progress-bar`—This option suppresses the cURL download progress bar, which can interfere with the request.
- `--header "Authorization: Basic dGVzdDp0ZXN0"`—This custom header provides a base64-encoded user name and password to be used to authenticate with your appliance. In this example, `dGVzdDp0ZXN0` resolves to the user name:password key pair: test:test.
- `-D /cygdrive/c/tmp/auth.txt`—This file name and path include the response from your appliance. The contents of this file appear as follows:

  ```
  HTTP/1.1 100 Continue

  HTTP/1.1 200 OK
  Date: Wed, 15 Jan 2014 03:03:15 GMT
  X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  Content-Length: 0
  Content-Type: text/plain; charset=UTF-8
  ```

- `-F form=foo`— The `-F` option and the subsequent empty form force the cURL tool to use the HTTP POST request.
- `https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/auth/login`—The authentication request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the actual IP address of your appliance.

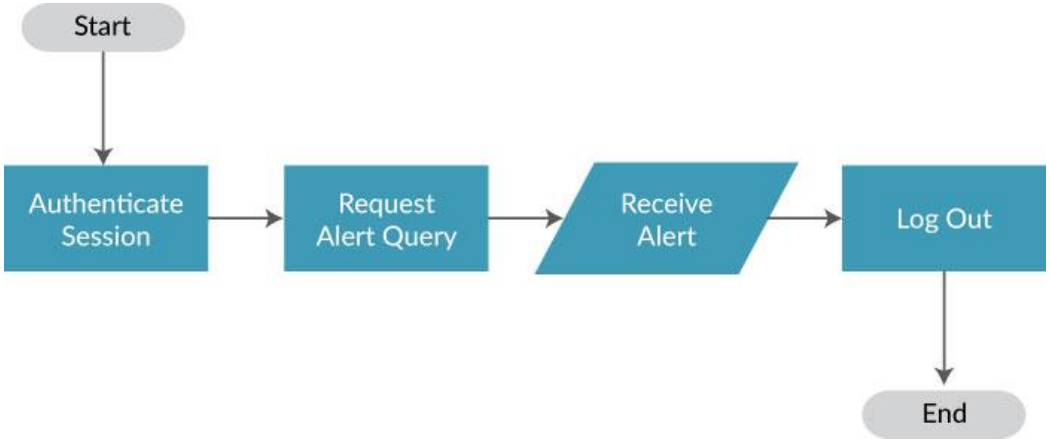
Results

The `auth.txt` file is populated with the response data.

Alerts

The alert request uses the HTTP GET method to retrieve alert data from your appliance. The responses to your alert request can be formatted in either JSON or XML. On the Central Management appliance, you can use the alert acknowledgment request to confirm that you have reviewed the alert so that it is no longer listed in the Web UI.

The following flow chart shows how to issue a basic alert request:



Responses are limited to 200 alerts; this limit cannot be changed. If there are more alerts than 200, the HTTP response code is 206. To avoid receiving the 206 code, reduce the duration of your request until the HTTP response code is 200.

By default, requests are limited to a 12-hour duration. Alerts are either retrieved for the 12 hours after the start time or the 12 hours preceding the end time. You can specify the duration using the `duration` option.

This section covers the following:

- View existing alerts. See Alert Request on the next page.
- Acknowledge a single alert. See Alert Acknowledgment Request on page 48.

Alert Request

You can request existing alert profiles using an HTTP GET request. You can also apply filters to requests. To view existing alerts, send the following HTTP GET request URL and headers:

```
GET https://<address>/wsapis/[v1.2.0|v2.0.0]/alerts?<filters>
```

Availability

This command is available on the following appliances:

- Central Management
- Malware Analysis
- Email Security — Server Edition
- File Protect
- Network Security

Headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
Accept: [Content-Type]
```

Options

- *address*—The IP address of the appliance running the Web Services API.
- *API-Token*—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- *Client-Token*—(Optional) This client token is provided by FireEye. For more information about the client token, contact your sales representative.
- *Content-Type*—(Optional) You can request responses in one of two alert formats:
  - `application/xml`—(Default) If content type is not specified, alerts are delivered in the XML format.
  - `application/json`—Specify this option to receive alerts in JSON format.

The JSON output uses the pretty-print format, which includes line breaks between values.

Filters

Use the filters in the following table to limit your request.

Filter	Description
`alert_id`	Specifies the ID number of the alert to retrieve. Syntax: `?alert_id=`*`id_number`* or `/alert/`*`id_number`* Example: `alerts?alert_id=13705` or `alerts/alert/13705`
`callback_domain`	Searches for alerts that include callbacks to the specified domain. Syntax: `callback_domain=`*`domain`* Example: `callback_domain=onecompany.com`
`dst_ip`	The destination IPv4 address related to the malware alert. Syntax: `dst_ip=`*`ip_address`* Example: `dst_ip=xxx.xxx.xxx.xxx`
`duration`	Specifies the time interval to search. This filter is used with either the `start_time` or `end_time` filter. If duration, start time, and end time are not specified, the system defaults to `duration=48_hours, end_time=`*`current_time`*. If only duration is specified, the `end_time` defaults to the current time.  You cannot specify both a `start_time` filter and an `end_time` filter in the same request. Syntax: `duration=`*`time_interval`* • `1_hour` • `2_hours` • `6_hours` • `12_hours` • `24_hours` • `48_hours` Example: `duration=1_hour&start_time=2017-06-21T16:30:00.000-07:00`

Filter	Description
`end_time`	Specifies the end time of the search. This filter is used with the `duration` filter. If the `end_time` is specified but not the `duration`, the system defaults to `duration=12_hours`, ending at the specified `end_time`.  You cannot specify both a `start_time` filter and an `end_time` filter in the same request. Syntax: `end_time=YYYY-MM-DDTHH:mm:ss.sss-OH:om` • `YYYY`—Year (1900 and later) • `MM`—Month (01-12) • `DD`—Day (01-31) • `HH`—Hour (01-24) • `mm`—Minutes (01-59) • `ss.sss`—Seconds (01-59.999) • `OH:om`—Time offset from UTC Example: `duration=1_hour&end_time=2017-06-21T16:30:00.000-07:00`
`file_name`	The name of the malware file. Syntax: `file_name="file_name"` Example: `file_name="Trojan.Zlob"`
`file_type`	The malware file type. Syntax: `file_type=`*`file_type`* Example: `file_type=com`
`info_level`	Specifies the level of information to be returned. The default is `concise`. • `concise` • `normal` • `extended` Syntax: `info_level=`*`option`* Example: `info_level=normal` **Note:** When using API v1.2.0 at info_level normal or extended, the response includes ATI data. This information is not included in the response when using v2.0.0. To retrieve ATI data for the specific alert ID, use the ATI Details Request on page 163.

Filter	Description
`malware_name`	The name of the malware object. Syntax: `malware_name=`*`name`* Example: `malware_name=trojan.exe`
`malware_type`	The type of the malware object: • `domain_match` • `malware_callback` • `malware_object` • `web_infection` • `infection_match` Syntax: `malware_type=`*`name`* Example: `malware_type=malware_object`
`md5`	Searches for alerts that include a specific MD5 hash.  The `md5` filter is not time dependent; it does not default to `duration=12_hours`. Syntax: `md5=md5hash` Example: `md5=8bc944dbd052ef51652e70a5104492e3`  The system tests for a valid MD5 hash. Using this filter without a qualified MD5 hash will return a 400 Bad Request response.
`recipient_email`	The email address of the malware object receiver. This filter does not default to `duration=12_hours`. Syntax: `recipient_email=`*`email_address`* Example: `recipient_email=jane.doe@somecompany.com`
`sender_email`	The email address of the malware object sender. This filter does not default to `duration=12_hours`. Syntax: `sender_email=`*`email_address`* Example: `sender_email=jane.doe@somecompany.com`
`src_ip`	The source IPv4 address related to the malware alert. Syntax: `src_ip=ip_address` Example: `src_ip=xxx.xxx.xxx.xxx`

Filter	Description
start_time	Specifies the start time of the search. This filter is used with the duration filter. If the start_time is specified but not the duration, the system defaults to duration=12_hours, starting at the specified start_time. You cannot specify both a start_time filter and an end_time filter in the same request. Syntax: start_time=YYYY-MM-DDTHH:mm:ss.sss-OH:om • YYYY—Year (1900 and later) • MM—Month (01-12) • DD—Day (01-31) • HH—Hour (01-24) • mm—Minutes (01-59) • ss.sss—Seconds (01-59.999) • OH:om—Time offset from UTC Example: duration=1_hour&start_time=2017-06-21T16:30:00.000-07:00
url	Searches for a specific alert URL. Syntax: url=url Example: url=http://cms/alerts/list?id=3

Example Request with No Filtering

In this example, the search's duration filter will be set to 12_hours (default), and the end_time filter will be set to the current time (default).

```
GET https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/alerts?
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

Example Request with Filtering

This example specifies the start time and duration.

```
GET https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/
alerts?start_time=2018-07-03T21:19:01:39:000%2b00:00&duration=2_hours
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

Alert Response

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
Content-Type: [Content-Type]
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Response Fields

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 400—Request unsuccessful because the filter value was invalid.
- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Bad Request—Request unsuccessful because the filter value was invalid.
- Date—Standard HTML date format.
- Content-Type—(Optional) You can request responses in one of two formats:
  - `application/xml`—(Default).
  - `application/json`—Must be specified using the `Accept` header.
- *`API-Token`*—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- *`Client-Token`*—(Optional) This client token is provided by FireEye. For more information about the client token, contact your sales representative.

Example Response—Central Management

```
HTTP/1.1 200 OK
Date: Fri, 19 Oct 2018 09:00:00 GMT
```

Body:

Line breaks have been added for readability.

```
{
  "alert": [
    {
      "explanation": {
        "malwareDetected": {
          "malware": [
            {
```

```
              "md5Sum":"fe4d8f227520e2468dd1019496ef0604",
              "sha256":"b71e3012e93f11a7b0b179ea54eeb0e787d02acc48705833e
414a5e57a6a2032",
              "name":"Malware.Binary.FEC2",
              "originalInfectionId":3181,
              "originalInfectionType":"MALWARE_OBJECT",
              "originalInfectionUrl":"https://10.11.113.143/botnets/events_
for_bot?ma_id=3181"
            },
            {
              "md5Sum":"fe4d8f227520e2468dd1019496ef0604",
              "sha256":"b71e3012e93f11a7b0b179ea54eeb0e787d02acc48705833e
414a5e57a6a2032",
              "application":"application:57",
              "httpHeader":"GET http://getapac.com/75.html HTTP/1.1\r\nUser-
Agent: Mozilla/4.0 (Windows XP 5.1) Java/1.6.0_16\r\nHost:
getapac.com\r\nAccept: text/html, image/gif, image/jpeg, *; q=.2, */*;
q=.2\r\nProxy-Connection: keep-alive\r\n\r\n HTTP/1.0 200 OK\r\nDate: Tue, 16
Apr 2013 23:53:28 GMT\r\nServer: Apache\r\nExpires: Mon, 20 Aug 2002 02:00:00
GMT\r\nPragma: no-cache\r\nCache-Control: no-cache\r\nContent-Transfer-
Encoding: binary\r\nContent-Disposition: inline;
filename=setup.exe\r\nContent-Length: 39296\r\nContent-Type:
application/octet-stream\r\nX-Cache: MISS from localhost\r\nX-Cache-Lookup:
MISS from localhost:80\r\nVia: 1.0 localhost (squid/3.1.19)\r\nConnection:
keep-alive\r\n\r\n",
              "original":"setup.exe",
              "name":"Malware.Binary.FEC2",
              "originalInfectionId":3181,
              "originalInfectionType":"MALWARE_OBJECT",
              "originalInfectionUrl":"https://10.11.113.143/botnets/events_
for_bot?ma_id=3181",
              "sid":"0",
              "type":"exe",
              "stype":"avs"
            },
            {
              "md5Sum":"fe4d8f227520e2468dd1019496ef0604",
              "sha256":"b71e3012e93f11a7b0b179ea54eeb0e787d02acc48705833e
414a5e57a6a2032",
              "application":"application:57",
              "httpHeader":"GET http://getapac.com/75.html HTTP/1.1\r\nUser-
Agent: Mozilla/4.0 (Windows XP 5.1) Java/1.6.0_16\r\nHost:
getapac.com\r\nAccept: text/html, image/gif, image/jpeg, *; q=.2, */*;
q=.2\r\nProxy-Connection: keep-alive\r\n\r\n HTTP/1.0 200 OK\r\nDate: Tue, 16
Apr 2013 23:53:28 GMT\r\nServer: Apache\r\nExpires: Mon, 20 Aug 2002 02:00:00
GMT\r\nPragma: no-cache\r\nCache-Control: no-cache\r\nContent-Transfer-
Encoding: binary\r\nContent-Disposition: inline;
filename=setup.exe\r\nContent-Length: 39296\r\nContent-Type:
application/octet-stream\r\nX-Cache: MISS from localhost\r\nX-Cache-Lookup:
MISS from localhost:80\r\nVia: 1.0 localhost (squid/3.1.19)\r\nConnection:
keep-alive\r\n\r\n",
              "original":"setup.exe",
              "name":"JavaExploit.EncryptedPayload",
              "originalInfectionId":3181,
              "originalInfectionType":"MALWARE_OBJECT",
              "originalInfectionUrl":"https://10.11.113.143/botnets/events_
for_bot?ma_id=3181",
              "type":"exe"
            }
          ]
        },
        "osChanges": [
          {
```

```
            "application": {"app-name":"Windows Explorer"},
            "os": {
              "name":"windows",
              "arch":"x64",
              "version":"6.1.7601",
              "sp":1
            },
            "file_informational": [
              {
                "mode":"close",
                "fid": {
                  "ads":"",
                  "content": 3377699720613027
                },
                "sha1sum":"ba5a1564d46348272f970f3c836a9f038528017d",
                "md5sum":"8f66978e66faf1262eca66984f9ee056",
                "processinfo": {
                  "imagepath":"C:\\Windows\\System32\\taskhost.exe",
                  "md5sum":"639774c9acd063f028f6084abf5593ad",
                  "pid":3020
                },
                "sha256sum":"3169bac13d2b500e9deb43c9cbcc27eadfba4d94870c
f7698cb58297d111212b",
                "ntstatus":"0x0",
                "filesize":24576,
                "no_extend":true,
                "value":"C:\\Windows\\System32\\config\\RegBack\\SECURITY",
                "CreateOptions":"0x0",
                "timestamp":2243
              },
              {
                "mode":"close",
                "fid": {
                  "ads":"",
                  "content":1125899906949946
                },
                "processinfo": {
                  "imagepath":"C:\\Windows\\System32\\taskhost.exe",
                  "md5sum":"639774c9acd063f028f6084abf5593ad",
                  "pid":3020
                },
                "ntstatus":"0x0",
                "no_extend":true,
                "value":"C:\\Windows\\System32\\config\\RegBack\\SECURITY.
LOG1",
                "CreateOptions":"0x0",
                "timestamp":2300
              },
              {
                "mode":"close",
                "fid": {
                  "ads":"",
                  "content":1125899906949947
                },
                "processinfo": {
                  "imagepath":"C:\\Windows\\System32\\taskhost.exe",
                  "md5sum":"639774c9acd063f028f6084abf5593ad",
                  "pid":3020
                },
                "ntstatus":"0x0",
                "no_extend":true,
                "value":"C:\\Windows\\System32\\config\\RegBack\\SECURITY
.LOG2",
```

```
                "CreateOptions":"0x0",
                "timestamp":2315
              },
              {
                "mode":"close",
                "fid": {
                  "ads":"",
                  "content":281474976922429
                },
                "sha1sum":"4e9c5284532d348c4845014c349aa88c231e96e4",
                "md5sum":"240fb08bc218a72a1bc6a245d52e7314",
                "processinfo": {
                  "imagepath":"C:\\Program Files\\Windows
Defender\\MpCmdRun.exe",
                  "md5sum":"6bd4d7f68924301051c22e8a951aecba",
                  "pid":3136
                },
                "sha256sum":"a31dcd30c693424b189878d5bd5201cd150578dd906b
547613a709dccce7978a",
                "ntstatus":"0x0",
                "filesize":6662,
                "no_extend":true,
                "value":"C:\\Windows\\Temp\\MpCmdRun.log",
                "CreateOptions":"0x0",
                "timestamp":10183
              },
              {
                "mode":"close",
                "fid": {
                  "ads":"",
                  "content":4222124650748166
                },
                "sha1sum":"af9075a443b76bbe741eceb4188847ac93ff6d6b",
                "md5sum":"f857040c35dc58409500336994a0ef2a",
                "processinfo": {
                  "imagepath":"N/A",
                  "pid":4
                },
                "sha256sum":"97cc6174ef09d68f1693e2821a5e71a24578a86f64c
662a030da93509e483066",
                "ntstatus":"0x0",
                "filesize":196608,
                "no_extend":true,
                "value":"C:\\Windows\\Logs\\SystemRestore\\PropertyPage
.0.etl",
                "CreateOptions":"0x0",
                "timestamp":11184
              },
              {
                "mode":"close",
                "fid": {
                  "ads":"",
                  "content":3659174697325736
                },
                "sha1sum":"15e828174e57fd35b4675d6e06c9c1c01830d2ca",
                "md5sum":"e1ac844fc640df3517f42b32c31b3c05",
                "processinfo": {
                  "imagepath":"C:\\Windows\\System32\\taskhost.exe",
                  "md5sum":"639774c9acd063f028f6084abf5593ad",
                  "pid":3020
                },
                "sha256sum":"d0af7af8ff3c3ba6bbb4289dc4e5b2ea1410d72e8615
3d747473e9faead853b1",
```

```
                "ntstatus":"0x0",
                "filesize":62521344,
                "no_extend":true,
                "value":"C:\\Windows\\System32\\config\\RegBack
\\SOFTWARE",
                "CreateOptions":"0x0",
                "timestamp":11467
              },
              {
                "mode":"close",
                "fid": {
                  "ads":"",
                  "content":1125899906949948
                },
                "processinfo": {
                  "imagepath":"C:\\Windows\\System32\\taskhost.exe",
                  "md5sum":"639774c9acd063f028f6084abf5593ad",
                  "pid":3020
                },
                "ntstatus":"0x0",
                "no_extend":true,
                "value":"C:\\Windows\\System32\\config\\RegBack
\\SOFTWARE.LOG1",
                "CreateOptions":"0x0",
                "timestamp":12375
              },
              {
                "mode":"close",
                "fid": {
                  "ads":"",
                  "content":1125899906949949
                },
                "processinfo": {
                  "imagepath":"C:\\Windows\\System32\\taskhost.exe",
                  "md5sum":"639774c9acd063f028f6084abf5593ad",
                  "pid": 3020
                },
                "ntstatus":"0x0",
                "no_extend": true,
                "value":"C:\\Windows\\System32\\config\\RegBack
\\SOFTWARE.LOG2",
                "CreateOptions":"0x0",
                "timestamp": 12381
              }
            ],
            "uac": [
              {
                "mode":"service",
                "buffered":true,
                "no_extend":true,
                "value":"Volume Shadow Copy",
                "timestamp":10905,
                "status":"running"
              },
              {
                "mode":"service",
                "buffered":true,
                "no_extend":true,
                "value":"Microsoft Software Shadow Copy Provider",
                "timestamp":12887,
                "status":"running"
              }
            ],
```

```
            "end-of-report":"",
            "process_informational": [
              {
                "fid":{
                  "ads":"",
                  "content":281474976725189
                },
                "parentname":"C:\\Program Files\\Windows Defender
\\MpCmdRun.exe",
                "sha256sum":"9afd12eede0db98a35aba52f53041efa4a2f2a0367
3672c7ac530830b7152392",
                "pid":2192,
                "filesize":190976,
                "ppid":3136,
                "mode":"started",
                "cmdline":"\"c:\\program files\\windows defender\\
MpCmdRun.exe\" Scan -ScheduleJob -WinTask -RestrictPrivilegesScan -Reinvoke",
                "sha1sum":"2ae2a6b863616b61ccb550fc1a145ae025896de1",
                "md5sum":"6bd4d7f68924301051c22e8a951aecba",
                "no_extend":true,
                "value":"C:\\Program Files\\Windows Defender\\MpCmdRun.exe",
                "timestamp":10153
              },
              {
                "fid": {
                  "ads":"",
                  "content":281474976780111
                },
                "parentname":"C:\\Windows\\System32\\services.exe",
                "sha256sum":"N/A",
                "pid":1492,
                "filesize":1600512,
                "ppid":480,
                "mode":"started",
                "cmdline":"C:\\Windows\\system32\\vssvc.exe",
                "sha1sum":"1d6f5a5de7154b75144c6a033c36fd86ff2bbe9b",
                "md5sum":"b60ba0bc31b0cb414593e169f6f21cc2",
                "no_extend":true,
                "value":"C:\\Windows\\System32\\VSSVC.exe",
                "timestamp":10547
              },
              {
                "fid": {
                  "ads":"",
                  "content":281474976737050
                },
                "parentname":"C:\\Windows\\System32\\services.exe",
                "sha256sum":"N/A",
                "pid":3632,
                "filesize":27136,
                "ppid":480,
                "mode":"started",
                "cmdline":"C:\\Windows\\System32\\svchost.exe -k swprv",
                "sha1sum":"619652b42afe5fb0e3719d7aeda7a5494ab193e8",
                "md5sum":"c78655bc80301d76ed4fef1c1ea40a7d",
                "no_extend":true,
                "value":"C:\\Windows\\System32\\svchost.exe",
                "timestamp":10836
              }
            ],
            "os_monitor": {
              "date":"Sep 19 2018",
              "build":795854,
```

```
              "time":"12:59:48",
              "version":"17R1.7"
            },
            "malicious-alert": [
              {
                "classtype":"static_log",
                "display-msg":"Static Analysis Malware.Binary.FEC2"
              },
              {
                "classtype":"Static-Analysis",
                "display-msg":"Static Analysis Malware.Binary.FEC2"
              },
              {
                "classtype":"static_log",
                "display-msg":"Static Analysis JavaExploit.EncryptedPayload"
              },
              {
                "classtype":"Static-Analysis",
                "display-msg":"Static Analysis JavaExploit.EncryptedPayload"
              },
              {
                "classtype":"sa_only",
                "display-msg":"Heuristic"
              }
            ],
            "analysis": {
              "mode":"malware",
              "product":"MPS",
              "ftype":"exe",
              "version":1.3977
            }
          },
          {
            "process": {
              "mode":"started",
              "fid": {
                "ads":"",
                "content":1688849860268247
              },
              "parentname":"C:\\WINDOWS\\explorer.exe",
              "cmdline":"\"C:\\WINDOWS\\system32\\ntvdm.exe\" -f -i1",
              "sha1sum":"df36cf59f700fc0b3b60c009b8b877d6233fdd72",
              "md5sum":"681b807e53bdada337735c28c0e48a1b",
              "sha256sum":"a0be52e7d076ed8e33a4b5ab309cd23ad0272570c7e87
fe6e3444712ad467d62",
              "pid":3456,
              "filesize":420864,
              "value":"C:\\WINDOWS\\system32\\ntvdm.exe",
              "timestamp":3478,
              "ppid": 1864
            },
            "application": {"app-name":"Windows Explorer"},
            "os": {
              "name":"windows",
              "arch":"x86",
              "version":"5.1.2600",
              "sp":3
            },
            "file_informational": [
              {
                "mode":"close",
                "fid": {
                  "ads":"",
```

```
                  "content":844424930200765
                },
                "sha1sum":"863bbf5f7f4114a1307c6bad5dd89224d511fed5",
                "md5sum":"4a587187d760161311010b03417b3c3f",
                "processinfo": {
                  "imagepath":"C:\\WINDOWS\\system32\\ntvdm.exe",
                  "md5sum":"681b807e53bdada337735c28c0e48a1b",
                  "pid":3456
                },
                "sha256sum":"b7792de7a6d7abb649a8a22e9048d0468b604ca98b
8978bdd1171356af6d5f49",
                "ntstatus":"0x0",
                "filesize":2686,
                "no_extend":true,
                "value":"C:\\WINDOWS\\Temp\\scs14.tmp",
                "CreateOptions":"0x0",
                "timestamp":3614
              },
              {
                "mode":"close",
                "fid": {
                  "ads":"",
                  "content":562949953490275
                },
                "sha1sum":"8565ed558ad273232104e0b10cd87cff723a1eca",
                "md5sum":"71f4b39c5eb73df738ad3e0dacd89057",
                "processinfo": {
                  "imagepath":"C:\\WINDOWS\\system32\\ntvdm.exe",
                  "md5sum":"681b807e53bdada337735c28c0e48a1b",
                  "pid":3456
                },
                "sha256sum":"d504b1c272cd0c92c4a365086cf884a4889653c89d56
02b6dadeffb33b83951d",
                "ntstatus":"0x0",
                "filesize":1670,
                "no_extend":true,
                "value":"C:\\WINDOWS\\Temp\\scs15.tmp",
                "CreateOptions":"0x0",
                "timestamp":3943
              }
            ],
            "end-of-report":"",
            "os_monitor": {
              "date":"Sep 19 2018",
              "build":795854,
              "time":"12:59:48",
              "version":"17R1.7"
            },
            "malicious-alert": [
              {
                "classtype":"static_log",
                "display-msg":"Static Analysis Malware.Binary.FEC2"
              },
              {
                "classtype":"Static-Analysis",
                "display-msg":"Static Analysis JavaExploit.EncryptedPayload"
              },
              {
                "classtype":"static_log",
                "display-msg":"Static Analysis JavaExploit.EncryptedPayload"
              },
              {
                "classtype":"Static-Analysis",
```

```
                "display-msg":"Static Analysis Malware.Binary.FEC2"
              },
              {
                "classtype":"NTVDM-Process-Launch-Activity",
                "display-msg":"Startup behavior anomalies observed"
              },
              {
                "classtype":"sa_only",
                "display-msg":"Heuristic"
              }
            ],
            "analysis": {
              "mode":"malware",
              "product":"MPS",
              "ftype":"exe",
              "version":1.3977
            }
          }
        ]
      },
      "src": {
        "ip":"157.204.181.231",
        "mac":"00:20:18:11:ff:45",
        "port": 0
      },
      "alertUrl":"https://qa-cm7500-4-9-20/event_stream/events_for_bot?ma_
id=261146",
      "action":"notified",
      "occurred":"2018-10-18 16:46:41 +0000",
      "dst": {
        "mac":"02:14:17:da:c9:2f",
        "port": 0,
        "ip":"249.207.161.251"
      },
      "applianceId":"000BABCD66F2",
      "id": 261146,
      "rootInfection": 3181,
      "sensorIp":"10.11.113.155",
      "name":"MALWARE_OBJECT",
      "severity":"MAJR",
      "uuid":"c9391258-1a79-4b54-be8e-144ddb5f118f",
      "ack":"yes",
      "product":"WEB_MPS",
      "sensor":"cms-nx2500-3",
      "vlan": 0,
      "malicious":"yes"
    }
  ],
  "appliance":"CMS",
  "version":"CMS (CMS) 8.4.0.805144",
  "msg":"normal",
  "alertsCount": 1
}
```


Note: The "uuid" and "ack" fields are only supported in v2.0.0.

cURL Code Sample: Alerts

The following code sample can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSkH --no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/alerts
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This option allows you to specify a custom header with the `--header` switch.
- `--no-progress-bar`—This option suppresses the cURL download progress bar, which can interfere with the request.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header provides the API-Token that was returned during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token value in the code sample with the token value received in the response to your authentication request.

  By default, the `X-FeApi-Token` times out after 15 minutes of inactivity.

- `https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/alerts`—The alert request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.

Results

This code sample returns XML-formatted alert data from your appliance. If you do not receive any alert data and you did not encounter an error message, check your appliance to see whether any alert data is available.

Alert Details Request

Gets details for a single alert.

```
GET https://<address>/wsapis/[v1.2.0|v2.0.0]/alerts/alert/<alert_id>
```

Availability

This command is available on the following appliances:

- Central Management
- Malware Analysis
- Email Security — Server Edition
- File Protect
- Network Security

Required headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
Accept: application/xml
```

Parameters

- *address*—The IP address of the appliance running the Web Services API.
- *alert_ID*—The infection ID. You must also specify the Alert-Type.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- Client-Token—(Optional) This client token is provided by FireEye. For more information about the client token, contact your sales representative.

Example Request

```
GET https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/alerts/alert/4790
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
Accept: application/json
```

Alert Details Response

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
HTTP/1.1 200 OK
Date: Tue, 14 May 2019 22:17:56 GMT
Content-Type: application/xml
```

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<alerts appliance="eMPS" version="eMPS (eMPS) 8.3.0.852440" msg="concise"
xmlns="http://www.fireeye.com/alert/2014/AlertSchema">
  <ns2:alert appliance-id="002590867AAA" id="4790" name="malware-object"
severity="majr" uuid="b435583b-1c23-4a80-b893-203245073ed4" ack="no"
product="Email MPS" vlan="0" malicious="yes" sc-version="866.106">
    <ns2:explanation>
      <ns2:malware-detected>
        <ns2:malware name="Malware.Binary">
          <ns2:md5sum>5e747bddd6a759b0a591ab4bb3b5254b</ns2:md5sum>

          <ns2:sha256>cfbb1006d9e6c2660b4876fecef9789c1a3ac0c807181277a2778c5
9d9b8675f</ns2:sha256>
        </ns2:malware>
      </ns2:malware-detected>
    </ns2:explanation>
    <ns2:src>
      <ns2:smtp-mail-from>testuser1@aedev.com</ns2:smtp-mail-from>
    </ns2:src>
    <ns2:alert-url>https://camelback-sunil-
ex.eng.fireeye.com/emps/eanalysis?e_id=5116&amp;type=attch</ns2:alert-url>
    <ns2:action>blocked</ns2:action>
    <ns2:occurred>2019-05-14T20:53:44.722Z</ns2:occurred>
    <ns2:dst>
      <ns2:smtp-to>testuser2@aedev.com</ns2:smtp-to>
    </ns2:dst>
    <ns2:smtp-message>
      <ns2:subject>Test Email</ns2:subject>
    </ns2:smtp-message>
  </ns2:alert>
</alerts>
```

Response Fields

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 4xx—Request unsuccessful because unknown or invalid fields were included in the input.
  - 5xx—Request unsuccessful because the server encountered a problem.
- Response Message—A standard HTML response message.
  - Empty—Request successful.
  - Invalid Client Request—Request unsuccessful because unknown or invalid fields were included in the input.
  - Server encountered a problem...retry later—Request unsuccessful because the server encountered a problem.
- Date—Standard HTML date format.
- alert fields—The fields returned vary depending on the alert. See the *Alert Notifications* reference guide for descriptions of available fields.

Example Response

```
HTTP/1.1 200 OK
Date: Tue, 14 May 2019 22:17:56 GMT
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<alerts appliance="eMPS" version="eMPS (eMPS) 8.3.0.852440" msg="concise"
xmlns="http://www.fireeye.com/alert/2014/AlertSchema">
  <ns2:alert appliance-id="002590867AAA" id="4790" name="malware-object"
severity="majr" uuid="b435583b-1c23-4a80-b893-203245073ed4" ack="no"
product="Email MPS" vlan="0" malicious="yes" sc-version="866.106">
    <ns2:explanation>
      <ns2:malware-detected>
        <ns2:malware name="Malware.Binary">
          <ns2:md5sum>5e747bddd6a759b0a591ab4bb3b5254b</ns2:md5sum>

          <ns2:sha256>cfbb1006d9e6c2660b4876fecef9789c1a3ac0c807181277a2778c5
9d9b8675f</ns2:sha256>
        </ns2:malware>
      </ns2:malware-detected>
    </ns2:explanation>
    <ns2:src>
      <ns2:smtp-mail-from>testuser1@aedev.com</ns2:smtp-mail-from>
    </ns2:src>
    <ns2:alert-url>https://test39-ex.eng.fireeye.com/emps/eanalysis?e_
id=5116&amp;type=attch</ns2:alert-url>
    <ns2:action>blocked</ns2:action>
    <ns2:occurred>2019-05-14T20:53:44.722Z</ns2:occurred>
    <ns2:dst>
      <ns2:smtp-to>testuser2@aedev.com</ns2:smtp-to>
    </ns2:dst>
    <ns2:smtp-message>
      <ns2:subject>Test Email</ns2:subject>
    </ns2:smtp-message>
  </ns2:alert>
</alerts>
```

cURL Code Sample: Alert Details

The following code sample can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSkH --no-progress-bar
https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/alerts/alert/4790 -X 'GET' --header
"X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx" -H 'Accept:
application/xml' -i
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.

- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This option allows you to specify a custom header with the `--header` switch.
- `--no-progress-bar`—This option suppresses the cURL download progress bar, which can interfere with the request.
- `https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/alerts/alert/4790`—The alert acknowledgment request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance. Replace `4790` with the infection ID or alert UUID of interest.
- `-X 'GET'`—This option specifies using the GET method.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header provides the API-Token that was returned during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token value in the code sample with the token value received in the response to your authentication request.

  By default, the `X-FeApi-Token` times out after 15 minutes of inactivity.

- `-H 'Accept: application/xml'`—This header specifies that the server's response body is expected to be in XML format.
- `-i`—This option returns the HTTP header in the response.

Results

This code sample returns the details of alert 4790. The response is in XML.

Alert Acknowledgment Request

You can use the alert acknowledgment request to confirm that you have reviewed the alert so that it is no longer listed in the Web UI. To acknowledge a single alert, send the following HTTP POST request URL, headers, and body:

```
POST https://<cm_address>/wsapis/v1.2.0/alerts/alert/[<alert_ID>|<UUID>]
```

```
POST https://<cm_address>/wsapis/v2.0.0/alerts/alert/<UUID>
```

Availability

This command is available on the following appliances:

- Central Management

Required headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
Accept: application/json
Content-Type: application/json
```

Body:

```
annotation: [Annotation]
alertType: [Alert-Type]
```

Parameters

- *cm_address*—The IP address of the Central Management appliance running the Web Services API.
- *alert_ID*— (v1.2.0 only) The infection ID. You must also specify the Alert-Type.
- *UUID*—The universally unique identifier (UUID) for the alert.
- schema_compatibility—(v2.0.0 only) Produce XML and JSON content compatible with the upgraded schema. `true` is the only accepted value. Omit this option if you are using an older schema and do not want schema compatibility. If using this option, you must use UUID for the alert.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- Client-Token—(Optional) This client token is provided by FireEye. For more information about the client token, contact your sales representative.

Example Request Using the Infection ID

```
POST https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/alerts/alert/1234
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
Accept: application/json
Content-Type: application/json
```

Body:

```
{
   "annotation" : "<string>"
   "alertType" : "<string>"
}
```

Request body fields:

- `annotation`—You must specify a comment, such as "Discovered on December 1".
- `alertType`—If you use the infection ID for the alert_ID, you must specify the type of alert, such as `"Malware Object"`.

Example Request Using the Alert UUID

```
POST https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/alerts/alert/7d9e9883-37e4-
4802-a364-08e3fd6efb6a?schema_compatibility=true
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

Body:

```
{
   "annotation" : "Discovered by John Doe"
}
```

Alert Acknowledgment Response

After the alert acknowledgment request is received, your appliance validates the API token and sends a response code and message.

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
```

Response Fields

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 4xx—Request unsuccessful because unknown or invalid fields were included in the input.
  - 5xx—Request unsuccessful because the server encountered a problem.

- Response Message—A standard HTML response message.
  - Empty—Request successful.
  - Invalid Client Request—Request unsuccessful because unknown or invalid fields were included in the input.
  - Server encountered a problem...retry later—Request unsuccessful because the server encountered a problem.
- Date—Standard HTML date format.

Example Response

```
HTTP/1.1 200 OK
Date: Thu, 23 Nov 2017 13:39:42 GMT
```

cURL Code Sample: Alert Acknowledgment

The following code sample can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSkH --no-progress-bar
https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/alerts/alert/2133 -X 'POST' --data-
binary '{"annotation":"Discovered on December 1","alertType":"Malware
Callback"}' --header "X-FeApi-Token:
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx" -H 'Accept:
application/json' -H 'Content-Type: application/json' -i
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This option allows you to specify a custom header with the `--header` switch.

- `--no-progress-bar`—This option suppresses the cURL download progress bar, which can interfere with the request.
- `https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/alerts/alert/2133`—The alert acknowledgment request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance. Replace `1234` with the infection ID or alert UUID of interest.
- `-X 'POST'`—This option specifies using the POST method.
- `--data-binary '{"annotation":"Discovered on December 1","alertType":"Malware Callback"}'`—This option specifies the comment added to the acknowledged alert and the type of alert.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header provides the API-Token that was returned during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token value in the code sample with the token value received in the response to your authentication request.

  By default, the `X-FeApi-Token` times out after 15 minutes of inactivity.

- `-H 'Accept: application/json'`—This header specifies that the server's response body is expected to be in JSON format.
- `-H 'Content-Type: application/json'`—This header specifies that the request body is in JSON format.
- `-i`—This option returns the HTTP header in the response.

Results

This code sample returns a response code and message to indicate if your request was successful.

Artifacts

List Artifacts Data by ID

Downloads malware artifacts data for the specified alert ID as a zip file.

```
GET https://<address>/wsapis/v1.2.0/artifacts/<alert_type>/<alert_id>
```

Availability

This command is available on the following appliances:

- Central Management
- Malware Analysis
- Email Security — Server Edition
- File Protect
- Network Security

Required Header:

```
X-FeApi-Token: [API-Token]
```

Request Content-type:

```
application/octet-stream
```

Parameters

- address—This is the IP address of the appliance running the Web Services API.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- alert_type—Type of alert, for example, `malwareobject`.
- alert_id—ID of the alert.

Example Request

```
GET https://<address>/wsapis/v1.2.0/artifacts/<alert_type>/<alert_id>
```

List Artifacts Data by ID Response

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 500—Request unsuccessful because the server encountered a problem.

- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Internal Server Error—Request unsuccessful because the server encountered a problem.

cURL Code Sample: List Artifacts Data by ID

The following code sample can be copied and executed from any command-line interface that includes the cURL library.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSk --header "X-FeApi-Token: IHAT75KulvFZ2fz7NqMJRIRRCmNYQFuXXX=" --
header "Accept:application/octet-stream"
"https://xxx.xxx.xxx.xxx/wsapis/v1.2.0/artifacts/malwareobject/1" -o file.zip
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `https://xxx.xxx.xxx.xxx/wsapis/v1.2.0/artifacts/malwareobject/1}`—The fetch request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.
- `-o file.zip`—This option specifies the name of the output file.

Results

The specified alert's metadata is returned as a zip file called `file.zip`. It contains files which have details of malware artifacts as well as a screen capture video file.

List Artifacts Data by UUID

Downloads malware artifacts data for the specified UUID as a zip file.

`GET https://<address>/wsapis/{v1.2.0|v2.0.0}/artifacts/<uuid>`

Availability

This command is available on the following appliances:

- Central Management
- Malware Analysis
- Email Security — Server Edition
- File Protect
- Network Security

Required Header:

`X-FeApi-Token: [API-Token]`

Request Content-type:

- `application/octet-stream` (v1.2.0)
- `application/zip` (v2.0.0)

Options

- *`address`*—This is the IP address of the appliance running the Web Services API.
- *`uuid`*—Universally unique ID of the alert.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.

Example Request

`GET https://<address>/wsapis/v2.0.0/artifacts/<uuid>`

List Artifacts Data by UUID Response

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 500—Request unsuccessful because the server encountered a problem.

- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Internal Server Error—Request unsuccessful because the server encountered a problem.

cURL Code Sample: List Artifacts Data by UUID

The following code sample can be copied and executed from any command-line interface that includes the cURL library.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSk --header "FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxx=" --header
"Accept:application/zip"
https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/artifacts/dce3d3d0-c362-4780-8c16-
cc44ab776XXX -o file.zip
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/artifacts/dce3d3d0-c362-4780-8c16-cc44ab776XXX`—The fetch request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.
- `-o file.zip`—This option specifies the name of the output file.

Results

The specified alert's data is returned as a zip file called `file.zip`. It contains files which have details of malware artifacts as well as a screen capture video file.

List Artifacts Metadata by ID

Gets malware artifacts metadata for the specified alert ID.

`GET https://<address>/wsapis/v1.2.0/artifacts/<alert_type>/<alert_id>/meta`

Availability

This command is available on the following appliances:

- Central Management
- Malware Analysis
- Email Security — Server Edition
- File Protect
- Network Security

Required Header:

`X-FeApi-Token: [API-Token]`

Request Content-type:

- `application/xml`
- `application/json`

Parameters

- *`address`*—This is the IP address of the appliance running the Web Services API.
- *`API-Token`*—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- *`alert_type`*—Type of alert, for example, `malwareobject`.
- *`alert_id`*—ID of the alert.

Example Request

`GET https://<address>/wsapis/v1.2.0/artifacts/<alert_type>/<alert_id>/meta`

List Artifacts Metadata by ID Response

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 500—Request unsuccessful because the server encountered a problem.

- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Internal Server Error—Request unsuccessful because the server encountered a problem.

Metadata in XML:

```
<artifactsMetaData>
  <artifactsInfoList>
    <artifactsInfo>
      <artifactName>1.malware</artifactName>
      <artifactSize>26.19 KB</artifactSize>
      <artifactType>malware</artifactType>
    </artifactsInfo>
    <artifactsInfo>
      <artifactName>M1-1-2017-08-01-215227.pvna.pcap</artifactName>
      <artifactSize>109.67 KB</artifactSize>
      <artifactType>pcap</artifactType>
    </artifactsInfo>
    <artifactsInfo>
      <artifactName>M1-1-2017-08-01-215227.flv</artifactName>
      <artifactSize>1414.70 KB</artifactSize>
      <artifactType>flv</artifactType>
    </artifactsInfo>
  </artifactsInfoList>
  <alertId>1</alertId>
  <alertType>Malware Object</alertType>
  <appliance>0025904E22AC</appliance>
  <applianceId>0025904E22AC</applianceId>
  <version>MAS (MAS) 8.1.0.394276</version>
</artifactsMetaData>
```

Metadata in JSON:

```
{
  "artifactsInfoList":[
    {
      "artifactType":"original_email",
      "artifactName":"429PgJ5HCRzY18vp",
       "artifactSize":"3950"
    },
    {
      "artifactType":"archived_object",
      "artifactName":"4567.malware",
      "artifactSize":"1982"
    },
    {
      "artifactType":"vm_capture",
      "artifactName":"M4528-128-2018-09-12-144413.pvna.pcap",
      "artifactSize":"4228"
    },
    {
      "artifactType":"vm_capture",
      "artifactName":"M4528-129-2018-09-12-144413.pvna.pcap",
      "artifactSize":"1048"
    }
  ]
}
```

cURL Code Sample: List Artifacts Metadata by ID

The following code sample can be copied and executed from any command-line interface that includes the cURL library.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSk --header "X-FeApi-Token: IHAT75KulvFZ2fz7NqMJRIRRCmNYQFXXX=" --
header "Accept:application/json"
"https://xxx.xxx.xxx.xxx/wsapis/v1.2.0/artifacts/malwareobject/1/meta"
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `https://xxx.xxx.xxx.xxx/wsapis/v1.2.0/artifacts/malwareobject/1/meta`—The fetch request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.

Results

The specified alert's metadata is returned in JSON.

List Artifacts Metadata by UUID

Gets malware artifacts metadata for the specified UUID.

`GET https://<address>/wsapis/{v1.2.0|v2.0.0}/artifacts/<uuid>/meta`

For v1.2.0, the schema for alerts is different than for notifications. For v2.0.0, schema compatibility is available but not enforced.

Availability

This command is available on the following appliances:

- Central Management
- Malware Analysis
- Email Security — Server Edition
- File Protect
- Network Security

Required Header:

`X-FeApi-Token: [API-Token]`

Request Content-type:

- `application/xml` (v1.2.0)
- `application/json` (v1.2.0 and v2.0.0)

Parameters

- address—This is the IP address of the appliance running the Web Services API.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- uuid—Universally unique ID of the alert.

Options

`schema_compatibility`—(Boolean) Specify schema compatibility for alerts and notifications. Optional.

Example Request

```
GET https://<address>/wsapis/v2.0.0/artifacts/0cbf1657-a031-48de-9139-
3ad65404cd25/meta
```

List Artifacts Metadata by UUID Response


```
{
  "artifactsInfoList":[
    {
      "artifactType":"video_clip",
      "artifactName":"M1-1-2018-02-02-094512.flv",
      "artifactSize":"1944577"
    },
    {
      "artifactType":"vm_capture",
      "artifactName":"M1-1-2018-02-02-094512.pvna.pcap",
      "artifactSize":"7032"
    },
    {
      "artifactType":"archived_object",
      "artifactName":"1.malware",
      "artifactSize":"640554"
    }
  ]
}
```


- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 500—Request unsuccessful because the server encountered a problem.
- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Internal Server Error—Request unsuccessful because the server encountered a problem.

cURL Code Sample: List Artifacts Metadata by UUID

The following code sample can be copied and executed from any command-line interface that includes the cURL library.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSk --header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxx=" --header
"Accept:application/json"
https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/artifacts/dce3d3d0-c362-4780-8c16-
cc44ab77623b/meta
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.

- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxx="`—This custom header includes the API-Token that was returned by your appliance during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token in the sample with the token received in the response to your authentication request.
- `--header "Accept:application/json"`—Specifies JSON output.
- `https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/artifacts/dce3d3d0-c362-4780-8c16-cc44ab77623b/meta`—The fetch request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.

Results

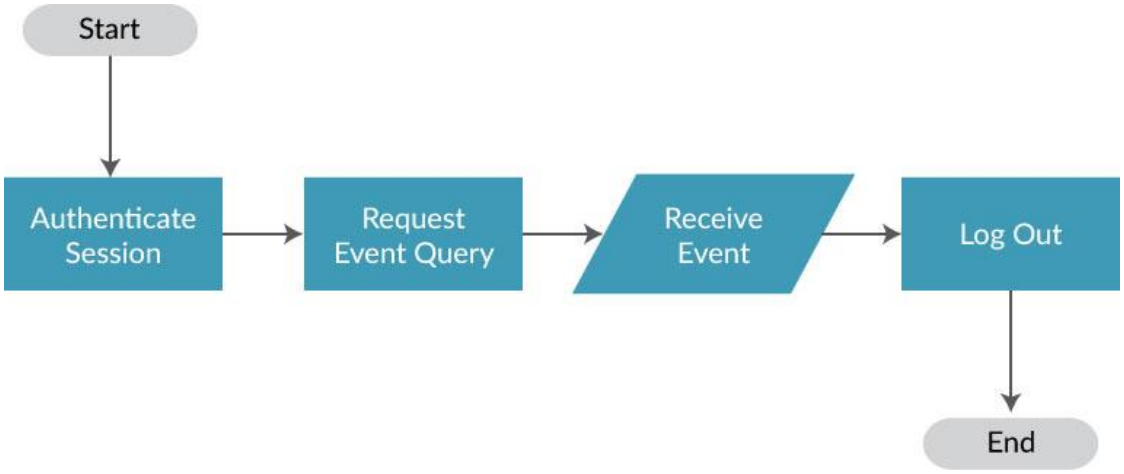
The specified alert's metadata is returned in JSON.

Events

The event request uses the HTTP GET method to retrieve Multi-Vector Virtual Execution (MVX) correlated Intrusion Prevention System (IPS) event data from the Network Security appliance managed by your Central Management appliance. The responses to your event request can be formatted in either JSON or XML.

You must have an IPS-enabled appliance to be able to retrieve IPS event data.

The following flow chart shows how to issue a basic event request:



Responses are limited to 200 events. This limit cannot be changed. If there are more entries than 200, only 200 entries will be returned.

By default, requests are limited to a 12-hour duration. You can specify the duration using the `duration` option.

Event Request

Requests information about existing events using an HTTP GET request. You can also apply filters to requests.

```
GET https://<cm_address>/wsapis/{v1.2.0|v2.0.0}/events?<filters>
```

Availability

This command is available on the following appliances:

- Central Management
- Network Security

Required headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
Accept: [Content-Type]
```

Parameters

- address—The IP address of the FireEye appliance running the Web Services API.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- Client-Token—(Optional) This client token is provided by FireEye. For more information about the client token, contact your sales representative.
- Content-Type—(Optional) You can request responses in two formats:
  - `application/xml`—(Default) If content type is not specified, events are delivered in the XML format.
  - `application/json`—Specify this option to receive events in JSON format.

The JSON output uses the pretty-print format, which includes line breaks between values.

Filters

Use the filters in the following table to limit your request.

Filter	Description
duration	Specifies the time interval to search. This filter is used with the end_time filter. If the duration is not specified, the system defaults to duration=12_hours, end_time=*current_time* Syntax: duration=time_interval • 1_hour • 2_hours • 6_hours • 12_hours • 24_hours • 48_hours Example: duration=1_hour&end_time=2015-01-24T16:30:00.000-07:00
end_time	Specifies the end time of the search. This filter is used with the duration filter. If the end_time is specified but not the duration, the system defaults to duration=12_hours, ending at the specified end_time. Syntax: end_time=YYYY-MM-DDTHH:mm:ss.sss-OH:om • YYYY—Year (1900 and later) • MM—Month (01-12) • DD—Day (01-31) • HH—Hour (01-24) • mm—Minutes (01-59) • ss.sss—Seconds (01-59.999) • OH:om—Time offset from UTC Example: duration=1_hour&end_time=2015-01-24T16:30:00.000-07:00
event_type	The type of event. The value must be set to Ips%20Event. Example: event_type=Ips%20Event
mvx_correlated_only	Boolean. Specifies whether to include all IPS events or MVX-correlated events only. Default: false. Example: mvx_correlated_only=true

Example Request with No Filtering

In this example, the search's duration filter is set to 12_hours (default), the end_time filter is set to the current time (default), and all IPS events will be returned.

```
GET https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/events?mvx_correlated_
only=false
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

Example Request with Filtering

This example specifies the event type, end time, and duration.

```
GET https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/events?duration=48_hours&end_
time=2015-05-23T01:08:04.000-00:00&event_type=Ips%20Event'
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

Event Response

After the event request is received, your appliance validates the API-Token and returns the requested data.

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
Content-Type: [Content-Type]
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Response Fields

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 400—Request unsuccessful because the filter value was invalid.
  - 500—Request unsuccessful because the server encountered a problem.
- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Bad Request—Request unsuccessful because the filter value was invalid.
  - Internal Server Error—Request unsuccessful because the server encountered a problem.
- Date—Standard HTML date format.

Example Response (XML)

```
HTTP/1.1 200 OK
Date: Fri, 20 Sep 2015 08:00:00 GMT
```

Body:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<eventsResponse>
   <eventType>Ips Events</eventType>
   <events>
       <event>
          <actionTaken>1</actionTaken>
          <attackMode>server</attackMode>
          <dstIp>xx.xx.xx.xx</dstIp>
          <dstMac>00:00:50:40:00:44</dstMac>
          <dstPort>34352</dstPort>
          <eventId>982377</eventId>
          <interfaceId>3</interfaceId>
          <occurred>2015-10-06T14:03:22-07:00</occurred>
          <protocol>6</protocol>
          <ruleName>MySQL XML Functions Scalar XPath Denial of Service</ruleName>
          <sensorId>7</sensorId>
          <severity>7</severity>
          <signatureIden>85302536</signatureIden>
          <signatureMatchCnt>1</signatureMatchCnt>
          <signatureRev>4</signatureRev>
          <srcIp>xxx.x.xxx.xxx</srcIp>
          <srcMac>00:00:00:50:40:55</srcMac>
          <srcPort>3306</srcPort>
          <vlan>0</vlan>
          <vmVerified>true</vmVerified>
       </event>
...,
...,
...,
       <event>
          <actionTaken>33</actionTaken>
          <attackMode>client</attackMode>
          <dstIp>xx.xxx.xxx.xxx</dstIp>
          <dstMac>00:50:56:f7:db:db</dstMac>
          <dstPort>80</dstPort>
          <eventId>982380</eventId>
          <interfaceId>3</interfaceId>
          <occurred>2015-10-06T14:32:17-07:00</occurred>
          <protocol>6</protocol>
          <ruleName>Windows Executable Download As Image File</ruleName>
          <sensorId>7</sensorId>
          <severity>7</severity>
           <signatureIden>85305176</signatureIden>
          <signatureMatchCnt>1</signatureMatchCnt>
          <signatureRev>19</signatureRev>
          <srcIp>xxx.xxx.xxx.xxx</srcIp>
          <srcMac>00:0c:29:81:69:4f</srcMac>
          <srcPort>1174</srcPort>
          <vlan>0</vlan>
          <vmVerified>true</vmVerified>
       </event>
   </events>
</eventsResponse>
```

Example Response Including All IPS Events (JSON)

```
{
  "eventType":"Ips Events",
  "events":[
```

```
{
  "eventId":11,
  "occurred":"2018-11-01T15:43:56-07:00",
  "srcIp":"28.188.24.38",
  "srcPort":1057,
  "dstIp":"85.6.103.48",
  "dstPort":80,
  "vlan":0,
  "signatureMatchCnt":1,
  "signatureIden":85305159,
  "signatureRev":17,
  "severity":7,
  "vmVerified":true,
  "srcMac":"d6:96:0a:84:24:15",
  "dstMac":"00:50:56:e5:3f:c5",
  "ruleName":"Trojan.Ramnit Infected Page Download",
  "sensorId":"raj-nx",
  "cveId":null,
  "actionTaken":33,
  "attackMode":"client",
  "interfaceId":4,
  "protocol":6,
  "incidentId":1989
},
{
  "eventId":12,
  "occurred":"2018-11-01T15:44:20-07:00",
  "srcIp":"59.252.28.97",
  "srcPort":1079,
  "dstIp":"11.41.112.187",
  "dstPort":80,
  "vlan":0,
  "signatureMatchCnt":1,
  "signatureIden":85311177,
  "signatureRev":3,
  "severity":5,
  "vmVerified":true,
  "srcMac":"00:20:18:11:ff:02",
  "dstMac":"02:75:ac:9f:b4:c0",
  "ruleName":"Rig Exploit Kit File Download",
  "sensorId":"raj-nx",
  "cveId":null,
  "actionTaken":33,
  "attackMode":"client",
  "interfaceId":4,
  "protocol":6,
  "incidentId":null
},
{
  "eventId":7,
  "occurred":"2018-11-01T15:39:54-07:00",
  "srcIp":"75.65.20.45",
  "srcPort":49195,
  "dstIp":"20.65.68.181",
  "dstPort":8080,
  "vlan":0,
  "signatureMatchCnt":1,
  "signatureIden":85301264,
  "signatureRev":15,"severity":7,
  "vmVerified":true,
  "srcMac":"00:20:18:11:01:65",
  "dstMac":"00:01:6c:a9:2f:27",
  "ruleName":"Adobe Multiple Products Embedded JBIG2 Stream Buffer
```

```
Overflow",
      "sensorId":"raj-nx",
      "cveId":"cve,CVE-2009-0658",
      "actionTaken":33,
      "attackMode":"client",
      "interfaceId":4,
      "protocol":6,
      "incidentId":null
    }
  ]
}
```

cURL Code Sample: Events

The following code sample can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -G -qgsSkH --no-progress-bar --header "X-FeApi-Token:
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/events --data-urlencode
"duration=48_hours" --data-urlencode "end_time=2015-09-23T01:08:04.000-00:00"
--data-urlencode "event_type=Ips Event"
```

This cURL sample includes the following options:

- `-G`—This option specifies an HTTP GET request.
- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This option allows you to specify a custom header with the `--header` switch.
- `--no-progress-bar`—This option suppresses the cURL download progress bar, which can interfere with the request.

- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header provides the API-Token that was returned during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token value in the code sample with the token value received in the response to your authentication request.

  By default, the `X-FeApi-Token` times out after 15 minutes of inactivity.

- `https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/events`—The event request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.
- `--data-urlencode "duration=48_hours"`—This option specifies the time interval to search.
- `--data-urlencode "end_time=2015-09-23T01:08:04.000-00:00"`—This option specifies the end time of the search.
- `--data-urlencode "event_type=Ips Event"`—This option specifies the type of event.

Results

This code sample returns XML-formatted event data from your appliance. If you do not receive any event data and you did not encounter an error message, check your appliance to see whether any event data is available.

List Event Filters Request

Lists configured and default event filters.

```
GET https://<cm_address>/wsapis/v2.0.0/config/network/eventfilter
```

Availability

This command is available on the following appliances:

- Network Security

Required headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Optional header:

```
Accept: application/json
```

Options

- `type`—`<filter_type>` or `default`. Optional. If the filter is not applied, configured filters for all the protocols will be returned.

Parameters

- address—The IP address of the FireEye appliance running the Web Services API.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- Client-Token—(Optional) This client token is provided by FireEye. For more information about the client token, contact your sales representative.

Example Request

```
GET https://<cm_
address>/wsapis/v2.0.0/config/network/eventfilter?type=default
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

List Event Filters Response

After the event request is received, your appliance validates the API-Token and returns the requested data.

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
```

```
Content-Type: application/json
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Response Fields

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 500—Request unsuccessful because the server encountered a problem.
- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Internal Server Error—Request unsuccessful because the server encountered a problem.
- Date—Standard HTML date format.

Example Response

```
HTTP/1.1 200 OK
Date: Fri, 23 Sep 2018 08:00:00 GMT
```

Body:

```
[
  {
    "filtername": "http",
    "field":"http:url",
    "op_type":"regex",
    "index":2,
    "value":"alexa.com"
  },
  {
    "filtername": "http",
    "field":"http:url",
    "op_type":"regex",
    "index":1,
    "value":"google.com"
  }
]
```

cURL Code Sample: List Event Filters

The following code sample can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

```
curl -X POST -qgsSk --header 'X-FeApi-Token: XXXXXXXXXXXXXX
https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/config/network/eventfilter?type=http
```

This cURL sample includes the following options:

- `-X 'POST'`—This option specifies using the POST method.
- `-q`—This option specifies that the `curlrc` configuration file will not be read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header includes the API-Token that was returned by your appliance during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token in the sample with the token received in the response to your authentication request.
- `--header "Accept: application/json"`—This header specifies that the server's response body is expected to be in JSON format.
- `https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/config/network/eventfilter?type=http`—The event filter request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.

Results

This code sample lists `http` event filters.

Add an Event Filter Request

Creates one or more new event filters.

```
POST https://<cm_address>/wsapis/v2.0.0/config/network/eventfilter/add
```

Availability

This command is available on the following appliances:

- Network Security

Required headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Optional header:

```
Accept: application/json
```

Parameters

- address—The IP address of the FireEye appliance running the Web Services API.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- Client-Token—(Optional) This client token is provided by FireEye. For more information about the client token, contact your sales representative.
- Content-Type—(Optional) Specify this option to receive events in JSON format.

Request body:

Pass the following parameters as the `options` field in the request submission:

```
[
  {
    "filter_name" : "<filter-name1>",
    "field_name" : "<field-1>",
    "field_value" : <value1>
  },
  {
    "filter_name" : "<filter-name2>",
    "field_name" : "<field-2>",
    "field_value" : <value2>
  }
]
```

Example Request

In this example, the search's `duration` filter is set to `12_hours` (default), and the `end_time` filter is set to the current time (default).

```
POST https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/config/network/eventfilter/add
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

Add an Event Filter Response

After the event request is received, your appliance validates the API-Token and returns the requested data.

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
Content-Type: application/json
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Response Fields

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 404—Request unsuccessful because the filter value was invalid.
  - 500—Request unsuccessful because the server encountered a problem.
- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Bad Request—Request unsuccessful because the filter value was invalid.
  - Internal Server Error—Request unsuccessful because the server encountered a problem.
- Date—Standard HTML date format.

Example Response

```
HTTP/1.1 200 OK
Date: Fri, 23 Sep 2018 08:00:00 GMT

{
  "http http.url regex google.com" : "Filter already configured",
  "http http.url regex fireeye.com":"Operation was successful.\n"
}
```

cURL Code Sample: Add an Event Filter

The following code sample can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

```
curl -X POST -qgsSk --header 'X-FeApi-Token: XXXXXXXXXXXXXX' -F 'options=
[{"filter_name":"my_new_filter","field_name":"http:url", "field_value" :
```

```
"example.com"}]'
https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/config/network/eventfilter/add
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` configuration file will not be read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This option allows you to specify a custom header with the `--header` switch.
- `https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/config/network/eventfilter/add`—The event filter request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.
- `-X 'POST'`—This option specifies using the POST method.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header includes the API-Token that was returned by your appliance during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token in the sample with the token received in the response to your authentication request.
- `--header "Accept: application/json"`—This header specifies that the server's response body is expected to be in JSON format.
- `-F 'options=[{"filter_name":"my_new_filter","field_name":"http:url", "field_value" : "example.com"}]'`—This set of options defines the parameters for the new event filters. For more information, see Add an Event Filter Request on page 76.

Results

This code sample creates a new event filter called `my_new_filter`.

Delete an Event Filter Request

Deletes one or more event filters.

```
POST https://<cm_address>/wsapis/v2.0.0/config/network/eventfilter/delete
```

You can only delete configured filters. Default filters cannot be deleted.

Availability

This command is available on the following appliances:

- Network Security

Required headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Optional header:

```
Accept: application/json
```

Parameters

- address—The IP address of the FireEye appliance running the Web Services API.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- Client-Token—(Optional) This client token is provided by FireEye. For more information about the client token, contact your sales representative.
- Content-Type—(Optional) Specify this option to receive events in JSON format.

Request body:

Pass the following parameters as the `options` field in the request submission:

```
[
  {
    "filter_name" : "<filter-name1>",
    "field_name" : "<field-1>",
    "field_value" : <value1>
  },
  {
    "filter_name" : "<filter-name2>",
    "field_name" : "<field-2>",
    "field_value" : <value2>
  }
]
```

Example Request

```
POST https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/config/network/eventfilter/delete
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

Delete an Event Filter Response

After the event request is received, your appliance validates the API-Token and returns the requested data.

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
Content-Type: application/json
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Response Fields

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 404—Request unsuccessful because the filter value was invalid.
  - 500—Request unsuccessful because the server encountered a problem.
- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Bad Request—Request unsuccessful because the filter value was invalid.
  - Internal Server Error—Request unsuccessful because the server encountered a problem.
- Date—Standard HTML date format.

Example Response

```
HTTP/1.1 200 OK
Date: Fri, 23 Feb 2018 08:00:00 GMT
{
  "http http.url regex alexa.com" : "Filter Not found" ,
  "http http.url regex fireeye.com":"Operation was successful.\n"
}
```

cURL Code Sample: Delete an Event Filter

The following code sample can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

```
curl -X POST -qgsSk --header 'X-FeApi-Token: XXXXXXXXXXXXXX' -F 'options=
[{"filter_name":"my_new_filter","field_name":"http:url", "field_value" :
```

```
"example.com"}]'
https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/config/network/eventfilter/delete
```

This cURL sample includes the following options:

- `-X 'POST'`—This option specifies using the POST method.
- `-q`—This option specifies that the `curlrc` configuration file will not be read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/config/network/eventfilter/delete`—The event filter request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header includes the API-Token that was returned by your appliance during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token in the sample with the token received in the response to your authentication request.
- `--header "Accept: application/json"`—This header specifies that the server's response body is expected to be in JSON format.
- `-F 'options=[{"filter_name":"my_new_filter","field_name":"http:url", "field_value" : "example.com"}]'`—This set of options defines which event filters should be deleted. For more information, see Delete an Event Filter Request on page 79.

Results

This code sample deletes the specified event filters.

List Protocols Request

Lists protocols and the supported fields for each protocol.

```
GET https://<cm_address>/wsapis/v2.0.0/config/network/eventfilter/protocols
```

Availability

This command is available on the following appliances:

- Network Security

Required headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Optional header:

```
Accept: application/json
```

Parameters

- address—The IP address of the FireEye appliance running the Web Services API.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- Client-Token—(Optional) This client token is provided by FireEye. For more information about the client token, contact your sales representative.
- Content-Type—(Optional) Specify this option to receive events in JSON format.

Example Request

```
GET https://<cm_address>/wsapis/v2.0.0/config/network/eventfilter/protocols
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

List Protocols Response

After the event request is received, your appliance validates the API-Token and returns the requested data.

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
Content-Type: application/json
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Response Fields

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 500—Request unsuccessful because the server encountered a problem.
- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Internal Server Error—Request unsuccessful because the server encountered a problem.
- Date—Standard HTML date format.

Example Response

```
HTTP/1.1 200 OK
Date: Fri, 23 Sep 2018 08:00:00 GMT
{
  "dns": [
    "event_type",
    "src_ip",
    "src_port",
    "dest_ip",
    "dest_port",
    "proto",
    "dns.type",
    "dns.id",
    "dns.rrname",
    "dns.rrtype",
    "dns.tx_id",
    "dns.rcode",
    "dns.ttl",
    "dns.rdata"
  ],
  "http": [
    "event_type",
    "src_ip",
    "src_port",
    "dest_ip",
    "dest_port",
    "proto",
    "tx_id",
    "http.hostname",
    "http.url",
    "http.http_user_agent",
    "http.xff",
    "http.http_content_type",
    "http.http_refer",
    "http.http_method",
    "http.protocol",
    "http.status",
    "http.redirect",
    "http.length"
  ]
}
```

cURL Code Sample: List Protocols

The following code sample can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

```
curl -X GET -qgsSk --header 'X-FeApi-Token: XXXXXXXXXXXXXX
https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/config/network/eventfilter/protocols
```

This cURL sample includes the following options:

- `-X 'GET'`—This option specifies using the GET method.
- `-q`—This option specifies that the `curlrc` configuration file will not be read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header includes the API-Token that was returned by your appliance during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token in the sample with the token received in the response to your authentication request.
- `https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/config/network/eventfilter/protocols`—The event filter request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.

Results

This code sample lists protocols and their supported fields.

Email Quarantine Management

Use the following APIs to search and download quarantined emails:

- List Quarantined Emails on the next page
  `GET https://<address>/wsapis/v2.0.0/emailmgmt/quarantine`
- Release Quarantined Emails on page 89
  `POST https://<address>/wsapis/v2.0.0/emailmgmt/quarantine/release`
- Delete Quarantined Emails on page 92
  `POST https://<address>/wsapis/v2.0.0/emailmgmt/quarantine/delete`
- Download Quarantined Email on page 95
  `GET https://<address>/wsapis/v2.0.0/emailmgmt/quarantine/<queue_id>`

List Quarantined Emails

Lists quarantined emails.

```
GET https://<address>/wsapis/v2.0.0/emailmgmt/quarantine
```

Availability

This command is available on the following appliances:

- Central Management
- Email Security — Server Edition

Required Header:

```
X-FeApi-Token: [API-Token]
```

Options

- address—This is the IP address of the appliance running the Web Services API.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.

Parameters

- `start_time`—(YYYY-MM-DD'T'HH:MM:SS.SSS-HHMM) `end_time`—(YYYY-MM-DD'T'HH:MM:SS.SSS-HHMM). These filters are optional, but if used, they must be passed as a pair. Default: `now()` - 24 hours.
- `from:<string>`—The email sender. Optional.
- `subject:<string>`—The email subject. Must be URL encoded. Optional.
- `limit`—Number of records to return (default: 10000). Optional.
- `appliance_id`—Optional.

Example Request

```
GET https://<address>/wsapis/v2.0.0/emailmgmt/quarantine
```

List Quarantined Emails Response

- Response Code—A standard HTML response code.
  - 200—Request successful.

Email Security — Server Edition:

```
[
  {
```

```
    "email_uuid" : "69a7e8f2-4bdd-460a-be8f-891ece18a10f",
    "queue_id"   : "AAABBBCCCDD",
    "message_id" : "XXXYYYZZZPPP",
    "timestamp"  : "2019-07-04T00:00:00.000-00:00",
    "from"       : "user@domain.com",
    "subject"    : "send me all your money"
  }
]
```

Central Management:

```
[
  {
    "email_uuid": "eb306a5a-e84d-4f39-b166-8f2c687efcdd",
    "queue_id": "45T1YF48LBz16vPQ",
    "message_id": "retroactive_detection_E-74805_vgtnl@automation.com",
    "completed_at": "2019-06-18T21:35:18",
    "from": "test@testretro.com",
    "subject": "E-74805 - Test mail",
    "appliance_id": "00259085F550
  }
]
```

cURL Code Sample: List Quarantined Emails

The following code sample can be copied and executed from any command-line interface that includes the cURL library.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSk --header "X-FeApi-Token: IHAT75KulvFZ2fz7NqMJRIRRCmNYQFuXXX="
"https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/emailmgmt/quarantine"
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.

- `https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/emailmgmt/quarantine`—The quarantine request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.

Results

This example returns a JSON array of email quarantine objects.

Release Quarantined Emails

Releases and deletes quarantined emails.

`POST https://<address>/wsapis/v2.0.0/emailmgmt/quarantine/release`

Availability

This command is available on the following appliances:

- Central Management
- Email Security — Server Edition

Required Header:

`X-FeApi-Token: [API-Token]`

Request Content-type:

`application/json`

Options

- address—This is the IP address of the appliance running the Web Services API.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.

Parameters

`sensorName`—(Central Management only) The sensor display name.

Request body:

```
{
  "queue_ids" : ["<qid1>", "<qid4>", "<qid3>", "<qid1>"]
}
```

A maximum of 100 entries is supported.

Example Request

Email Security — Server Edition:

`POST https://<address>/wsapis/v2.0.0/emailmgmt/quarantine/release`

Central Management:

```
POST
https://<address>/wsapis/v2.0.0/emailmgmt/quarantine/release?sensorName=blade
1-vex3
```

Release Quarantined Emails Response

- Response Code—200
    - Request successful if all queue IDs were successfully released. If partial failure occurs, 200 OK is returned with details of the failure.
- Response Message—Empty body on success.

cURL Code Sample: Release Quarantined Emails

The following code sample can be copied and executed from any command-line interface that includes the cURL library.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSk -X POST --header "X-FeApi-Token:
IHAT75KulvFZ2fz7NqMJRIRRCmNYQFuXXX=" --header "Accept:application/json"
"https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/emailmgmt/quarantine/release" --data '
{"queue_ids": ["463jzF5NOhzShwd"]}'
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-X POST`—This option specifies using the POST method.
- `https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/emailmgmt/quarantine/release`—The quarantine release request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.
- `--data '{"queue_ids": ["463jzF5NOhzShwd"]}'`—Specifies the emails to be released and deleted.

Results

This example releases and deletes the specified email quarantine objects.

Delete Quarantined Emails

Deletes quarantined emails.

```
POST https://<address>/wsapis/v2.0.0/emailmgmt/quarantine/delete
```

Availability

This command is available on the following appliances:

- Central Management
- Email Security — Server Edition

Required Header:

```
X-FeApi-Token: [API-Token]
```

Request Content-type:

```
application/json
```

Options

- address—This is the IP address of the appliance running the Web Services API.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.

Parameters

- `sensorName`—(Central Management only) The sensor from which to delete email.

Request body:

```
{
  "queue_ids" : ["<qid1>", "<qid4>", "<qid3>", "<qid1>"]
}
```

A maximum of 100 entries is supported.

Example Request

Email Security — Server Edition:

```
POST https://<address>/wsapis/v2.0.0/emailmgmt/quarantine/delete
```

Central Management:

```
POST
https://<address>/wsapis/v2.0.0/emailmgmt/quarantine/delete?sensorName=blade
1-vex3
```

Delete Quarantined Emails Response

- Response Code—200
  - Request successful if all queue IDs were successfully deleted. If partial failure occurs, 200 OK is returned with details of the failure.
- Response Message—Empty body on success.

cURL Code Sample: Delete Quarantined Emails

The following code sample can be copied and executed from any command-line interface that includes the cURL library.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSk -X POST --header "X-FeApi-Token:
IHAT75KulvFZ2fz7NqMJRIRRCmNYQFuXXX=" --header "Accept:application/json"
"https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/emailmgmt/quarantine/delete " --data '
{"queue_ids": ["463jzF5NOhzShwd"]}'
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-X POST`—This option specifies using the POST method.
- `https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/emailmgmt/quarantine/delete`—The quarantine delete request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.
- `--data '{"queue_ids": ["463jzF5NOhzShwd"]}'`—Specifies the emails to be deleted.

Results

This example deletes the specified email quarantine objects.

Download Quarantined Email

Downloads a quarantined email as a zip file.

```
GET https://<address>/wsapis/v2.0.0/emailmgmt/quarantine/<queue_id>
```

Availability

This command is available on the following appliances:

- Central Management
- Email Security — Server Edition

Required Header:

```
X-FeApi-Token: [API-Token]
```

Request Content-type:

```
application/octet-stream
```

Options

- address—This is the IP address of the appliance running the Web Services API.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.

Parameters

- *queue_id*—The ID of the quarantined email.
- sensorName—(Central Management only) The sensor display name.

Example Request

Email Security — Server Edition:

```
GET https://<address>/wsapis/v2.0.0/emailmgmt/quarantine/45vCN64lNOz2m2QB
```

Central Management:

```
GET
https://<address>/wsapis/v2.0.0/emailmgmt/quarantine/45vCN64lNOz2m2QB?sensorN
ame=blade1-vex3
```

Download Quarantined Email Response

- Response Code—A standard HTML response code.
    - 200—Request successful.

- Response Message—A standard HTML response message.
    - OK—Request successful.

cURL Code Sample: Download Quarantined Email

The following code sample can be copied and executed from any command-line interface that includes the cURL library.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSk --header "X-FeApi-Token: IHAT75KulvFZ2fz7NqMJRIRRCmNYQFuXXX=" --
header "Accept:application/octet-stream"
"https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/emailmgmt/quarantine/45vCN64lN0z2m2QB"
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/emailmgmt/quarantine/45vCN64lN0z2m2QB`—The quarantine download URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance, and 45vCN64lN0z2m2QB with

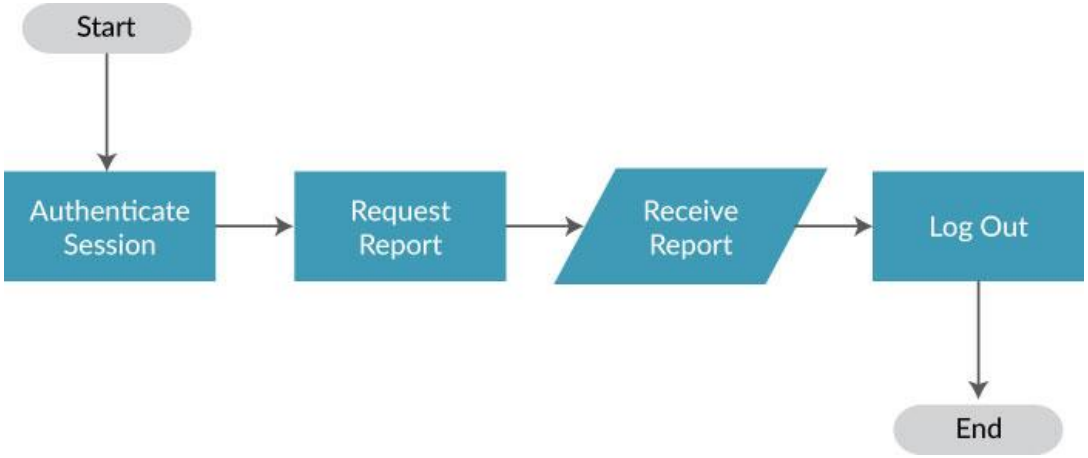
Results

This example downloads a zip file of the specified email quarantine object.

Reports and Statistics

The report request returns requested reports. You can specify the type of report and use filters to limit your search.

The following flow chart shows how to make a basic report request:



Report by Time Request

Returns reports on selected alerts by specifying a `time_frame` value or a `start_time` and `end_time` of the search range.

Availability

This command is available on the following appliances:

- Central Management
- Malware Analysis
- Email Security — Server Edition
- File Protect
- Network Security

The following syntax can be used to request a report:

Report Request Using a Specified Time Frame

```
GET https://<cm_address>/wsapis/v1.2.0/reports/report?report_
type=<reportName>&type=<reportType>
&time_frame=<timeFrame>&limit=<limit>&interface=<interface>
```

Header:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Report Request Using a Start and End Time

```
https://<cm_address>/wsapis/v1.2.0/reports/report?report_
type=<reportName>&time_frame=between &type=<reportType>&start_time=<start_
time>&end_time=<end_time>
```

Header:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

If you do not include a time frame or start and end time with your request, the system defaults to the pastWeek time frame.

Parameters

- cm_address—This is the IP address of the Central Management appliance running the Web Services API.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.

- Client-Token (Optional)— This client token is provided by FireEye. For more information about the client token, contact your sales representative.
- Report Type—Specify the report type using the `report_type` option and the output type using the `type` option:

Report	report_type	type	Series
FX Series Executive Summary	fmpsFileExecutiveSummary	pdf	FX
Email Antivirus Report	empsEmailAVReport	csv	EX
Email Activity Report	empsEmailActivity	pdf	EX
Email Executive Summary	empsEmailExecutiveSummary	pdf	EX
Email Hourly Status	empsEmailHourlyStat	csv	EX
Website Callback Server Report	mpsCallBackServer	csv	NX
Website Executive Summary	mpsExecutiveSummary	pdf	NX
Website Infected Host Trends	mpsInfectedHostsTrend	csv	NX
Website Malware Activity	mpsMalwareActivity	csv or pdf	NX
Website Antivirus Report	mpsWebAVReport	csv	NX
IPS Executive Summary Report	ipsExecutiveSummary	csv or pdf	NX
IPS Top N Attacks Report	ipsTopNAttack	csv or pdf	NX
IPS Top N Attackers Report	ipsTopNAttacker	csv or pdf	NX
IPS Top N Victims Report	ipsTopNVictim	csv or pdf	NX
IPS Top N MVX-Correlated Report	ipsTopNMvxVerified	csv or pdf	NX
Alert Details Report	alertDetailsReport	pdf	NX

Requests for `ipsTopNAttack`, `ipsTopNAttacker`, `ipsTopNVictim`, or `ipsTopNMvxVerified` reports must be used with the `limit` parameter set to either 25, 50, 75, or 100.

You must have an Intrusion Prevention System (IPS)-enabled appliance to be able to generate the IPS reports.

Time Frame (Optional)

Specify a time frame:

Time Frame	Description
`start_time`	Searches between two specified time frames. When specifying a `start_time` value, you must specify both a `start_time` and an `end_time` value. Follow the format: Syntax: `start_time=<start_time>&end_time=<end_time>` Where both the start time and end time follow the format: `start_time="yyyy-MM-ddTHH:mm:ss.SSSXXX"` or `start_time="yyyy-MM-ddTHH:mm:ssXXX"` • yyyy—Year (1900 and later) • MM—Month (01-12) • dd—Day (01-31) • HH—Hour (01-24) • mm—Minutes (01-59) • ss.sss—Seconds (01-59.999) • XX:XX—Time offset from UTC. Example: `start_time="2001-07-04T12:08:56.235-07:00"` or `start_time="2001-07-04T12:08:56.235-07"`
`end_time`	Searches between two specified time frames. When specifying an `end_time` value, you must specify both a `start_time` and an `end_time` value. Follow the format: Syntax: `end_time=<start_time>&end_time=<end_time>` Where both the start time and end time follow the format: `end_time="yyyy-MM-ddTHH:mm:ss.SSSXXX"` or `end_time="yyyy-MM-ddTHH:mm:ssXXX"` • yyyy—Year (1900 and later) • MM—Month (01-12) • dd—Day (01-31) • HH—Hour (01-24) • mm—Minutes (01-59) • ss.sss—Seconds (01-59.999) • XX:XX—Time offset from UTC. Example: `end_time="2001-07-04T12:08:56.235-07:00"` or `end_time="2001-07-04T12:08:56.235-07"`

Time Frame	Description
`pastWeek`	Searches the past week.
`pastMonth`	Searches the past month.
`pastThreeMonth`	Searches the past three months.
`between`	Searches between two times.
`today`	Searches today.
`oneDayAgo`	Searches the past day.
`twoDaysAgo`	Searches the past two days.
`threeDaysAgo`	Searches the past three days.
`fourDaysAgo`	Searches the past four days.
`fiveDaysAgo`	Searches the past five days.
`sixDaysAgo`	Searches the past six days.
`pastHour`	Searches the past hour.
`pastDay`	Searches the past day.

- Limit—This option is required only for IPS "Top N" reports. The `limit` option sets the maximum number (N) of items covered by each report.
- Interface—This option is required only for IPS reports. The `interface` option sets the Internet interface to one of the following values:
  - A
  - B
  - AB

- Infection ID and Infection Type (Optional)—Use the combination of `infection_id` and `infection_type` options to specify a unique alert to describe in the Alert Details Report. If one option is used alone and does not specify a unique alert, an error message is produced. The following infection types are supported:
  - `malware-object`
  - `malware-callback`
  - `infection-match`
  - `domain-match`
  - `web-infection`

  To obtain the infection ID and infection type, submit an alert request.
- ID (Optional)—The `id` option is an alternative to the `infection_id` and `infection_type` options. Specify a unique ID using the internal database unique ID of the alert record.

Example Request

```
https://<cm_address>/wsapis/v1.2.0/reports/
report?report_type=empsEmailAVReport&time_frame=between&type=csv&start_
time="2001-07-04T12:08:56.235-07"&end_time="2001-09-04T12:08:56.235-07"
```

cURL Code Sample: Generating a Report

The following code sample can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSkH --no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/reports/report?report_
type=empsEmailHourlyStat
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.

- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This option allows you to specify a custom header with the `--header` switch.
- `--no-progress-bar`—This option suppresses the cURL download progress bar, which can interfere with the request.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header provides the API-Token that was returned during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token value in the code sample with the token value received in response to your authentication request.

  By default, the `X-FeApi-Token` times out after 15 minutes of inactivity.

- `https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/reports/report?report_type=empsEmailHourlyStat`—The report request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance. The `report_type=empsEmailHourlyStat` will return a `.csv` file.

Results

An Email Hourly Status report in CSV format is returned inline.

cURL Code Sample: Finding the Infection Type and Infection ID

To obtain the infection type and infection ID of an alert, submit an alert request. An alert request returns the infection type and infection ID of all alerts that match your filters.

The following code sample can be copied and executed from any command-line interface that includes the cURL library.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSkH --no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/alerts?duration=1_hour
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This option allows you to specify a custom header with the `--header` switch.
- `--no-progress-bar`—This option suppresses the cURL download progress bar, which can interfere with the request.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header provides the API-Token that was returned during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token value in the code sample with the token value received in the response to your authentication request.

  By default, the `X-FeApi-Token` times out after 15 minutes of inactivity.

- `https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/alerts?duration=1_hour`—The alert request. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance. In this example, the `alerts?duration=1_hour` filter returns alerts that were detected in the previous hour.

Results

The infection type and infection ID of all alerts that match your filters are returned.

Alert ID Response

Look for the line with `alert id="8351" name="malware-object"` in the following example to find the infection ID and the infection type.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<alerts appliance="CMS" version="CMS (CMS) 7.4.0.239904" msg="concise"
xmlns:ns2="http://www.fireeye.com/alert/2013AlertSchema">
<ns2:alert id="8351" name="malware-object" severity="majr" product="Web MPS"
sensor="wmps4">
```

```
        <ns2:explanation>
            <ns2:malware-detected>
                <ns2:malware name="Trojan.Downloader">
                    <ns2:md5sum>2c72f5572741eab4d47afa5d3575b7b8</ns2:md5sum>
                </ns2:malware>
            </ns2:malware-detected>
        </ns2:explanation>
        <ns2:src>
            <ns2:ip>xxx.xxx.xxx.xxx</ns2:ip>
        </ns2:src>
        <ns2:alert-url>https://localhost:8080/botnets/events_for_bot?ma_
id=8351</ns2:alert-url>
        <ns2:action>notified</ns2:action>
        <ns2:occurred>2014-08-06T18:00:44.467Z</ns2:occurred>
        <ns2:dst>
            <ns2:port>123</ns2:port>
            <ns2:ip>xxx.xxx.xxx.xxx</ns2:ip>
        </ns2:dst>
    </ns2:alert>
</alerts>
```

Response Fields

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 400—Request unsuccessful because the filter value was invalid.
  - 500—Request unsuccessful because the server encountered a problem.
- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Bad Request—Request unsuccessful because the filter value was invalid.
  - Internal Server Error—Request unsuccessful because the server encountered a problem.

cURL Code Sample: Generating a Report for a Unique Alert

Use the infection ID and infection type in a report request to get details about a specific alert.

The following code sample can be copied and executed from any command-line interface that includes the cURL library.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSkH --no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
"https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/reports/ report?report_
type=alertDetailsReport&infection_id=8351&infection_type=malware-object"
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This option allows you to specify a custom header with the `--header` switch.
- `--no-progress-bar`—This option suppresses the cURL download progress bar. This progress bar can interfere with the request.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header provides the API-Token that was returned during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token value in the code sample with the token value received in response to your authentication request.

  By default, the `X-FeApi-Token` times out after 15 minutes of inactivity.

- `"https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/reports/report?report_type=alertDetailsReport&infection_id=8351&infection_type=malware-object"`—The report request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance. The generated Alert Details Report will provide details of a malware object with an infection ID of `8351`.

Results

The requested report is returned inline as unformatted data. You need to redirect the output to a PDF file to see a formatted version.

cURL Code Sample: Specifying the Location of the Generated Report

The following code sample can be copied and executed from any command-line interface that includes the cURL library.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSk --no-progress-bar
--header "Accept: application/pdf" --header "X-FeApi-Token:
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
"https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/reports/ report?report_
type=alertDetailsReport&infection_id=6713675&infection_type=malware-object"
-o ./results_pdf/wso.report.6713675.pdf
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `--no-progress-bar`—This option suppresses the cURL download progress bar. This progress bar can interfere with the request.
- `--header "Accept: application/pdf"`—This option specifies a PDF version of the report.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header provides the API-Token that was returned during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token value in the code sample with the token value received in the response to your authentication request.

  By default, the `X-FeApi-Token` times out after 15 minutes of inactivity.

- `"https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/reports/report?report_type=alertDetailsReport&infection_id=6713675&infection_type=malware-object"`—The report request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance. The generated Alert Details Report will provide details of a malware object with an infection ID of `6713675`.
- `-o`—This option redirects the output to a file.
- `./results_pdf/wso.report.6713675.pdf`—This path specifies where the generated report will be saved.

Results

The requested report is saved to the specified path.

Report by ID Request

Returns reports on selected alerts by specifying the alert's `id` or by specifying the `infection_id` and `infection_type`.

Availability

This command is available on the following appliances:

- Central Management
- Malware Analysis
- Email Security — Server Edition
- File Protect
- Network Security

The following syntax can be used to request a report:

Report Request Using the ID

```
GET https://<address>/wsapis/v1.2.0/reports/report?report_
type=alertDetailsReport&id=<ID>
```

Header:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Report Request Using the Infection ID and Infection Type

```
GET https://<address>/wsapis/v1.2.0/reports/report?report_
type=alertDetailsReport&infection_id=<infectionID>& infection_
type=<infectionType>
```

Header:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Options

- address—This is the IP address of the appliance running the Web Services API.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- Client-Token (Optional)— This client token is provided by FireEye. For more information about the client token, contact your sales representative.
- Report Type—Specify the report type using the `report_type` option and the output type using the `type` option:

Report	report_type	type
Alert Details Report	alertDetailsReport	pdf

- Infection ID and Infection Type (Optional)—Use the combination of `infection_id` and `infection_type` options to specify a unique alert to describe in the Alert Details Report. If one option is used alone and does not specify a unique alert, an error message is produced. The following infection types are supported:
  - `malware-object`
- ID (Optional)—The `id` option is an alternative to the `infection_id` and `infection_type` options. Specify a unique alert using the internal database unique ID of the alert record.

Example Requests

```
https://<address>/wsapis/v1.2.0/reports/report?report_
type=alertDetailsReport&infection_id=8351&infection_type=malware-object
```

```
https://<address>/wsapis/v1.2.0/reports/report?report_
type=alertDetailsReport&id=1664
```

cURL Code Sample: Finding the Infection Type and Infection ID

To obtain the infection type and infection ID of an alert, submit an alert request. An alert request returns the infection type and infection ID of all alerts that match your filters.

The following code sample can be copied and executed from any command-line interface that includes the cURL library.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSkH --no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/reports/report?report_
type=alertDetailsReport&infection_id=8351&infection_type=malware-object
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.

- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This option allows you to specify a custom header with the `--header` switch.
- `--no-progress-bar`—This option suppresses the cURL download progress bar, which can interfere with the request.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header provides the API-Token that was returned during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token value in the code sample with the token value received in the response to your authentication request.

  By default, the `X-FeApi-Token` times out after 15 minutes of inactivity.

- `https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/reports/report?report_type=alertDetailsReport&infection_id=8351&infection_type=malware-object`—The report request. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance. In this example, the `?report_type=alertDetailsReport&infection_id=8351&infection_type=malware-object` filter specifies the infection ID and type.

Results

The infection type and infection ID of all alerts that match your filters are returned.

Alert ID Response

Look for the line with `alert id="8351" name="malware-object"` in the following example to find the infection ID and the infection type.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<alerts appliance="MAS" version="MAS (MAS) 7.7.0.406866" msg="concise"
xmlns:ns2=
"http://www.fireeye.com/alert/2013/AlertSchema">
   <ns2:alert id="8351" name="malware-object" severity="minr" product=MAS">
        <ns2:explanation>
            <ns2:malware-detected>
                <ns2:malware name="Trojan.Downloader">
                    <ns2:md5sum>2c72f5572741eab4d47afa5d3575b7b8</ns2:md5sum>
                </ns2:malware>
            </ns2:malware-detected>
        </ns2:explanation>
        <ns2:src>
            <ns2:ip>xxx.xxx.xxx.xxx</ns2:ip>
```

```
        </ns2:src>
        <ns2:alert-url>https://localhost:8080/botnets/events_for_bot?ma_
id=8351</ns2:alert-url>
        <ns2:action>notified</ns2:action>
        <ns2:occurred>2014-08-06T18:00:44.467Z</ns2:occurred>
        <ns2:dst>
            <ns2:port>123</ns2:port>
            <ns2:ip>xxx.xxx.xxx.xxx</ns2:ip>
        </ns2:dst>
    </ns2:alert>
</alerts>
```

Response Fields

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 400—Request unsuccessful because the filter value was invalid.
  - 500—Request unsuccessful because the server encountered a problem.
- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Bad Request—Request unsuccessful because the filter value was invalid.
  - Internal Server Error—Request unsuccessful because the server encountered a problem.

cURL Code Sample: Generating a Report for a Unique Alert

Use the infection ID and infection type in a report request to get details about a specific alert.

The following code sample can be copied and executed from any command-line interface that includes the cURL library.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSkH --no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
"https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/reports/ report?report_
type=alertDetailsReport&infection_id=8351&infection_type=malware-object"
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.

- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This option allows you to specify a custom header with the `--header` switch.
- `--no-progress-bar`—This option suppresses the cURL download progress bar. This progress bar can interfere with the request.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header provides the API-Token that was returned during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token value in the code sample with the token value received in response to your authentication request.

  By default, the `X-FeApi-Token` times out after 15 minutes of inactivity.

- `"https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/reports/report?report_type=alertDetailsReport&infection_id=8351&infection_type=malware-object"`—The report request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance. The generated Alert Details Report will provide details of a malware object with an infection ID of `8351`.

Results

The requested report is returned inline as unformatted data. You need to redirect the output to a PDF file to see a formatted version.

cURL Code Sample: Specifying the Location of the Generated Report

The following code sample can be copied and executed from any command-line interface that includes the cURL library.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSk --no-progress-bar
--header "Accept: application/pdf" --header "X-FeApi-Token:
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
"https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/reports/ report?report_
```

```
type=alertDetailsReport&infection_id=6713675&infection_type=malware-object"
-o ./results_pdf/wso.report.6713675.pdf
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `--no-progress-bar`—This option suppresses the cURL download progress bar. This progress bar can interfere with the request.
- `--header "Accept: application/pdf"`—This option specifies a PDF version of the report.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header provides the API-Token that was returned during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token value in the code sample with the token value received in the response to your authentication request.

  By default, the `X-FeApi-Token` times out after 15 minutes of inactivity.

- `"https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/reports/report?report_type=alertDetailsReport&infection_id=6713675&infection_type=malware-object"`—The report request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance. The generated Alert Details Report will provide details of a malware object with an infection ID of `6713675`.
- `-o`—This option redirects the output to a file.
- `./results_pdf/wso.report.6713675.pdf`—This path specifies where the generated report will be saved.

Results

The requested report is saved to the specified path.

Statistics Request

Retrieves performance statistics for a specified time range. On Email Security — Server Edition appliances, email statistics are returned. On Network Security appliances, protocol-related statistics are returned. The statistics are fetched locally.

You must have the `api_analyst` or `api_monitor` role.

The WSAPI service must be enabled on the appliance using the `wsapi enable` CLI command. See the *CLI Reference* for more information.

```
GET https://<IP_address>/wsapis/v2.0.0/statistics?start_time=2019-04-
01T03:02:13.552-00:00&end_time=2019-05-22T03:02:13.552-00:00
```

Availability

This command is available on the following appliances:

- Email Security — Server Edition
- Network Security

Required headers:

```
X-FeApi-Token: [API-Token]
```

Options

- IP_address—This is the IP address of the appliance running the Web Services API.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- Client-Token (Optional)— This client token is provided by FireEye. For more information about the client token, contact your sales representative.
- `start_time` and `end_time`—Searches between two specified time frames. Both the start time and end time must be in UTC format: "*yyyy-MM-dd*`T`*HH:mm:ss.SSS-XX:XX*" For example: `start_time="2001-07-04T12:08:56.235-07:00"`
  - `yyyy`—Year (1900 and later)
  - `MM`—Month (01-12)
  - `dd`—Day (01-31)
  - `HH`—Hour (01-24)
  - `mm`—Minutes (01-59)
  - `ss.sss`—Seconds (01-59.999)

  - XX:XX—Time offset from UTC.
- include_submission_stats—(Boolean) Provides statistics on completed, queued, and malicious submissions. Optional.

Usage

Statistics are collected every 10 minutes; it is recommended that you collect statistics up to the last 10 minutes. If you plan to use the statistics API in a script to pull data continuously, it is recommended that:

- start_time should be currentTime – 20 minutes.
- end_time should be currentTime – 10 minutes.
- When the adjusted end time is returned, it should be used as the start time for the next iteration.

For example:

```
GET https://172.16.172.234:443/wsapis/v2.0.0/statistics?start_time=2019-04-
29T22:02:00.000-00:00&end_time=2019-04-29T22:12:55.248-00:00&include_
submission_stats=true
```


```
{
  "applianceStats": {
    "FeExTotalEmailsWithRetroDetection": 0,
    "FeExTotalEmails": 1662,
    "FeExTotalEmailsWithRiskwareMatch": 0,
    "FeExTotalEmailsWithBadUrls": 2,
    "FeExTotalEmailsWithRiskwareBlock": 0,
    "FeExTotalEmailsBypassed": 0,
    "FeExTotalEmailsAnalyzed": 657,
    "FeExTotalBadEmails": 5,
    "FeExTotalEmailBypassAnalysisTimeout": 2,
    "FeExTotalEmailsWithAttachments": 118,
    "FeExTotalEmailsQuarantined": 5,
    "FeExTotalEmailsWithUrls": 582,
    "FeExTotalEmailsWithBadAttachments": 3
  },
  "adjustedEndTime": "2019-04-29T22:12:00",
  "adjustedStartTime": "2019-04-29T22:02:00",
  "currentTime": "2019-04-29T22:22:55.32074"
  "submissionStats": {
    "FeComCompletedSubmissions": {
      "file": 0,
      "url": 0
    },
    "FeComMaliciousSubmissions": {
      "file": 0,
      "url": 0
    },
    "FeComQueuedSubmissions": {
      "file": 102,
      "url": 40
    }
  }
}
```

Use the value of `adjustedEndTime` from the results of the above call as the `start_time` in the following call:

```
GET https://172.16.172.234:443/wsapis/v2.0.0/statistics?start_time=2019-04-29T22:12:00.000-00:00&end_time=2019-04-29T22:22:55.568-00:00
```


```
{
  "applianceStats": {
    "FeExTotalEmailsWithRetroDetection": 0,
    "FeExTotalEmails": 1662,
    "FeExTotalEmailsWithRiskwareMatch": 0,
    "FeExTotalEmailsWithBadUrls": 4,
    "FeExTotalEmailsWithRiskwareBlock": 0,
    "FeExTotalEmailsBypassed": 0,
    "FeExTotalEmailsAnalyzed": 658,
    "FeExTotalBadEmails": 6,
    "FeExTotalEmailBypassAnalysisTimeout": 2,
    "FeExTotalEmailsWithAttachments": 117,
    "FeExTotalEmailsQuarantined": 6,
    "FeExTotalEmailsWithUrls": 581,
    "FeExTotalEmailsWithBadAttachments": 2
  },
  "adjustedEndTime": "2019-04-29T22:22:00",
  "adjustedStartTime": "2019-04-29T22:12:00",
  "currentTime": "2019-04-29T22:32:55.652528"
}
```


Next iteration:

```
GET https://172.16.172.234:443/wsapis/v2.0.0/statistics?start_time=2019-04-29T22:22:00.000-00:00&end_time=2019-04-29T22:32:55.887-00:00
```


```
{
  "applianceStats": {
    "FeExTotalEmailsWithRetroDetection": 0,
    "FeExTotalEmails": 1665,
    "FeExTotalEmailsWithRiskwareMatch": 0,
    "FeExTotalEmailsWithBadUrls": 1,
    "FeExTotalEmailsWithRiskwareBlock": 0,
    "FeExTotalEmailsBypassed": 0,
    "FeExTotalEmailsAnalyzed": 650,
    "FeExTotalBadEmails": 5,
    "FeExTotalEmailBypassAnalysisTimeout": 15,
    "FeExTotalEmailsWithAttachments": 120,
    "FeExTotalEmailsQuarantined": 5,
    "FeExTotalEmailsWithUrls": 583,
    "FeExTotalEmailsWithBadAttachments": 4
  },
  "adjustedEndTime": "2019-04-29T22:32:00",
  "adjustedStartTime": "2019-04-29T22:22:00",
  "currentTime": "2019-04-29T22:42:56.000417"
}
```

Statistics Response

Response Fields

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 400—Invalid inputs
  - 404—Statistics not found
  - 500—Request unsuccessful because the server has encountered a problem; retry later.
  - 503—The WSAPI service was not enabled on the appliance
- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Error trying to process submission—Request unsuccessful because the server has encountered a problem; retry later.
  - Not found
  - Server error
  - Service unavailable
- `currentTime`—The time the request was submitted. All timestamps in the response are in UTC format.
- `adjustedEndTime`—The end timestamp that data was pulled from the DB.
- `adjustedStartTime`—The start timestamp that data was pulled from the DB.

  If the request time range is more than 24 hours ago, the data will be pulled from the hourly rollups. If the time window is within the last 24 hours, the stored procedure will pull the data from min-rollups table.

If the time range is more than 24 hours ago, the adjusted start time and end time will be truncated to the hour. When both the adjusted start time and end time are the same, there will be no measures for those segments.

Example

```
GET https://<IP_address>/wsapis/v2.0.0/statistics?start_time=2019-04-
25T09:00:00.000-00:00&end_time=2019-04-25T09:59:00.000-00:00
```

```
{
  "applianceStats": {
    "FeExTotalEmailsWithRetroDetection": 0,
    "FeExTotalEmails": 0,
    "FeExTotalEmailsWithRiskwareMatch": 0,
    "FeExTotalEmailsWithBadUrls": 0,
```

```
    "FeExTotalEmailsWithRiskwareBlock": 0,
    "FeExTotalEmailsBypassed": 0,
    "FeExTotalEmailsAnalyzed": 0,
    "FeExTotalBadEmails": 0,
    "FeExTotalEmailBypassAnalysisTimeout": 2,
    "FeExTotalEmailsWithAttachments": 0,
    "FeExTotalEmailsQuarantined": 0,
    "FeExTotalEmailsWithUrls": 0,
    "FeExTotalEmailsWithBadAttachments": 0
  },
  "adjustedEndTime": "2019-04-25T09:00:00",
  "adjustedStartTime": "2019-04-25T09:00:00",
  "currentTime": "2019-04-13T22:11:52.475053"
}
```


In the above example, both the adjusted start time and end time are truncated to the same hour: 2019/04/26 09:00:00.

Another example: Using a start time and end time of 04/26/2019 08:59:00 to 04/26/2019 09:59:00, the API returns data for the adjusted start time and end time: 04/26/2019 08:00:00 to 04/26/2019 09:00:00, so the actual results are for almost an hour earlier.

```
GET https://<IP_address>/wsapis/v2.0.0/statistics?start_time=2019-04-
25T08:59:00.000-00:00&end_time=2019-04-25T09:59:00.000-00:00
```


```
{
  "applianceStats": {
    "FeExTotalEmailsWithRetroDetection": 0,
    "FeExTotalEmails": 8079,
    "FeExTotalEmailsWithRiskwareMatch": 0,
    "FeExTotalEmailsWithBadUrls": 6,
    "FeExTotalEmailsWithRiskwareBlock": 0,
    "FeExTotalEmailsBypassed": 0,
    "FeExTotalEmailsAnalyzed": 3150,
    "FeExTotalBadEmails": 21,
    "FeExTotalEmailBypassAnalysisTimeout": 8,
    "FeExTotalEmailsWithAttachments": 575,
    "FeExTotalEmailsQuarantined": 21,
    "FeExTotalEmailsWithUrls": 2825,
    "FeExTotalEmailsWithBadAttachments": 15
  },
  "adjustedEndTime": "2019-04-25T09:00:00",
  "adjustedStartTime": "2019-04-25T08:00:00",
  "currentTime": "2019-04-13T22:15:45.5564"
}
```


Email Security — Server Edition response fields:

- FeExTotalEmails—Number of emails received
- FeExTotalEmailsAnalyzed—Number of emails analyzed by MVX
- FeExTotalBadEmails—Total emails received with malicious contents
- FeExTotalEmailsQuarantined—Number of emails quarantined (emails with riskware-block are included)
- FeExTotalEmailsBypassed—Number of emails bypassed
- FeExTotalEmailBypassAnalysisTimeout—The length of time (in minutes) an email is in analysis.

- FeExTotalEmailsWithAttachments—Number of emails with attachments
- FeExTotalEmailsWithBadAttachments—Number of emails with malicious attachments
- FeExTotalEmailsWithUrls—Number of emails with body URLs
- FeExTotalEmailsWithBadUrls—Number of emails with malicious body URLs
- FeExfTotalEmailsWithRiskwareMatch—Number of emails with riskware match (emails with riskware-block are not included)
- FeExfTotalEmailsWithRiskwareBlock—Number of blocked emails due to riskware
- FeExTotalEmailsWithRetroDetection—Number of emails detected via retroactive detection (this includes all types of retro: FAUDE, remote correlation and object retro detection)

Network Security response fields:

- FeNxTotalBytes—Total number of bytes (in KBs) for the given time range
- FeNxMinBytesRate—Minimum rate (kbps) for the given timeframe, measured every 1 minute
- FeNxMaxBytesRate—Maximum rate (kbps) for the given timeframe, measured every 1 minute
- FeNxTotalHttpBytes—Total number of HTTP bytes (in KBs) for the given time range
- FeNxMinHttpRate—Minimum HTTP byte rate (kbps) for the given timeframe, measured every 1 minute
- FeNxMaxHttpRate—Maximum HTTP byte rate (kbps) for the given timeframe, measured every 1 minute
- FeNxTotalImapBytes—Total number of IMAP bytes (in KBs) for the given time range
- FeNxMinImapRate—Minimum IMAP kbps for the given timeframe
- FeNxMaxImapRate—Maximum IMAP kbps for the given timeframe
- FeNxTotalDnsBytes—Total number of DNS bytes (in KBs) for the given time range
- FeNxMinDnsRate—Minimum UDP kbps for the given timeframe
- FeNxMaxDnsRate—Maximum DNS kbps for the given timeframe
- FeNxTotalIpBytes—Total number of IP bytes (in KBs) for the given time range
- FeNxMinIpRate—Minimum IP kbps for the given timeframe
- FeNxMaxIpRate—Maximum IP kbps for the given timeframe
- FeNxTotalPopBytes—Total number of POP bytes (in KBs) for the given time range
- FeNxMinPopRate—Minimum POP kbps for the given timeframe
- FeNxMaxPopRate—Maximum POP kbps for the given timeframe

- FeNxTotalRpcBytes—Total number of RPC bytes (in KBs) for the given time range
- FeNxMinRpcRate—Minimum RPC kbps for the given timeframe
- FeNxMaxRpcRate—Maximum RPC kbps for the given timeframe
- FeNxTotalSmbBytes—Total number of SMB bytes (in KBs) for the given time range
- FeNxMinSmbRate—Minimum SMB kbps for the given timeframe
- FeNxMaxSmbRate—Maximum SMB kbps for the given timeframe
- FeNxTotalSmtpBytes—Total number of SMTP bytes (in KBs) for the given time range
- FeNxMinSmtpRate—Minimum SMTP kbps for the given timeframe
- FeNxMaxSmtpRate—Maximum SMTP kbps for the given timeframe
- FeNxTotalSshBytes—Total number of SSH bytes (in KBs) for the given time range
- FeNxMinSshRate—Minimum SSH kbps for the given timeframe
- FeNxMaxSshRate—Maximum SSH kbps for the given timeframe
- FeNxTotalTcpBytes—Total number of TCP bytes (in KBs) for the given time range
- FeNxMinTcpRate—Minimum TCP kbps for the given timeframe
- FeNxMaxTcpRate—Maximum TCP kbps for the given timeframe
- FeNxTotalUdpBytes—Total number of UDP bytes (in KBs) for the given time range
- FeNxMinUdpRate—Minimum UDP kbps for the given timeframe
- FeNxMaxUdpRate—Maximum UDP kbps for the given timeframe
- FeNxTotalVlanBytes—Total number of VLAN bytes (in KBs) for the given time range
- FeNxMinVlanRate—Minimum VLAN kbps for the given timeframe
- FeNxMaxVlanRate—Maximum VLAN kbps for the given timeframe
- FeComTotalMalwareObjectAlerts—Total number of Malware Object alerts
- FeComTotalRiskwareObjectAlerts—Total number of Riskware Object alerts
- FeNxTotalMalwareCallbackAlerts—Total number of Malware Callback alerts
- FeNxTotalWebInfectionAlerts—Total number of Web Infection alerts
- FeNxTotalDomainMatchAlerts—Total number of Domain Match alerts
- FeNxTotalInfectionMatchAlerts—Total number of Infection Match alerts
- FeNxTotalRiskwareCallbackAlerts—Total number of Riskware Callback alerts
- FeNxTotalRiskwareInfectionAlerts—Total number of Riskware Infection alerts
- FeNxTotalSmartVisionAlerts—Total number of SmartVision alerts

- FeNxTotalIpsEvents—Total number of IPS events

Example response body—Email Security — Server Edition:

It is possible that a transaction has not been completely processed at the time the API statistics are collected. Because of this, the numbers that you see for a transaction may not be complete if that transaction is being processed. For example:

```
FeExTotalEmails = 4238
FeEXTotalEmailsBypassed= 1840
FeEXTotalEmailsAnalyzed =2138
```

FeEXTotalEmailsBypassed + FeEXTotalEmailsAnalyzed does not equal to 4238 because some emails are still in processed and are not completely analyzed.


```
{
  "applianceStats": {
    "FeExTotalEmailsWithRetroDetection": 1,
    "FeExTotalEmails": 4238,
    "FeExTotalEmailsWithRiskwareMatch": 0,
    "FeExTotalEmailsWithBadUrls": 18,
    "FeExTotalEmailsWithRiskwareBlock": 4,
    "FeExTotalEmailsBypassed": 1840,
    "FeExTotalEmailsAnalyzed": 2138,
    "FeExTotalBadEmails": 18,
    "FeExTotalEmailBypassAnalysisTimeout": 8,
    "FeExTotalEmailsWithAttachments": 332,
    "FeExTotalEmailsQuarantined": 21,
    "FeExTotalEmailsWithUrls": 1978,
    "FeExTotalEmailsWithBadAttachments": 0
  },
  "adjustedEndTime": "2019-04-09T22:10:00",
  "adjustedStartTime": "2019-04-09T22:04:00",
  "currentTime": "2019-04-09T22:21:30.83766"
}
```


Example response body using include_submission_stats=true flag—Network Security:


```
{
  "currentTime": "2019-04-01T02:08:35.089403",
  "adjustedStartTime": "2019-04-01T01:00:00",
  "adjustedEndTime": "2019-04-01T02:08:00",
  "applianceStats": {
    "FeNxMinDnsRate": 0,
    "FeNxTotalPopBytes": 68,
    "FeNxMaxHttpRate": 125.895691,
    "FeNxTotalSmbBytes": 68,
    "FeNxMaxSmbRate": 2.048839,
    "FeNxTotalSshBytes": 68,
    "FeNxMaxVlanRate": 0,
    "FeNxTotalMalwareCallbackAlerts": 106,
    "FeNxMinSshRate": 0,
    "FeNxMaxIpRate": 131.090439,
    "FeNxTotalInfectionMatchAlerts": 11,
    "FeNxMinSmtpRate": 0,
    "FeNxMaxUdpRate": 6.048085,
    "FeNxTotalBytes": 68,
    "FeNxMinVlanRate": 0,
    "FeNxMinUdpRate": 0,
    "FeNxMaxRpcRate": 0.016655,
    "FeNxMinPopRate": 0,
    "FeNxMinTcpRate": 0,
```

```
    "FeNxMinRpcRate": 0,
    "FeNxMinBytesRate": 0,
    "FeNxMaxSmtpRate": 1.865765,
    "FeNxMinSmbRate": 0,
    "FeNxTotalSmtpBytes": 68,
    "FeNxTotalRiskwareCallbackAlerts": 2,
    "FeNxMaxBytesRate": 131.118591,
    "FeNxMinImapRate": 0,
    "FeNxTotalVlanBytes": 68,
    "FeNxMinIpRate": 0,
    "FeNxTotalHttpBytes": 68,
    "FeNxTotalRpcBytes": 68,
    "FeNxMaxDnsRate": 1.01648,
    "FeNxTotalDnsBytes": 68,
    "FeNxMaxImapRate": 0,
    "FeNxMaxPopRate": 0,
    "FeNxTotalUdpBytes": 68,
    "FeNxTotalIpBytes": 68,
    "FeNxMaxSshRate": 0,
    "FeNxTotalDomainMatchAlerts": 12,
    "FeComTotalMalwareObjectAlerts": 21,
    "FeNxMinHttpRate": 0,
    "FeNxTotalImapBytes": 68,
    "FeNxMaxTcpRate": 131.080902,
    "FeNxTotalTcpBytes": 68
  }
  "submissionStats": {
  "FeComCompletedSubmissions": {
    "file": 0,
    "url": 0
  },
  "FeComQueuedSubmissions": {
    "file": 232649,
    "url": 918
  },
  "FeComMaliciousSubmissions": {
    "file": 0,
    "url": 0
  }
}
```


cURL Code Sample: Statistics

The following code sample can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSkH --no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/statistics?start_time=2017-06-
01T03:02:13.552-00:00&end_time=2017-06-02T03:02:13.552-00:00&include_
submission_stats=false
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This option allows you to specify a custom header with the `--header` switch.
- `--no-progress-bar`—This option suppresses the cURL download progress bar, which can interfere with the request.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header provides the API-Token that was returned during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token value in the code sample with the token value received in response to your authentication request.

  By default, the `X-FeApi-Token` times out after 15 minutes of inactivity.

- `https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/statistics?start_time=2017-06-01T03:02:13.552-00:00&end_time=2017-06-02T03:02:13.552-00:00&include_submission_stats=false`—The statistics request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.

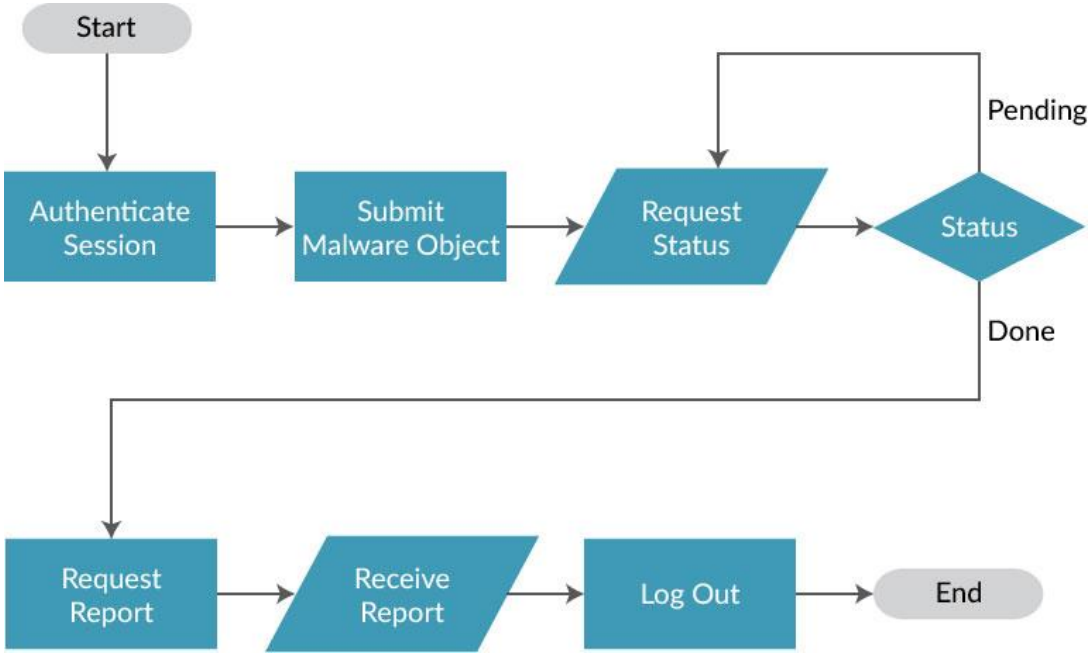
Results

The requested statistics are returned.

Malware Objects

These requests allow you to submit unknown malware objects to an appliance through the Central Management appliance for detailed analysis. You can also submit unknown malware objects or URLs directly to an appliance (version 7.7.0 or higher). Submissions can be a single file, or an archive of multiple files. Individual files within the archive are processed independently. You can also use these requests to review the malware object or URL submissions and the status of each submission.

The following flow chart shows how to submit a malware object. On appliances other that the Central Management, a similar process is used to submit URLs.



For each malware object submitted, you need to include a submission options attachment that includes a JSON-formatted option string and a submission object file that includes the malware object to be tested.

After the malware object is submitted, the appliance returns a submission key. You use this key to determine the status of the submission and to retrieve the completed analysis report.

Submission Key Format on Central Management Appliances

The submission key format is as follows:

xxx_y

- xxx—Submission number
- y—Non-Central Management appliance sensor ID within the Central Management appliance

For example:

245_3

Submission Key Format on Other Appliances

The submission key format is as follows:

xxx

- xxx—Submission number, which can be any length.

For example:

7709

When you submit URLs, the appliance returns a list ID. You use this ID to determine the status of the submission and to retrieve the completed analysis report.

This section covers the following:

The submit file request replaces the submit malware object request.

- Submitting malware objects. For more information, see Submit Malware Object Request on the facing page.
- Submitting files. For more information, see Submit File Request on page 146.
- Submitting URLs. For more information, see Submit URL Request on page 151.

Submit Malware Object Request

Uploads a single file for scanning.

Central Management and Malware Analysis:

```
POST https://<address>/wsapis/[v1.2.0|v2.0.0]/submissions
```

VX Series:

```
POST https://<address>/wsapis/mvx/[v1.2.0|v2.0.0]/submissions
```

Availability

This command is available on the following appliances:

- Central Management
- Malware Analysis
- VX Series

Required headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Request Body:

```
<!--Submission File Set-->
<!--Submit Options Attachment-->
MIME Type application/json
<!--Submit File Attachment-->
MalwareFile1.zip
```

Parameters

- address—The IP address of the appliance running the Web Services API.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- Client-Token—(Optional) This client token is provided by FireEye. For more information about the client token, contact your sales representative.

Submission Options

These options are added as the first part of a multipart MIME attachment to the body of the document. The options should be encoded as a JSON attachment.

Format

Malware Analysis and Central Management:

The JSON-formatted attachment should include the following values:

```
{
  \"application\":\"value\",
```

```
  \"timeout\":\"value\",
  \"priority\":\"value\",
  \"profiles\":\"value\",
  \"analysistype\":\"value\",
  \"force\":\"value\",
  \"prefetch\":\"value\"
}
```

VX Series:

```
{
  \"timeout\":\"value\"
}
```

application	Specifies the ID of the application to be used for the analysis. To determine the available applications for a specific profile, use the Malware Analysis configuration request. For more information, see Configuration Information Request on page 168.  For Malware Analysis appliances (7.7 and higher) and Central Management appliances that manage Malware Analysis appliances (7.7 and higher), setting the application value to -1 allows the Malware Analysis appliance to choose the application for you. For other appliances, setting the application value to 0 allows the Malware Analysis appliance to choose the application for you.
timeout	Sets the analysis timeout (in seconds).
priority	Sets the analysis priority: (default: Normal) • 0—Normal: adds analysis to the bottom of queue. • 1—Urgent: places the analysis at the top of the queue.
profiles	Selects the Malware Analysis profile to use for analysis. To determine the available profiles, use the Malware Analysis configuration request. For more information, see Configuration Information Request on page 168.

`analysistype`	Specifies the analysis mode. • `1`—Live: analyze suspected files live within the Malware Analysis Multi-Vector Virtual Execution (MVX) analysis engine. • `2`—Sandbox: analyze suspected files in a closed, protected environment.
`force`	Specifies whether to perform an analysis on the file even if the file exactly matches an analysis that has already been performed. In most cases, it is not necessary to reanalyze malware. (default: `false`) • `false`—Do not analyze duplicate files. • `true`—Force analysis
`prefetch`	Specifies whether to determine the file target based on an internal determination rather than browsing to the target location. • `0`—No • `1`—Yes. If `analysistype` is set to `2` for sandbox analysis, `prefetch` must be set to 1.
`enable_vnc`	Optional. Specifies whether to enable VNC while making a submission on an Malware Analysis appliance. Default: false. (v2.0.0 only).

properties	Optional. Specifies additional context about the submission on an Malware Analysis appliance. This context is then sent to Guest Images. The following fields are defined: • application_context—Meta information about the application including but not limited to: ◦ arguments ◦ file name ◦ file path ◦ parent path ◦ file owner/creator ◦ permissions • guest_config—Guest images configuration. • artifact_extract_config—Artifact extraction parameters.

Example Request for a Single File (Malware Analysis)

```
POST https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

Request Body:

```
MIME Type application/json

{"analysistype":"1", "priority":"0", "profiles":["win7-sp1"], "force":"true",
"application":"69", "prefetch":"0", "timeout":"500", "enable_vnc":"true",
"application_context": {"file_name":"xyz.pdf"}} MalwareFile1.exe
```

Example Request for Multiple Files Using a Zip File

```
POST https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

Request Body:

```
<!-- Request File Set 1 -->

MIME Type application/json
```

```
{"analysisType":"1", "priority":"0", "profiles":["win7-sp1"],
"force":"true","application":"69", "prefetch":"0", "timeout":"500"}
MalwareFile1.zip
```

Submission Response

After the Central Management appliance receives the submission request, it forwards the submission request to the managed appliance. The managed appliance acknowledges the request and supplies the submission key. The submission key identifies the unique file submitted for analysis.

The submission key is in JSON format.

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
```

Body:

```
[Submission_Key]
```

Response Fields

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 400—Request unsuccessful because the filter value was invalid.
- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Bad Request—Request unsuccessful because the filter value was invalid.
- Date—Standard HTML date format.
- Submission_Key—A JSON-formatted unique submission key that identifies the submitted file for subsequent status and retrieval requests.

Example

```
HTTP/1.1 200 OK
Date: Fri, 17 Nov 2017 08:00:00 GMT
```

Body—Central Management:

```
[{"ID":"3831_5"}]
```

Body—VX Series:

```
{"uuid":"57ee22a2-0ae2-44df-a8a4-a5fef41881cc","brokerId":"0CC47A39D7D0"}
```

Body—Malware Analysis:

```
[
  {
```

```
    "ID":"347",
    "submission_details":"[{"vnc_port":[],"id":347,"uuid":"31d31602-39c0-
4e6a-b60b-b98290f5f609"}]"
  }
]
```

cURL Code Sample: Malware Object Submission

The following code sample can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

Malware Analysis and Central Management:

```
curl -qgsSkH "Content-Type: multipart/form-data"
--no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
-F "filename=@cygdrive/c/tmp/test.txt"
-F "options={\"application\":\"2\",\"timeout\":\"500\",\"priority\":\"0\",
  \"profiles\":[\"win7-sp1\"],\"analysistype\":\"1\",\"force\":\"true\",
  \"prefetch\":\"0\", \"properties\":{\"application_context\":{\"file_
name\":\"xyz.pdf\"}}}"
https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions
```

VX Series only:

```
curl -qgsSkH "Content-Type: multipart/form-data"
--no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
-F "filename=@cygdrive/c/tmp/test.txt"
-F "options={\"timeout\":\"500\"}"
https://xxx.xxx.xxx.xxx:443/wsapis/mvx/v2.0.0/submissions
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This option allows you to specify a custom header with the `--header` switch.

- `Content-Type: multipart/form-data`—This option encodes the data as a multipart form.
- `--no-progress-bar`—This option suppresses the cURL download progress bar, which can interfere with the request.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header includes the API-Token that was returned by your appliance during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token in the sample with the token received in the response to your authentication request.
- `-F "filename=@cygdrive/c/tmp/test.txt`—This option includes the `test.txt` file as an attachment to the message body.

  This example assumes you are using a Windows PC and referencing the following file name and location: `C:/tmp/test.txt`. The file location `cygdrive/c/tmp/test.txt` is the Cygwin-defined POSIX-equivalent location and file.

- `-F "options={\"timeout\":\"500\"}"`—This option defines the submission parameters for the first file. For more information, see Submission Options on page 127.
- `https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions`—The submission request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.
- VX Series: `https://xxx.xxx.xxx.xxx:443/wsapis/mvx/v2.0.0/submissions`—The submission request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.

Results

The requested submission returns a submission key. This key is used to retrieve status and test results.

Submission Results Request

Returns a malware file analysis report in XML format.

Central Management and Malware Analysis:

```
GET https://<address>/wsapis/[v1.2.0|v2.0.0]/submissions/results/[Submission_
Key]
```

VX Series:

```
GET https://<address>/wsapis/mvx/[v1.2.0|v2.0.0]/submissions/result/
[Submission_Key]
```

By default, the results will be in concise mode with just the basic information. If you want more details, use the `info_level=normal` or `info_level=extended` option:

```
GET https://<address>/wsapis/[v1.2.0|v2.0.0]/submissions/results/[Submission_
Key]?info_level=normal
```

```
GET https://<address>/wsapis/[v1.2.0|v2.0.0]/submissions/results/[Submission_
Key]?info_level=extended
```

Availability

This command is available on the following appliances:

- Central Management
- Malware Analysis
- VX Series

Required headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Options

- address—The IP address of the appliance running the Web Services API.
- Submission_Key—Provided by your appliance during the submission process, this key identifies the unique file submitted for analysis.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- Client-Token—(Optional) This client token is provided by FireEye. For more information about the client token, contact your sales representative.

Example Request

Central Management:

```
GET https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions/results/3831_5
```

Other appliances:

```
GET https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/submissions/results/7709
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

Results Response

After the submission results request is received, the appliance forwards the malware object data back to the remote server.

If you make a results request before the analysis is complete, you will receive a response with no analysis data.

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
```

Body:

```
[Result Data]
```

Response Fields

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 401—Request unsuccessful due to incorrect session token.
  - 404—Request unsuccessful due to incorrect submission key.
- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Unauthorized—Request unsuccessful due to incorrect session token.
  - Not Found—Request unsuccessful due to incorrect submission key.
- Date—Standard HTML date format.
- Results Data—The analysis data of the submitted malware object.

Example

```
HTTP/1.1 200 OK
Date: Wed, 8 Aug 2018 03:39:00 GMT
```

Body—Central Management:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<alerts appliance="CMS" version="CMS (CMS) 8.3.0.774206" msg="concise"
xmlns="http://www.fireeye.com/alert/2014/AlertSchema">
  <alert appliance-id="00239085164A" id="19542" root-infection="11161"
sensor-ip="172.16.xxx.50" name="web-infection" severity="majr" product="Web
MPS" sensor="praveen-nx" vlan="0" malicious="yes">
```

```
    <explanation>
      <malware-detected>
        <malware name="Malware.Binary.url" original-infection-id="11161"
original-infection-type="web-infection" original-infection-
url="https://172.16.240.11/botnets/events_for_bot?ma_id=11161"/>
      </malware-detected>
    </explanation>
    <src>
      <ip>196.188.xxx.237</ip>
      <port>1174</port>
    </src>
    <alert-url>https://jijo-cms1.eng.fireeye.com/event_stream/events_for_
bot?inc_id=19542</alert-url>
    <action>notified</action>
    <occurred>2018-07-26T22:27:56.899Z</occurred>
    <dst>
      <mac>00:00:00:00:00:00</mac>
      <port>80</port>
      <ip>79.182.xxx.188</ip>
    </dst>
  </alert>
</alerts>
```

Body—Malware Analysis:

```
<alerts appliance="MAS" version="MAS (MAS) 8.2.0.764951" msg="concise"
xmlns="http://www.fireeye.com/alert/2014/AlertSchema">
  <alert appliance-id="0025904E22AC" id="481" name="malware-object"
severity="majr" product="MAS" vlan="0" malicious="yes">
    <explanation>
      <malware-detected>
        <malware name="Pdf.Exploit.Dropped-78">
          <md5sum>7a4702a43e781846b74e1ea79b73e639</md5sum>

<sha256>0a4bb590eaf23e959083ea9217272b2e39a85803239f6f0708647d4a271caad6</sha
256>
        </malware>
      </malware-detected>
    </explanation>
  <src/>
  <alert-url>https://saturn-mas.eng.fireeye.com/malware_
analysis/analyses?maid=481</alert-url>
  <action>notified</action>
  <occurred>2018-08-01T19:02:40.968Z</occurred>
  <dst>
    <mac></mac>
  </dst>
  </alert>
</alerts>
```

cURL Code Sample: Submission Results Request

The following code sample can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

Central Management:

```
curl -qgsSkH "Content-Type: multipart/form-data"
--no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions/results/3831_5
```

Malware Analysis:

```
curl -qgsSkH "Content-Type: multipart/form-data"
--no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions/results/415
```

VX Series:

```
curl -qgsSkH "Content-Type: multipart/form-data"
--no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
https://xxx.xxx.xxx.xxx:443/wsapis/mvx/v2.0.0/submissions/result/415
```

This cURL sample performs the following tasks:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This option allows you to specify a custom header with the `--header` switch.
- `Content-Type: multipart/form-data`—This option encodes the data as a multipart form.
- `--no-progress-bar`—This option suppresses the cURL download progress bar, which can interfere with the request.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header includes the API-Token that was returned by your appliance during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token in the sample with the token received in response to your authentication request.

- `https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions/results/3831_5`—(Central Management) The submission request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance. Replace `415_75` with the submission key of interest.
- `https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions/results/415`—(Malware Analysis) The submission request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance. Replace `415` with the submission key of interest.
- `https://xxx.xxx.xxx.xxx:443/wsapis/mvx/v2.0.0/submissions/result/415`—(VX Series) The submission request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance. Replace `415` with the submission key of interest.

By default, the results will be in concise mode with just the basic information. If you want more details, add the `?info_level=normal` or `?info_level=extended` option at the end of the URL.

Results

The requested submission returns an XML-formatted malware analysis report.

Submission Queue Size Request

Gets the total number of running and queued submissions.

```
GET https://<address>/wsapis/v2.0.0/submissions/queueSize
```

Availability

This command is available on the following appliances:

- Malware Analysis

Required headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Parameters

- address—The IP address of the appliance running the Web Services API.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- Client-Token—(Optional) This client token is provided by FireEye. For more information about the client token, contact your sales representative.

Example Request

```
GET https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions/queueSize
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

Submission Queue Size Response

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]

{"queueSize":int}
```

Response Fields

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 401—Request unsuccessful because the session token was incorrect.

- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Unauthorized—Request unsuccessful because the session token was incorrect.
- Date—Standard HTML date format.
- queueSize—Total number of queued and running submissions.

Example

```
HTTP/1.1 200 OK
Date: Fri, 13 Jul 2018 09:00:00 GMT

{"queueSize":1138}
```

cURL Code Sample: Submission Queue Size

The following code samples can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSkH --no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
https://xxx.xxx.xxx.xxx:443/wsapis/mvx/v2.0.0/submissions/queueSize
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This switch allows you to specify a custom header with the `--header` switch.
- `--no-progress-bar`—This option suppresses the cURL download progress bar, which can interfere with the request.

- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header includes the API-Token that was returned by your appliance during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token in the sample with the token received in the response to your authentication request.
- `https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions/queueSize`—The queue size request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.

Results

This example returns the number of submissions.

Submission Status Request

Checks the status of submissions.

Central Management and Malware Analysis:

```
GET https://<address>/wsapis/[v1.2.0|v2.0.0]/submissions/status/<Submission_
Key>
```

VX Series:

```
GET https://<address>/wsapis/mvx/
[v1.2.0|v2.0.0]/submissions/status/<Submission_Key>
```

Availability

This command is available on the following appliances:

- Central Management
- Malware Analysis
- VX Series

Required headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Parameters

- address—The IP address of the appliance running the Web Services API.
- Submission Key—Provided by your appliance during the submission process, this key identifies the unique file submitted for analysis.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- Client-Token—(Optional) This client token is provided by FireEye. For more information about the client token, contact your sales representative.

Example Request

Central Management:

```
GET https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions/status/3831_5
```

Malware Analysis:

```
GET https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions/status/7709
```

VX Series:

```
GET https://xxx.xxx.xxx.xxx:443/wsapis/mvx/v2.0.0/submissions/status/7709
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

Submission Status Response

After the Central Management appliance receives the submission status request, it forwards the submission request to the managed appliance. The managed appliance analyzes the malware object and produces a malware object report. This report can be retrieved using the submission results request.

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
```

Body:

```
[Status Message]
```

Response Fields

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 401—Request unsuccessful because the session token was incorrect.
  - 404—Request unsuccessful because the submission key was incorrect.
- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Unauthorized—Request unsuccessful because the session token was incorrect.
  - Not Found—Request unsuccessful because the submission key was incorrect.
- Date—Standard HTML date format.
- Status Message—Provides the status of the file analysis. The format is either JSON or XML.
  - Submission not found.
  - In Progress.
  - Done.

Examples

```
HTTP/1.1 200 OK
Date: Fri, 17 Nov 2017 08:00:00 GMT
{"submissionStatus":"In Progress"}
```

```
HTTP/1.1 200 OK
Date: Fri, 17 Nov 2017 08:00:00 GMT
{"submissionStatus":"Done"}
```

```
HTTP/1.1 200 OK
Date: Fri, 17 Nov 2017 08:00:00 GMT
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<submissionStatus>
   <submissionStatus>In Progress</submissionStatus>
</submissionStatus>
```

```
HTTP/1.1 200 OK
Date: Fri, 17 Nov 2017 08:00:00 GMT
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<submissionStatus>
  <submissionStatus>Done</submissionStatus>
</submissionStatus>
```

cURL Code Sample: Submission Status

The following code samples can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

Central Management:

```
curl -qgsSkH "Content-Type: multipart/form-data"
--no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions/status/3831_5
```

VX Series:

```
curl -qgsSkH "Content-Type: multipart/form-data"
--no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
https://xxx.xxx.xxx.xxx:443/wsapis/mvx/v2.0.0/submissions/status/415
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.

- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This switch allows you to specify a custom header with the `--header` switch.
- `Content-Type: multipart/form-data`—This option encodes the data as a multipart form.
- `--no-progress-bar`—This option suppresses the cURL download progress bar, which can interfere with the request.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header includes the API-Token that was returned by your appliance during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token in the sample with the token received in the response to your authentication request.
- `https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions/status/3831_5`—(Central Management) The submission request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance. Replace `415_75` with the submission key of interest.
- `https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions/status/415`—(Malware Analysis appliances) The submission request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance. Replace `415` with the submission key of interest.
- `https://xxx.xxx.xxx.xxx:443/wsapis/mvx/v2.0.0/submissions/status/415`—(VX Series appliances) The submission request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance. Replace `415` with the submission key of interest.

Results

The requested submission returns one of two status responses:

- In Progress
- Done

When the status changes from `In Progress` to `Done`, you can then retrieve the submission results.

Submit File Request

```
POST https://<address>/wsapis/[v1.2.0|v2.0.0]/submissions/file
```

Availability

This command is available on the following appliances:

- Central Management
- Malware Analysis
- VX Series

Required headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Body:

```
<!--Submission File Set-->
<!--Submit Options Attachment-->
MIME Type application/json
<!--Submit File Attachment-->
MalwareFile1.zip
```

Parameters

- address—The IP address of the appliance running the Web Services API.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- Client-Token—(Optional) This client token is provided by FireEye. For more information about the client token, contact your sales representative.

Submission Options

These options are added as the first part of a multipart MIME attachment to the body of the document. The options should be encoded as a JSON attachment.

Format

The JSON-formatted attachment should include the following values:

```
{\"application\":\"[value]\", \"timeout\":\"[value]\",
\"priority\":\"[value]\", \"profiles\":[\"value\"],
\"analysistype\":\"[value]\", \"force\":\"[value]\",
\"prefetch\":\"[value]\"}
```

`application`	Specifies the ID of the application to be used for the analysis. To determine the available applications for a specific profile, use the Malware Analysis configuration request. For more information, see Configuration Information Request on page 168. Setting the application value to 0 allows the Malware Analysis appliance to choose the application for you.
`timeout`	Sets the analysis timeout (in seconds).
`priority`	Sets the analysis priority: (default: Normal) • `0`—Normal: adds analysis to the bottom of queue. • `1`—Urgent: places the analysis at the top of the queue.
`profiles`	Selects the Malware Analysis profile to use for analysis. To determine the available profiles, use the Malware Analysis configuration request. For more information, see Configuration Information Request on page 168.
`analysistype`	Specifies the analysis mode. • `1`—Live: analyze suspected files live within the Malware Analysis Multi-Vector Virtual Execution (MVX) analysis engine. • `2`—Sandbox: analyze suspected files in a closed, protected environment.
`force`	Specifies whether to perform an analysis on the file even if the file exactly matches an analysis that has already been performed. In most cases, it is not necessary to reanalyze malware. (default: `false`) • `false`—Do not analyze duplicate files. • `true`—Force analysis

prefetch	Specifies whether to determine the file target based on an internal determination rather than browsing to the target location. • 0—No • 1—Yes

Example Request for a Single File

```
POST https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions/file
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

Request Body:

```
MIME Type application/json
{"analysistype":"1", "priority":"0", "profiles":["win7-sp1"],
"force":"true", "application":"69", "prefetch":"0", "timeout":"500"}

MalwareFile1.exe
```

Example Request for Multiple Files Using a Zip File

```
POST https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions/file
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

Request Body:

```
<!-- Request File Set 1 -->
MIME Type application/json
{"analysisType":"1", "priority":"0", "profiles":["win7-sp1"], "force":"true",
       "application":"69", "prefetch":"0", "timeout":"500"}

MalwareFile1.zip
```

Submission Response

After the submission request is received, the Central Management appliance forwards the submission request to the Malware Analysis appliance. The Malware Analysis appliance acknowledges the request and supplies the submission key. The submission key identifies the unique file submitted for analysis.

The submission key is in JSON.

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
```

Body:

```
[Submission_Key]
```

Response Fields

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 400—Request unsuccessful because the filter value was invalid.
- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Bad Request—Request unsuccessful because the filter value was invalid.
- Date—Standard HTML date format.
- Submission_Key—A JSON-formatted unique submission key that identifies the submitted file for subsequent status and retrieval requests.

Example

```
HTTP/1.1 200 OK
Date: Fri, 17 Nov 2017 08:00:00 GMT
```

Body—Central Management:

```
[{"ID"."3831_5"}]
```

Body—other appliances:

```
[{"ID"."7709"}]
```

cURL Code Sample: File Submission

The following code sample can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSkH "Content-Type: multipart/form-data"
--no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
-F "filename=@test.txt"
-F "options={\"application\":\"2\",\"timeout\":\"500\",\"priority\":\"0\",
  \"profiles\":[\"win7-sp1\"],\"analysistype\":\"1\",\"force\":\"true\",
  \"prefetch\":\"0\"}"
https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions/file
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.

- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This option allows you to specify a custom header with the `--header` switch.
- `Content-Type: multipart/form-data`—This option encodes the data as a multipart form.
- `--no-progress-bar`—This option suppresses the cURL download progress bar, which can interfere with the request.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header includes the API-Token that was returned by your appliance during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token in the sample with the token received in the response to your authentication request.
- `-F "filename=@test.txt`—This option includes the `test.txt` file as an attachment to the message body.
- `-F "options= {\"application\":\"2\",\"timeout\":\"500\",\"priority\":\"0\", \"profiles\":[\"win7-sp1\"],\"analysistype\":\"1\",\"force\":\"true\", \"prefetch\":\"0\"}"`—This set of options defines the submission parameters for the first file. For more information, see Submission Options on page 146.
- `https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions/file`—The submission request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.

Results

The requested submission returns a submission key. This key is used to retrieve status and test results. For example:

```
[{"ID":"3831_5"}]
```

Submit URL Request

```
POST https://<address>/wsapis/[v1.2.0|v2.0.0]/submissions/url
```

Availability

This command is available on the following appliances:

- Central Management
- Malware Analysis

Required headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Body:

```
MIME Type application/json
```

Options

- address—The IP address of the appliance running the Web Services API.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- Client-Token—(Optional) This client token is provided by FireEye. For more information about the client token, contact your sales representative.

Submission Options

These options are added as the first part of a multipart MIME attachment to the body of the document. The options should be encoded as a JSON attachment.

Format

The JSON-formatted attachment should include the following values:

```
{\"timeout\":[value], \"priority\":[value], \"profiles\":[\"value\"],
\"application\":[value], \"force\":[value], \"analysistype\":[value],
\"prefetch\":[value], \"urls\":\"[value]\"}
```

`timeout`	Sets the analysis timeout (in seconds).
`priority`	Sets the analysis priority: (default: Normal) • `0`—Normal: adds analysis to the bottom of queue. • `1`—Urgent: places the analysis at the top of the queue.

`profiles`	Selects the Malware Analysis profile to use for analysis. To determine the available profiles, use the Malware Analysis configuration request. For more information, see Configuration Information Request on page 168.
`application`	Specifies the ID of the application to be used for the analysis. To determine the available applications for a specific profile, use the Malware Analysis configuration request. For more information, see Configuration Information Request on page 168.  Setting the application value to 0 allows the Malware Analysis appliance to choose the application for you.
`force`	Specifies whether to perform an analysis on the URL even if the URL exactly matches an analysis that has already been performed. In most cases, it is not necessary to reanalyze the URLs. (default: `false`) • `false`—Do not analyze duplicate URLs. • `true`—Force analysis
`analysistype`	Specifies the analysis mode. • `1`—Live: analyze suspected URLs live within the Malware Analysis Multi-Vector Virtual Execution (MVX) analysis engine. • `2`—Sandbox: analyze suspected URLs in a closed, protected environment.
`prefetch`	Specifies whether to determine the file target based on an internal determination rather than browsing to the target location. • `0`—No • `1`—Yes
urls	Specifies the URLs to submit for analysis. Separate the URLs with a comma.

Example Request

```
POST https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions/url
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

Request Body:

```
MIME Type application/json
{"timeout":200, "priority":1, "profiles":[ "win7-sp1","winxp-sp3"],
"application":2,"force":true,"analysistype":2,"prefetch":1,
"urls":["http://172.16.225.87/malsust/File_share/treasury65malware/
1134220120630 letter.pdf.xdp", "http://172.16.225.87/malsust/File_share/
treasury65malware/ContagioEncryptedXLS_
D116C745FE94C202934EF49F59D19950.xls"]}
```

Submit URL Response

After the submission request is received, the managed appliance acknowledges the request and supplies the list ID. The list ID identifies the URLs submitted for analysis.

The list ID is in JSON format.

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
```

Body:

```
[List_ID]
```

Response Fields

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 400—Request unsuccessful because the filter value was invalid.
  - 500—Request unsuccessful because the server has encountered a problem; retry later.
- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Invalid Client Request—Request unsuccessful because the filter value was invalid.
  - Error trying to process submission—Request unsuccessful because the server has encountered a problem; retry later.
- Date—Standard HTML date format.

- List_ID—A JSON-formatted unique value that identifies the submitted URLs for subsequent status and retrieval requests.

Example

```
HTTP/1.1 200 OK
Date: Fri, 17 Nov 2017 08:00:00 GMT
```

Body—Central Management:

```
[{"id":"L135_5"}]
```

Body—VX Series:

```
[{"id":"473"}]
```

cURL Code Sample: URL Submission

The following code sample can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -k -H "Content-Type: application/json" --header "X-FeApi-Token:
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx" -d "{\"timeout\":200,
\"priority\":1, \"profiles\":[\"win7-sp1\", \"application\":\"2\",
\"force\":\"true\", \"analysistype\":\"2\", \"prefetch\":1, \"urls\":
[\"http://xxx.xxx.xxx.xxx/stats/flashdata.php\"]}"
"https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions/url"
```

This cURL sample includes the following options:

- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H Content-Type: application/json`—This custom header specifies that the response is in JSON format.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header includes the API-Token that was returned by your appliance during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token in the sample with the token received in the response to your authentication request.

- `-d "{\"timeout\":200, \"priority\":1, \"profiles\":[\"win7-sp1\", \"application\":\"2\", \"force\":\"true\", \"analysistype\":\"2\", \"prefetch\":1, \"urls\": [\"http://xxx.xxx.xxx.xxx/stats/flashdata.php\"]}"`—This set of options defines the submission parameters for the URL being submitted. For more information, see Submission Options on page 151.
- `"https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/submissions/url"`—The submission request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.

Results

Central Management:

```
{"response":[{"id":"L135_5","link":
{"rel":"status","href":"/submissions/status/L135_5"}}]}
```

Managed appliances:

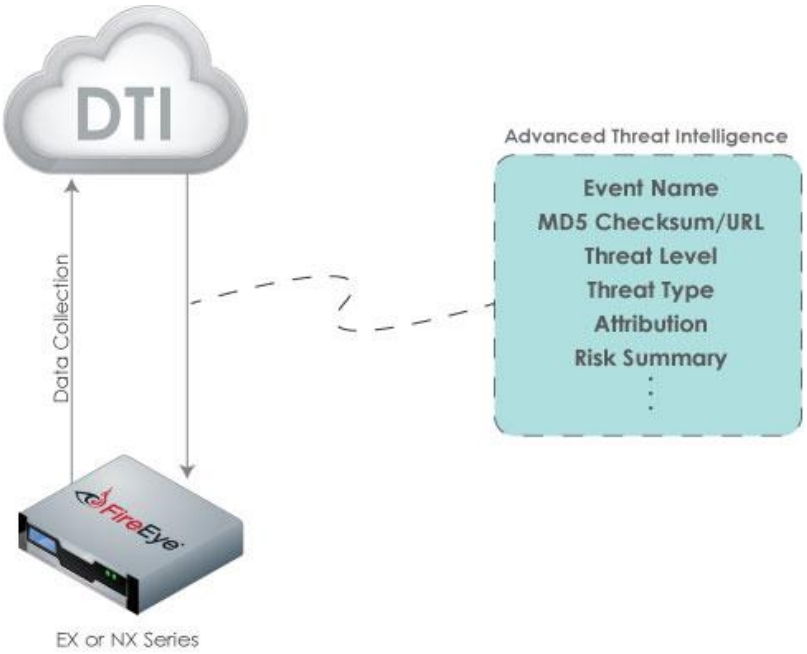
```
{"response":[{"id":"L473","link":
{"rel":"status","href":"/submissions/status/L473"}}]}
```

Retrieving ATI Details

Release 7.5.0 and higher support for ATI requires a two-way sharing CONTENT_UPDATES license with ATI support on the appliance that collects and displays the threat intelligence. Before you install the two-way sharing license and ATI license, you must upgrade to Release 7.5.0 or higher.

Advanced Threat Intelligence (ATI) is a cloud-based data collection and threat intelligence distribution feature that provides actionable information about Multi-Vector Virtual Execution (MVX) engine-verified events on Email Security — Server Edition and Network Security appliances. The threat intelligence tells you who is the threat actor behind an attack, what has been targeted or breached, and (if known) how to mitigate the threat. The FireEye Research Labs team continually uploads the latest threat intelligence to the FireEye Dynamic Threat Intelligence (DTI) cloud. When an MVX-verified event triggers an alert, the appliance queries the DTI server for threat intelligence and stores the additional information in its database. This request retrieves the details of the ATI alert, which includes the threat intelligence.

The following diagram shows the types of threat intelligence that ATI provides for malware object alerts, which are triggered by MD5 checksum matches on Email Security — Server Edition and Network Security appliances. For more information about ATI, see the *Network Security User Guide*.



Alerts Updated with ATI Details Request

Retrieves the IDs of alerts that have been updated with ATI information since a given time.

```
GET https://<address>/wsapis/v1.2.0/ati/<alert_type>?start_time=<from_date>
```

The 2.0.0 version of this API is deprecated in 2019.02.

Headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Availability

This command is available on the following appliances:

- Central Management
- Malware Analysis
- Email Security — Server Edition
- File Protect
- Network Security

Parameters

- *`address`*—The IP address of the appliance running the Web Services API.
- *`API-Token`*—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- *`Client-Token`* (Optional)— This client token is provided by FireEye. For more information about the client token, contact your sales representative.
- *`alert_type`*—Specify the alert type using the `alert_type` option:

Alert Type	alert_type
Malware object	`malwareobject`

- *from-date* (Optional)—Specifies a start time. Use the following format:

  `start_time="yyyy-MM-ddTHH:mm:ss.SSSXXX"` or
  `start_time="yyyy-MM-ddTHH:mm:ssXXX"`

  - `yyyy`—Year (1900 and later)
  - `MM`—Month (01-12)
  - `dd`—Day (01-31)
  - `HH`—Hour (01-24)
  - `mm`—Minutes (01-59)
  - `ss.SSS` or `ss`—Seconds (01-59.999)
  - `XXX` or `XX:XX`—Time offset from UTC.

  For example: `start_time="2018-07-04T12:08:56.235-07:00"` or
  `start_time="2018-07-04T12:08:56.235-07"`

If you do not include a start time with your request, the system defaults to the past 12 hours.

Example Request

```
GET https://xxx.xxx.xxx.xxx:443/wsapis/v1.2.0/ati/malwareobject?start_
time=2018-01-24T16:30:00.000-07:00
```

Alerts Updated with ATI Details Response

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
[Result Data]
```

Response Fields

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 401—Request unsuccessful because the session token was incorrect.
- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Unauthorized—Request unsuccessful because the session token was incorrect.
- Date—Standard HTML date format.
- Results Data—A list of alert IDs.

Example

```
HTTP/1.1 200 OK

Date: Mon, 17 Nov 2018 08:00:00 GMT

{"rawType":"com.fireeye.v110.rest.model.UpdatedInfIdRestModel",
"type":"com.fireeye.v110.rest.model.RestModelBase",
"entity":{"infIdList":[19849450, 14646770,20446085,20532909,20472984,
20264571,20264487,20222885,20214377,20059086,20011544,19961329,
19956463,19954394,19928265,19555190,19555999,15695625,16107393,
17043339,17228593,18519689,18863297,19951882,15695588,20486862,
20515961,20499506,20499229,20496310,20487352,20484363,20482195,
20479242,20477862,20444726,20434507,20432057,20393762,20337219,
20316793,20301927,20295564,20279219,20277420,20274796,20273790,
20260605,2025783

...

}
```

cURL Code Sample: Retrieving a List of Recently Updated Alerts

The following code sample can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSk --no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
--header "Accept: application/json"
"https://xxx.xxx.xxx.xxx/wsapis/v1.2.0/ati/
malwareobject?start_time=2018-11-24T16:30:00.000-07:00"
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.

- `--no-progress-bar`—This option suppresses the cURL download progress bar, which can interfere with the request.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header provides the API-Token that was returned during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token value in the code sample with the token value received in response to your authentication request.

  By default, the `X-FeApi-Token` times out after 15 minutes of inactivity.

- `--header "Accept: application/json"`—This option specifies that the request is in JSON format.
- `https://xxx.xxx.xxx.xxx/wsapis/v1.2.0/ati/malwareobject?start_time=2018-11-24T16:30:00.000-07:00`—The ATI request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance. Replace `malwareobject` with the alert type of interest. Replace `2018-11-24T16:30:00.000-07:00` with the appropriate start time.

Results

A list of alert IDs that have been updated with ATI information since the start time is returned.

ATI Details Request

Retrieves context information for the specified alert.

```
GET https://<address>/wsapis/[v1.2.0|v2.0.0]/ati/<alert_type>/<alert_id>/info
```

Headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Availability

This command is available on the following appliances:

- Central Management
- Malware Analysis
- Email Security — Server Edition
- File Protect
- Network Security

Parameters

- *address*—The IP address of the appliance running the Web Services API.
- *API-Token*—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- *Client-Token* (Optional)— This client token is provided by FireEye. For more information about the client token, contact your sales representative.
- *alert_type*—Specify the alert type using the `alert_type` option:

Alert Type	alert_type
Malware object	`malwareobject`

- *alert_id*—The ID of the alert.

Example Request

```
GET https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/ati/malwareobject/20460153/info
```

ATI Details Response

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
[Result Data]
```

Response Fields

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 401—Request unsuccessful because the session token was incorrect.
  - 404—Request unsuccessful because the alert ID was incorrect.
- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Unauthorized—Request unsuccessful because the session token was incorrect.
  - Not Found—Request unsuccessful because the alert ID was incorrect.
- Date—Standard HTML date format.
- Results Data—The ATI details.

Example

```
HTTP/1.1 200 OK
Date: Mon, 15 Jul 2019 09:00:00 GMT
[
  {
    "extracted_from": "NET_FLOW",
    "observable_type": "ip-address",
    "context_api": {
      "id": "ipaddr-characterization--1a92694f-331a-38c7-8715-4f6ed17ddbc3",
      "type": "ipaddr-characterization",
      "name": "Not_Attributed",
      "analysis_conclusion": "indeterminate"
    },
    "observable_value": "172.16.63.202"
  },
  {
    "extracted_from": "NET_FLOW",
    "observable_type": "ip-address",
    "context_api": {
      "id": "ipaddr-characterization--95f31448-d62d-3471-adc9-0e5ec118ff62",
      "type": "ipaddr-characterization",
      "name": "Not_Attributed",
      "analysis_conclusion": "indeterminate"
    },
    "observable_value": "172.16.63.222"
  }
]
```

cURL Code Sample: Retrieving ATI Details

The following code sample can be copied and executed from any command-line interface that includes the cURL library.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSk --no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
--header "Accept: application/json"
"https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/ati/malwareobject/20460153/info"
```

This cURL sample includes the following options:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `--no-progress-bar`—This option suppresses the cURL download progress bar, which can interfere with the request.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header provides the API-Token that was returned during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token value in the code sample with the token value received in the response to your authentication request.

  By default, the `X-FeApi-Token` times out after 15 minutes of inactivity.

- `--header "Accept: application/json"`—This option specifies that the request is in JSON format.
- `https://xxx.xxx.xxx.xxx/wsapis/v2.0.0/ati/malwareobject/20460153/info`—The ATI request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance. Replace `malwareobject` with the alert type of interest. Replace `20460153` with the alert ID of interest.

Results

The context information for the specified alert ID is returned.

System Information

This section covers the following:

Configuration Information Request

If run on the Central Management appliance, this request returns a list of guest image profiles and applications that are available on each appliance attached to the Central Management appliance. This information may be used to submit malware objects for analysis.

If run on other appliances, this request returns a list of guest image profiles and applications that are available on the appliance that you use to run the Web Services API.

```
GET https://<address>/wsapis/{v1.2.0|v2.0.0}/config
```

Availability

This command is available on the following appliances:

- Central Management
- Malware Analysis
- Email Security — Server Edition
- File Protect
- Network Security

Required headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Parameters

- *address*—The IP address of the appliance running the Web Services API.
- *API-Token*—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- *Client-Token*—(Optional) This client token is provided by FireEye. For more information about the client token, contact your sales representative.

Example Request

```
GET https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/config
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

Configuration Response

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
```

Body:

```
[Configuration Data]
```

Response

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 401—Request unsuccessful due to invalid session token.
- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Unauthorized—Request unsuccessful due to invalid session token.
- Date—Standard HTML date format.

Example

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:sysconfig xmlns:ns2="http://www.fireeye.com/fecmsapi/2015/ConfigSchema">
   <sensors>
       <sensor address="127.0.0.1" id="20" sensor_name="AX">
          <profiles>
               <profile name="winxp-sp3" id="43">
                  <applications>
                       <application id="57" name="Windows Explorer"/>
                       <application id="43" name="MS Word 2003"/>
                       <application id="45" name="MS Excel 2003"/>
                       <application id="47" name="MS PowerPoint 2003"/>
                       <application id="148" name="MS Word 2003 SP2"/>
                       <application id="149" name="MS Excel 2003 SP2"/>
                       <application id="150" name="MS PowerPoint 2003 SP2"/>
                       <application id="151" name="MS Word 2003 SP3"/>
                       <application id="152" name="MS Excel 2003 SP3"/>
                       <application id="153" name="MS PowerPoint 2003 SP3"/>
                       <application id="44" name="MS Word 2007"/>
                       <application id="46" name="MS Excel 2007"/>
                       <application id="48" name="MS PowerPoint 2007"/>
                       <application id="50" name="MS Outlook 2007"/>
                       <application id="154" name="Multiple MS Word X"/>
                       <application id="155" name="Multiple MS Excel X"/>
                       <application id="156" name="Multiple MS PowerPoint X"/>
                       <application id="29" name="Windows Media Player 11.0"/>
                       <application id="21" name="InternetExplorer 7.0"/>
                       <application id="23" name="InternetExplorer 8.0"/>
                       <application id="5" name="InternetExplorer 6.0"/>
                       <application id="157" name="Firefox 19.0"/>
                       <application id="16" name="Firefox 6.0"/>
                       <application id="61" name="Firefox 3.6"/>
```

```
            <application id="89" name="Chrome 26.0"/>
            <application id="80" name="Java JDK JRE 6.16"/>
            <application id="205" name="Java JDK JRE 7.13"/>
            <application id="167" name="Java JDK JRE 6.31"/>
            <application id="164" name="Java JDK JRE 7.0"/>
            <application id="212" name="Java JDK JRE 7.9"/>
            <application id="180" name="Multiple Java JDK JRE"/>
            <application id="15" name="QuickTime Player 7.6"/>
            <application id="26" name="RealPlayer 12.0"/>
            <application id="93" name="VLC Media Player 2.0"/>
            <application id="96" name="Multiple Adobe Reader X"/>
            <application id="32" name="Adobe Reader 9.0"/>
            <application id="30" name="Adobe Reader 7.0"/>
            <application id="31" name="Adobe Reader 8.0"/>
            <application id="85" name="Adobe Reader 9.4"/>
            <application id="8" name="Adobe Reader 10.0"/>
            <application id="94" name="Adobe Reader 10.1"/>
            <application id="95" name="Adobe Reader 11.0"/>
            <application id="97" name="Hancom Office Viewer 2007"/>
            <application id="71" name="RunDLL 1.0"/>
            <application id="84" name="Microsoft Compiled HTML Help"/>
            <application id="86" name="Microsoft Windows Help File"/>
            <application id="98" name="Windows Scripting Host"/>
            <application id="99" name="Command Prompt"/>
      </applications>
   </profile>
   <profile name="win7-sp1" id="65">
      <applications>
            <application id="67" name="Windows Media Player 12.0"/>
            <application id="57" name="Windows Explorer"/>
            <application id="44" name="MS Word 2007"/>
            <application id="46" name="MS Excel 2007"/>
            <application id="48" name="MS PowerPoint 2007"/>
            <application id="201" name="MS Word 2010 SP2"/>
            <application id="202" name="MS Excel 2010 SP2"/>
            <application id="203" name="MS PowerPoint 2010 SP2"/>
            <application id="204" name="MS Outlook 2010 SP2"/>
            <application id="188" name="MS Word 2013"/>
            <application id="183" name="MS Excel 2013"/>
            <application id="189" name="MS PowerPoint 2013"/>
            <application id="154" name="Multiple MS Word X"/>
            <application id="155" name="Multiple MS Excel X"/>
            <application id="156" name="Multiple MS PowerPoint X"/>
            <application id="2" name="InternetExplorer 9.0"/>
            <application id="158" name="InternetExplorer 10.0"/>
            <application id="23" name="InternetExplorer 8.0"/>
            <application id="211" name="Firefox 13.0"/>
            <application id="88" name="Firefox 17.0"/>
            <application id="107" name="Chrome 25.0"/>
            <application id="164" name="Java JDK JRE 7.0"/>
            <application id="178" name="Java JDK JRE 8.0"/>
            <application id="179" name="Java JDK JRE 7.60"/>
            <application id="180" name="Multiple Java JDK JRE"/>
            <application id="111" name="QuickTime Player 7.7"/>
            <application id="112" name="RealPlayer 16.0"/>
            <application id="93" name="VLC Media Player 2.0"/>
            <application id="96" name="Multiple Adobe Reader X"/>
            <application id="95" name="Adobe Reader 11.0"/>
            <application id="32" name="Adobe Reader 9.0"/>
            <application id="85" name="Adobe Reader 9.4"/>
            <application id="8" name="Adobe Reader 10.0"/>
            <application id="94" name="Adobe Reader 10.1"/>
            <application id="118" name="Hancom Office Viewer 2010"/>
```

```
                        <application id="71" name="RunDLL 1.0"/>
                        <application id="84" name="Microsoft Compiled HTML Help"/>
                        <application id="86" name="Microsoft Windows Help File"/>
                        <application id="98" name="Windows Scripting Host"/>
                        <application id="99" name="Command Prompt"/>
                     </applications>
                  </profile>
                  <profile name="win7x64-sp1" id="66">
                     <applications>
                        <application id="67" name="Windows Media Player 12.0"/>
                        <application id="57" name="Windows Explorer"/>
                        <application id="183" name="MS Excel 2013"/>
                        <application id="188" name="MS Word 2013"/>
                        <application id="189" name="MS PowerPoint 2013"/>
                        <application id="184" name="MS Outlook 2013"/>
                        <application id="170" name="InternetExplorer (64-bit) 11.0"/>
                        <application id="169" name="InternetExplorer 11.0"/>
                        <application id="2" name="InternetExplorer 9.0"/>
                        <application id="104" name="InternetExplorer X"/>
                        <application id="159" name="Firefox 26.0"/>
                        <application id="10001" name="Firefox 38.0"/>
                        <application id="185" name="Chrome 36.0"/>
                        <application id="164" name="Java JDK JRE 7.0"/>
                        <application id="178" name="Java JDK JRE 8.0"/>
                        <application id="179" name="Java JDK JRE 7.60"/>
                        <application id="180" name="Multiple Java JDK JRE"/>
                        <application id="111" name="QuickTime Player 7.7"/>
                        <application id="112" name="RealPlayer 16.0"/>
                        <application id="165" name="VLC Media Player 2.1"/>
                        <application id="96" name="Multiple Adobe Reader X"/>
                        <application id="95" name="Adobe Reader 11.0"/>
                        <application id="32" name="Adobe Reader 9.0"/>
                        <application id="85" name="Adobe Reader 9.4"/>
                        <application id="8" name="Adobe Reader 10.0"/>
                        <application id="94" name="Adobe Reader 10.1"/>
                        <application id="71" name="RunDLL 1.0"/>
                        <application id="84" name="Microsoft Compiled HTML Help"/>
                        <application id="86" name="Microsoft Windows Help File"/>
                        <application id="98" name="Windows Scripting Host"/>
                        <application id="99" name="Command Prompt"/>
                     </applications>
                  </profile>
               </profiles>
            </sensor>
      </sensors>
</ns2:sysconfig>
```

cURL Code Sample: Configuration

The following code sample can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSkH --no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/config
```

This cURL sample includes the following:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This option allows you to specify a custom header with the `--header` switch.
- `--no-progress-bar`—This option suppresses the cURL download progress bar, which can interfere with the request.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header returns the API-Token that was provided during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token in the sample with the token value received in the response to your authentication request.

  By default, the X-FeApi-Token times out after 15 minutes of inactivity.

- `https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/config`—The configuration request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.

Results

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns2:sysconfig xmlns:ns2="http://www.fireeye.com/fecmsapi/2013/ConfigSchema">
   <sensors>
       <sensor address="127.0.0.1" id="20" sensor_name="AX">
          <profiles>
               <profile name="winxp-sp3" id="43">
                  <applications>
                       <application id="57" name="Windows Explorer"/>
                       <application id="43" name="MS Word 2003"/>
                       <application id="45" name="MS Excel 2003"/>
                       <application id="47" name="MS PowerPoint 2003"/>
                       <application id="148" name="MS Word 2003 SP2"/>
                       <application id="149" name="MS Excel 2003 SP2"/>
                       <application id="150" name="MS PowerPoint 2003 SP2"/>
```

```
                <application id="151" name="MS Word 2003 SP3"/>
                <application id="152" name="MS Excel 2003 SP3"/>
                <application id="153" name="MS PowerPoint 2003 SP3"/>
                <application id="44" name="MS Word 2007"/>
                <application id="46" name="MS Excel 2007"/>
                <application id="48" name="MS PowerPoint 2007"/>
                <application id="50" name="MS Outlook 2007"/>
                <application id="154" name="Multiple MS Word X"/>
                <application id="155" name="Multiple MS Excel X"/>
                <application id="156" name="Multiple MS PowerPoint X"/>
                <application id="29" name="Windows Media Player 11.0"/>
                <application id="21" name="InternetExplorer 7.0"/>
                <application id="23" name="InternetExplorer 8.0"/>
                <application id="5" name="InternetExplorer 6.0"/>
                <application id="157" name="Firefox 19.0"/>
                <application id="16" name="Firefox 6.0"/>
                <application id="61" name="Firefox 3.6"/>
                <application id="89" name="Chrome 26.0"/>
                <application id="80" name="Java JDK JRE 6.16"/>
                <application id="205" name="Java JDK JRE 7.13"/>
                <application id="167" name="Java JDK JRE 6.31"/>
                <application id="164" name="Java JDK JRE 7.0"/>
                <application id="212" name="Java JDK JRE 7.9"/>
                <application id="180" name="Multiple Java JDK JRE"/>
                <application id="15" name="QuickTime Player 7.6"/>
                <application id="26" name="RealPlayer 12.0"/>
                <application id="93" name="VLC Media Player 2.0"/>
                <application id="96" name="Multiple Adobe Reader X"/>
                <application id="32" name="Adobe Reader 9.0"/>
                <application id="30" name="Adobe Reader 7.0"/>
                <application id="31" name="Adobe Reader 8.0"/>
                <application id="85" name="Adobe Reader 9.4"/>
                <application id="8" name="Adobe Reader 10.0"/>
                <application id="94" name="Adobe Reader 10.1"/>
                <application id="95" name="Adobe Reader 11.0"/>
                <application id="97" name="Hancom Office Viewer 2007"/>
                <application id="71" name="RunDLL 1.0"/>
                <application id="84" name="Microsoft Compiled HTML Help"/>
                <application id="86" name="Microsoft Windows Help File"/>
                <application id="98" name="Windows Scripting Host"/>
                <application id="99" name="Command Prompt"/>
            </applications>
        </profile>
        <profile name="win7-sp1" id="65">
           <applications>
                <application id="67" name="Windows Media Player 12.0"/>
                <application id="57" name="Windows Explorer"/>
                <application id="44" name="MS Word 2007"/>
                <application id="46" name="MS Excel 2007"/>
                <application id="48" name="MS PowerPoint 2007"/>
                <application id="201" name="MS Word 2010 SP2"/>
                <application id="202" name="MS Excel 2010 SP2"/>
                <application id="203" name="MS PowerPoint 2010 SP2"/>
                <application id="204" name="MS Outlook 2010 SP2"/>
                <application id="188" name="MS Word 2013"/>
                <application id="183" name="MS Excel 2013"/>
                <application id="189" name="MS PowerPoint 2013"/>
                <application id="154" name="Multiple MS Word X"/>
                <application id="155" name="Multiple MS Excel X"/>
                <application id="156" name="Multiple MS PowerPoint X"/>
                <application id="2" name="InternetExplorer 9.0"/>
                <application id="158" name="InternetExplorer 10.0"/>
                <application id="23" name="InternetExplorer 8.0"/>
```

```
                        <application id="211" name="Firefox 13.0"/>
                        <application id="88" name="Firefox 17.0"/>
                        <application id="107" name="Chrome 25.0"/>
                        <application id="164" name="Java JDK JRE 7.0"/>
                        <application id="178" name="Java JDK JRE 8.0"/>
                        <application id="179" name="Java JDK JRE 7.60"/>
                        <application id="180" name="Multiple Java JDK JRE"/>
                        <application id="111" name="QuickTime Player 7.7"/>
                        <application id="112" name="RealPlayer 16.0"/>
                        <application id="93" name="VLC Media Player 2.0"/>
                        <application id="96" name="Multiple Adobe Reader X"/>
                        <application id="95" name="Adobe Reader 11.0"/>
                        <application id="32" name="Adobe Reader 9.0"/>
                        <application id="85" name="Adobe Reader 9.4"/>
                        <application id="8" name="Adobe Reader 10.0"/>
                        <application id="94" name="Adobe Reader 10.1"/>
                        <application id="118" name="Hancom Office Viewer 2010"/>
                        <application id="71" name="RunDLL 1.0"/>
                        <application id="84" name="Microsoft Compiled HTML Help"/>
                        <application id="86" name="Microsoft Windows Help File"/>
                        <application id="98" name="Windows Scripting Host"/>
                        <application id="99" name="Command Prompt"/>
                    </applications>
                </profile>
                <profile name="win7x64-sp1" id="66">
                    <applications>
                        <application id="67" name="Windows Media Player 12.0"/>
                        <application id="57" name="Windows Explorer"/>
                        <application id="183" name="MS Excel 2013"/>
                        <application id="188" name="MS Word 2013"/>
                        <application id="189" name="MS PowerPoint 2013"/>
                        <application id="184" name="MS Outlook 2013"/>
                        <application id="170" name="InternetExplorer (64-bit) 11.0"/>
                        <application id="169" name="InternetExplorer 11.0"/>
                        <application id="2" name="InternetExplorer 9.0"/>
                        <application id="104" name="InternetExplorer X"/>
                        <application id="159" name="Firefox 26.0"/>
                        <application id="10001" name="Firefox 38.0"/>
                        <application id="185" name="Chrome 36.0"/>
                        <application id="164" name="Java JDK JRE 7.0"/>
                        <application id="178" name="Java JDK JRE 8.0"/>
                        <application id="179" name="Java JDK JRE 7.60"/>
                        <application id="180" name="Multiple Java JDK JRE"/>
                        <application id="111" name="QuickTime Player 7.7"/>
                        <application id="112" name="RealPlayer 16.0"/>
                        <application id="165" name="VLC Media Player 2.1"/>
                        <application id="96" name="Multiple Adobe Reader X"/>
                        <application id="95" name="Adobe Reader 11.0"/>
                        <application id="32" name="Adobe Reader 9.0"/>
                        <application id="85" name="Adobe Reader 9.4"/>
                        <application id="8" name="Adobe Reader 10.0"/>
                        <application id="94" name="Adobe Reader 10.1"/>
                        <application id="71" name="RunDLL 1.0"/>
                        <application id="84" name="Microsoft Compiled HTML Help"/>
                        <application id="86" name="Microsoft Windows Help File"/>
                        <application id="98" name="Windows Scripting Host"/>
                        <application id="99" name="Command Prompt"/>
                    </applications>
                </profile>
            </profiles>
        </sensor>
    </sensors>
</ns2:sysconfig>
```

System Health Request

Returns the overall system health status.

```
GET https://<address>/wsapis/v2.0.0/health/system
```

Availability

This command is available on the following appliances:

- Central Management
- Malware Analysis
- Email Security — Server Edition
- File Protect
- Network Security
- VX Series

Required headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Optional header:

```
Content-Type: application/json
```

Parameters

None.

Example Request

```
GET https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/health/system
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

System Health Response

Line breaks have been added for readability.

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
{
  "status": "string",
  "timeStamp": "string",
  "appliance": {
    "model": "string",
    "product": "string",
    "dtiMode": "string",
```

```
      "name": "string",
      "domainName": "eng.fireeye.com",
      "systemType": "string",
      "mvxMode": "string",
      "compositeVersion": "appliance n.n.n.nnnnnn #nnnnnn date hh:mm:ss x86_64
  build@vta442:FireEye/nnnnn",
      "edition": "edition",
      "dtiEnabled": "Boolean",
      "version": "appliance n.n.n.nnnnn",
      "components": {
        "upTime": {
          "status": "status",
          "upTimeDuration": "nnd nnh nnm nns",
          "upTimeMilliSeconds": "int",
          "name": "string"
        },
        "eula": {
          "status": "status",
          "accepted": "Boolean",
          "acceptedTime": "string",
          "name": "string"
        },
        "xxxxxLicense": {
          "status": "status",
          "perpetual": "string",
          "name": "string",
          "license": "string"
        },
        "temperature": {
          "status": "status",
          "high": "int",
          "name": "string",
          "currentTemp": "int",
          "low": "int"
        },
        "fann": {
          "status": "status",
          "speed": "int"
        },
        "location": {
          "status": "status",
          "timezone": "xxx/UTC",
          "utc_offset": "int",
          "name": "string",
          "geoLocation": "string"
        },
        "xxxxDisk": {
          "status": "status",
          "deviceName": "/dev/string",
          "bytesTotal": "int",
          "name": "string",
          "bytesUsed": "int",
          "fsType": "string",
          "bytesAvail": "int",
          "bytesFree": "int",
          "percentFree": "int"
        },
        "raid": {
          "status": "status",
          "name": "string"
        },
        "address": {
          "status": "status",
```

```
        "hostName": "string",
        "ipv6Enabled": "Boolean",
        "domainName": ["domain-name"],
        "ipv4": "addr"
      },
      "physicalDiskn": {
        "status": "status",
        "totalBytes": "int",
        "name": "string",
        "selfAssess": "string",
        "diskStatus": "string"
      },
      "usb": {
        "status": "status",
        "mounted": "Boolean",
        "name": "string"
      },
      "powerSupply": {
        "status": "status",
        "name": "string"
      },
      "systemSoftware": {
        "status": "status",
        "currentVersion": "8.3.0",
        "name": "string"
      }
    },
    "timezone": "xxx/UTC",
    "serial": "string",
    "customerId": "string",
    "id": "string"
  },
  "messageType": "string",
  "causeCode": "string",
  "version": "version"
}
```

Response

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 401—Request unsuccessful because the session token was invalid.
- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Unauthorized—Request unsuccessful because the session token was invalid.
- Date—Standard HTML date format.

Example

Line breaks have been added for readability.

Network Securityexample:


```
{
  "status": "warn",
  "timeStamp": "2018/11/06 15:25:35",
  "appliance": {
    "model": "FireEyeNX2500",
    "product": "wMPS",
    "dtiMode": "2Way",
    "name": "nx2500-8-9-40",
    "domainName": "",
    "systemType": "physical",
    "mvxMode": "sensor",
    "compositeVersion": "wmps wMPS (wMPS) 8.2.0.782612 #782612 2018-08-06
22:54:21 x86_64 build@vta448:FireEye/8.2.x",
    "edition": "Classic",
    "dtiEnabled": "true",
    "version": "wMPS (wMPS) 8.2.0.782612",
    "components": {
      "upTime": {
        "status": "ok",
        "upTimeDuration": "13d 0h 15m 27s",
        "upTimeMilliSeconds": "1124127744",
        "name": "upTime"
      },
      "eula": {
        "status": "ok",
        "accepted": "true",
        "acceptedTime": "2018/10/04 16:25:10",
        "name": "eula"
      },
      "physicalDisksda": {
        "status": "ok",
        "totalBytes": "1000204886016",
        "name": "physicalDisksda",
        "selfAssess": "Passed",
        "diskStatus": "Passed
      },
      "atiLicense": {
        "status": "ok",
        "expiresInSeconds": "28715664",
        "name": "atiLicense",
        "license": "ATI",
        "perpetual": "no",
        "expDate": "2019/10/05 00:00:00",
        "expInDays": "332"
      },
      "varDisk": {
        "status": "ok",
        "deviceName": "/dev/sda8",
        "bytesTotal": "33686241280",
        "name": "varDisk",
        "bytesUsed": "491610112",
        "fsType": "ext4",
        "bytesAvail": "31459872768",
        "bytesFree": "33194631168",
        "percentFree": "98"
      },
      "fan1": {
        "status": "ok",
        "speed": "8700"
      },
      "dbDisk": {
```

```
    "status": "ok",
    "deviceName": "/dev/sda9",
    "bytesTotal": "131977056256",
    "name": "dbDisk",
    "bytesUsed": "6444171264",
    "fsType": "ext4",
    "bytesAvail": "118805225472",
    "bytesFree": "125532884992",
    "percentFree": "95"
  },
  "temperature": {
    "status": "ok",
    "high": "75",
    "name": "temperature",
    "currentTemp": "41",
    "low": "5"
  },
  "ipsLicense": {
    "status": "ok",
    "expiresInSeconds": "28715664",
    "name": "ipsLicense",
    "license": "IPS",
    "perpetual": "no",
    "expDate": "2019/10/05 00:00:00",
    "expInDays": "332"
  },
  "systemSoftware": {
    "status": "warn",
    "latestVersion": "8.2.1",
    "currentVersion": "8.2.0",
    "warning": "latest version available",
    "name": "systemSoftware"
  },
  "location": {
    "status": "ok",
    "timezone": "Etc/UTC",
    "utc_offset": "0",
    "name": "location",
    "geoLocation": "unknown"
  },
  "dataDisk": {
    "status": "ok",
    "deviceName": "/dev/sda11",
    "bytesTotal": "730849366016",
    "name": "dataDisk",
    "bytesUsed": "200496271360",
    "fsType": "ext4",
    "bytesAvail": "493204267008",
    "bytesFree": "530353094656",
    "percentFree": "72"
  },
  "rootDisk": {
    "status": "ok",
    "deviceName": "/dev/sda4",
    "bytesTotal": "4160356352",
    "name": "rootDisk",
    "bytesUsed": "2332192768",
    "fsType": "ext4",
    "bytesAvail": "1596641280",
    "bytesFree": "1828163584",
    "percentFree": "43"
  },
  "configDisk": {
```

```
      "status": "ok",
      "deviceName": "/dev/sda7",
      "bytesTotal": "511461376",
      "name": "configDisk",
      "bytesUsed": "6096896",
      "fsType": "ext4",
      "bytesAvail": "474330112",
      "bytesFree": "505364480",
      "percentFree": "98"
    },
    "raid": {
      "status": "ok",
      "name": "raid"
    },
    "avEngineSophosLicense": {
      "status": "ok",
      "expiresInSeconds": "28715664",
      "name": "avEngineSophosLicense",
      "license": "AV_ENGINE_SOPHOS",
      "perpetual": "no",
      "expDate": "2019/10/05 00:00:00",
      "expInDays": "332"
    },
    "securityContent": {
      "status": "ok",
      "lastUploadFailed": "false",
      "name": "securityContent",
      "lastUpdateTime": "2018/11/06 14:53:54",
      "timestamp": "2018-11-06 21:10:00",
      "version": "780.146"
    },
    "fireeyeApplianceLicense": {
      "status": "ok",
      "perpetual": "yes",
      "name": "fireeyeApplianceLicense",
      "license": "FIREEYE_APPLIANCE"
    },
    "address": {
      "status": "ok",
      "hostName": "nx2500-8-9-40",
      "ipv6Enabled": "false",
      "domainName": ["eng.fireeye.com"],
      "ipv4": "10.11.113.155"
    },
    "usb": {
      "status": "ok",
      "mounted": "false",
      "name": "usb"
    },
    "cmsConnection": {
      "status": "ok",
      "name": "cmsConnection",
      "lastFormedAt": "2018/11/06 13:09:21",
      "lastBrokenAt": "2018/11/06 13:04:40",
      "lastAttemptedAt": "2018/11/06 13:09:01",
      "connected": "true",
      "brokenReason": "None",
      "failureReason": "Missing configuration"
    },
   "powerSupply": {
     "status": "ok",
     "name": "powerSupply"
    },
```

```
      "fireeyeSupportLicense": {
        "status": "ok",
        "expiresInSeconds": "28715664",
        "name": "fireeyeSupportLicense",
        "license": "FIREEYE_SUPPORT",
        "perpetual": "no",
        "expDate": "2019/10/05 00:00:00",
        "expInDays": "332"
      },
      "fan3": {
        "status": "ok",
        "speed": "8400"
      },
      "fan2": {
        "status": "ok",
        "speed": "8500"
      },
      "contentUpdatesLicense": {
        "status": "ok",
        "expiresInSeconds": "28715665",
        "name": "contentUpdatesLicense",
        "license": "CONTENT_UPDATES",
        "perpetual": "no",
        "expDate": "2019/10/05 00:00:00",
        "expInDays": "332"
      },
      "wsapiLicense": {
        "status": "ok",
        "expiresInSeconds": "28715664",
        "name": "wsapiLicense",
        "license": "WSAPI",
        "perpetual": "no",
        "expDate": "2019/10/05 00:00:00",
        "expInDays": "332"
      }
    },
    "timezone": "Etc/UTC",
    "serial": "AD1810AQ021",
    "customerId": "90016xxxx",
    "id": "C400ADA07xxx"
  },
  "messageType": "healthUpdate",
  "causeCode": "execution",
  "version": "1.0"
}
```


Central Management example:


```
{
   "status": "ok",
   "timeStamp": "2019/08/30 22:00:59",
   "appliance": {
      "product": "CMS",
      "dtiMode": "2Way",
      "name": "dali",
      "domainName": "eng.fireeye.com",
      "systemType": "physical",
      "mvxMode": "",
      "compositeVersion": "cms CMS (CMS) 8.7.0.870479 #870479 2019-08-28
18:41:43 x86_64 build@vta447:FireEye",
      "edition": "Classic",
      "dtiEnabled": "true",
      "version": "CMS (CMS) 8.7.0.870479",
```

```
"components": {
   "upTime": {
      "status": "ok",
      "upTimeDuration": "1d 2h 57m 57s",
      "upTimeMilliSeconds": "97077680",
      "name": "upTime"
   },
   "eula": {
      "status": "ok",
      "accepted": "true",
      "acceptedTime": "2019/07/12 18:41:24",
      "name": "eula"
   },
   "atiLicense": {
      "status": "ok",
      "expiresInSeconds": "27395941",
      "name": "atiLicense",
      "license": "ATI",
      "perpetual": "no",
      "expDate": "2020/07/13 00:00:00",
      "expInDays": "317"
   },
   "varDisk": {
      "status": "ok",
      "deviceName": "/dev/sda8",
      "bytesTotal": "33686241280",
      "name": "varDisk",
      "bytesUsed": "2278776832",
      "fsType": "ext4",
      "bytesAvail": "29672706048",
      "bytesFree": "31407464448",
      "percentFree": "93"
   },
   "fireeyeSupportLicense": {
      "status": "ok",
      "expiresInSeconds": "27395941",
      "name": "fireeyeSupportLicense",
      "license": "FIREEYE_SUPPORT",
      "perpetual": "no",
      "expDate": "2020/07/13 00:00:00",
      "expInDays": "317"
   },
   "dbDisk": {
      "status": "ok",
      "deviceName": "/dev/sda9",
      "bytesTotal": "3096215502848",
      "name": "dbDisk",
      "bytesUsed": "14837161984",
      "fsType": "ext4",
      "bytesAvail": "2924075167744",
      "bytesFree": "3081378340864",
      "percentFree": "99"
   },
   "temperature": {
      "status": "ok",
      "high": "80",
      "name": "temperature",
      "currentTemp": "21",
      "low": "0"
   },
   "systemSoftware": {
      "status": "ok",
      "currentVersion": "8.7.0",
```

```
      "name": "systemSoftware"
   },
   "location": {
      "status": "ok",
      "timezone": "Etc/UTC",
      "utc_offset": "0",
      "name": "location",
      "geoLocation": "unknown"
   },
   "dataDisk": {
      "status": "ok",
      "deviceName": "/dev/sda11",
      "bytesTotal": "4693939073024",
      "name": "dataDisk",
      "bytesUsed": "165065793536",
      "fsType": "ext4",
      "bytesAvail": "4292287692800",
      "bytesFree": "4528873279488",
      "percentFree": "96"
   },
   "rootDisk": {
      "status": "ok",
      "deviceName": "/dev/sda4",
      "bytesTotal": "4160356352",
      "name": "rootDisk",
      "bytesUsed": "1923219456",
      "fsType": "ext4",
      "bytesAvail": "2005614592",
      "bytesFree": "2237136896",
      "percentFree": "53"
   },
   "configDisk": {
      "status": "ok",
      "deviceName": "/dev/sda7",
      "bytesTotal": "511461376",
      "name": "configDisk",
      "bytesUsed": "6738944",
      "fsType": "ext4",
      "bytesAvail": "473688064",
      "bytesFree": "504722432",
      "percentFree": "98"
   },
   "raid": {
      "status": "ok",
      "name": "raid"
   },
   "fireeyeApplianceLicense": {
      "status": "ok",
      "perpetual": "yes",
      "name": "fireeyeApplianceLicense",
      "license": "FIREEYE_APPLIANCE"
   },
   "address": {
      "status": "ok",
      "ipv4": "172.17.56.46",
      "hostName": "dali",
      "ipv6Enabled": "false",
      "domainName": [
         "eng.fireeye.com"
      ]
   },
   "physicalDisk1": {
      "status": "ok",
```

```
      "totalBytes": "4000023301849",
      "name": "physicalDisk1",
      "selfAssess": "Passed",
      "diskStatus": "Online"
   },
   "physicalDisk0": {
      "status": "ok",
      "totalBytes": "4000023301849",
      "name": "physicalDisk0",
      "selfAssess": "Passed",
      "diskStatus": "Online"
   },
   "physicalDisk3": {
      "status": "ok",
      "totalBytes": "4000023301849",
      "name": "physicalDisk3",
      "selfAssess": "Passed",
      "diskStatus": "Online"
   },
   "physicalDisk2": {
      "status": "ok",
      "totalBytes": "4000023301849",
      "name": "physicalDisk2",
      "selfAssess": "Passed",
      "diskStatus": "Online"
   },
   "usb": {
      "status": "ok",
      "mounted": "false",
      "name": "usb"
   },
   "powerSupply": {
      "status": "ok",
      "name": "powerSupply"
   },
   "fan1": {
      "status": "ok",
      "speed": "3800"
   },
   "fan3": {
      "status": "ok",
      "speed": "3700"
   },
   "fan2": {
      "status": "ok",
      "speed": "3500"
   },
   "fan5": {
      "status": "ok",
      "speed": "3500"
   },
   "fan4": {
      "status": "ok",
      "speed": "3900"
   },
   "contentUpdatesLicense": {
      "status": "ok",
      "expiresInSeconds": "27395941",
      "name": "contentUpdatesLicense",
      "license": "CONTENT_UPDATES",
      "perpetual": "no",
      "expDate": "2020/07/13 00:00:00",
      "expInDays": "317"
```

```
            }
        },
        "id": "AC1F6B19DEA8",
        "timezone": "Etc/UTC",
        "model": "FireEyeCM4500",
        "customerId": "900162500",
        "serial": "FM1743QA008"
    },
    "messageType": "healthUpdate",
    "causeCode": "execution",
    "version": "1.0"
}
```


cURL Code Sample: System Health

The following code sample can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSkH --no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/health/system
```

This cURL sample includes the following:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This option allows you to specify a custom header with the `--header` switch.
- `--no-progress-bar`—This option suppresses the cURL download progress bar, which can interfere with the request.

- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header returns the API token that was provided during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token in the sample with the token value received in the response to your authentication request.

  By default, the X-FeApi-Token times out after 15 minutes of inactivity.

- `https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/health/system`—The system health request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.

Results

This example returns a detailed report of the current system health.

System Current Health Request

Returns the current system health status.

```
GET https://<address>/wsapis/v2.0.0/health/current
```

Availability

This command is available on the following appliances:

- Email Security — Server Edition

Required headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Parameters

- `service_id`—Returns status for the specified service.
- `category`—Returns status for the specified category. Value can be `system` or `services`.
- `status`—Returns status for the specified status. Value can be `HEALTHY`, `DEGRADED`, `FAILED`, or `DISABLED`.

Example Request

```
GET https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/health/current
```

```
GET https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/health/curren?category=system
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

System Current Health Response

Line breaks have been added for readability.

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
```

Response

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 401—Request unsuccessful because the session token was invalid.

- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Unauthorized—Request unsuccessful because the session token was invalid.
- Date—Standard HTML date format.

Example

Line breaks have been added for readability.

```
{
  "timestamp" : "yymmddhhmmss(UTC)",
  "system" : [
    {
      "name"        : "CPU Service",
      "service_id"  : "cpu",
      "description" : "CPU health status",
      "status"      : "HEALTHY"
      "details"     : {
        "text" : "CPU is currently healthy"
      }
    },
    {
      "name"        : "Disk Storage Service",
      "service_id"  : "DISKSTORAGE",
      "description" : "Disk Storage status",
      "status"      : "DEGRADED"
      "details"     : {
        "text" : "Disk is currently 80% full"
      }
    },
    {
      "name"        : "Memory Service",
      "service_id"  : "memory",
      "description" : "System memory status",
      "status"      : "FAILED"
      "details"     : {
        "text" : "Too much to memorize. It failed!"
      }
    }
  ],
  "services" : [
    {
      "name"        : "SNORT Service",
      "service_id"  : "snort",
      "description" : "Snort health status",
      "status"      : "HEALTHY"
      "details"     : {
        "text" : "Snort is running like a charm!"
      }
    },
    {
      "name"        : "URL Analyzer Service",
      "service_id"  : "URLANALYZER",
      "description" : "URL Analyzer Service  status",
      "status"      : "DEGRADED"
      "details"     : {
        "text" : "Cannot connect to the cloud service 80% times"
      }
    },
```

```
    {
      "name"        : "Localsig service",
      "service_id"  : "localsig",
      "description" : "Local signature Generation",
      "status"      : "DISABLED"
      "details"     : {
        "text" : "Localsig feature is currently disabled"
      }
    }
  ],
}
```

cURL Code Sample: System Current Health

The following code sample can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSkH --no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/health/current
```

This cURL sample includes the following:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This option allows you to specify a custom header with the `--header` switch.
- `--no-progress-bar`—This option suppresses the cURL download progress bar, which can interfere with the request.

- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header returns the API token that was provided during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token in the sample with the token value received in the response to your authentication request.

  By default, the X-FeApi-Token times out after 15 minutes of inactivity.

- `https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/health/current`—The system health request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.

Results

This example returns a report of the current system health.

System Health History Request

Returns the system health status for a given time period.

```
GET https://<address>/wsapis/v2.0.0/health/history/<service_id>?start_
time=<UTC_time?&end_time=<UTC_time>
```

Availability

This command is available on the following appliances:

- Email Security — Server Edition

Required headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Parameters

- *service_id*—Specifies the service.
- start_time—Specifies the beginning of the time range in UTC format (yyyy-MM-dd'T'HH:mm:ss.SSSZ).
- end_time—Specifies the end of the time range in UTC format (yyyy-MM-dd'T'HH:mm:ss.SSSZ).

Example Request

```
GET https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/health/history/cpu?start_
time=yyyy-MM-dd'T'HH:mm:ss.SSSZ&end_time=yyyy-MM-dd'T'HH:mm:ss.SSSZ
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

System Health History Response

Line breaks have been added for readability.

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
```

Response

- Response Code—A standard HTML response code.
  - 200—Request successful.
  - 401—Request unsuccessful because the session token was invalid.

- Response Message—A standard HTML response message.
  - OK—Request successful.
  - Unauthorized—Request unsuccessful because the session token was invalid.
- Date—Standard HTML date format.

Example

Line breaks have been added for readability.

```
[
  {
    "name"        : "CPU Service",
    "service_id"  : "cpu",
    "description" : "CPU health status",
    "status"      : "HEALTHY",
    "timestamp"   : "11111(UTC)",
    "details"     : {
      "text" : "CPU is currently healthy"
    }
  },
  {
    "name"        : "CPU Service",
    "service_id"  : "cpu",
    "description" : "CPU health status",
    "status"      : "DEGRADED",
    "timestamp"   : "2222(UTC)",
      "details"     : {
        "text" : "CPU load is over 90%"
      }
    },
    {
      "name"        : "CPU Service",
      "service_id"  : "cpu",
      "description" : "CPU health status",
      "status"      : "HEALTHY",
      "timestamp"   : "3333(UTC)",
      "details"     : {
        "text" : "CPU is currently healthy"
      }
    },
  . . .
]
```

cURL Code Sample: System Health History

The following code sample can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

In this sample, line breaks are added for readability. Remove these line breaks before you paste the code sample into your command-line tool.

```
curl -qgsSkH --no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
```

```
https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/health/history/cpu?start_time=2019-
01-15'T'09:03:00.000Z=&end_time=2019-03-15'T'12:00:00.000Z
```

This cURL sample includes the following:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.
- `-H`—This option allows you to specify a custom header with the `--header` switch.
- `--no-progress-bar`—This option suppresses the cURL download progress bar, which can interfere with the request.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header returns the API token that was provided during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token in the sample with the token value received in the response to your authentication request.

  By default, the X-FeApi-Token times out after 15 minutes of inactivity.

- `https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/health/history/cpu?start_time=2019-01-15'T'09:03:00.000Z=&end_time=2019-03-15'T'12:00:00.000Z`—The system health request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance, `cpu` with the service ID, and the times with the desired start and end times.

Results

This example returns a report of the system health history.

Central Management with IPS

The commands are available on the following appliance:

- Central Management

The base URL is /wsapis/v2.0.0/proxy/ipsgroup/. All API endpoints below are prefixed by the base URL. For example, for the `groups` API endpoint, the complete URL would be:

- `https://<CMS IP>/wsapis/v2.0.0/proxy/ipsgroup/groups`

List IPS Groups

Description

Return all IPS groups and their corresponding group members.
This API will filter all empty groups, groups with no Network Security appliances, and groups with Network Security appliances running less than version 9.0.x. Also appliances other than Network Security will be filtered out.

Curl Sample

```
curl -v -H 'Content-Type: application/json
'https://<cmshost>/wsapis/v2.0.0/proxy/ipsgroup/groups
```

Method

GET

Response

```
[
  {
    "appliances": [
      "65HA-1-148",
      "65HA-2-150",
      "dsg74"
    ],
    "group": "sysgroup.Web_MPS",
    "group_type": "system",
    "unsupported_appls": [
      "dsg20",
      "dsg21"
    ]
  },
  {
    "appliances": [
      "65HA-1-148",
      "65HA-2-150",
      "dsg74"
    ],
    "group": "all",
    "group_type": "system"
  },
  {
    "appliances": [
      "65HA-1-148",
      "65HA-2-150"
    ],
    "group": "6500-HA",
    "group_type": "nxha"
  }
]
```

Response Code

- 200
- 503

Compare Policy Configurations

Description

Diff a given appliance's IPS policy configuration on the fly with a target group.
Note that no state will be persisted in the back-end after the API call.

- `src_id (required)` appliance does not need to belong to the target group. The IPS configuration will be fetched from the source appliance directly if it is not in the cache.
  Note that the src_id ips configuration will be discarded after the API call if it's fetched
  directly from source appliance.
- `dst_group (required)` the target group to compare the src_appl IPS configuration with.
  Note that the API will not perform diff on IPS configurations of target appliances that have
  not been cached locally in CMS.

Curl Sample

```
curl -v -H 'Content-Type:
application/json''https://<cmshost>/wsapis/v2.0.0/proxy/ipsgroup/diff?src_
id=nx2&dst_group=sysgroup.Web_MPS'
```

Method

GET

Response

```
{
  "buckets": {
    "4789ac8fdd1c546372dfddcbb9ebef518b1ec6d791185059aa35cf4725ec18cb": {
      "65HA-1-148": {
        "appliance": "65HA-1-148",
        "appliance_id": "002590867E62",
        "content_version": "1.0",
        "fetch_time": 1580366154.3635938,
        "fetch_time_iso": "2020-01-30T06:35:54.363594+00:00",
        "hash":
"4789ac8fdd1c546372dfddcbb9ebef518b1ec6d791185059aa35cf4725ec18cb",
        "last_updated_time": 1580366154.3635938,
        "last_updated_time_iso": "2020-01-30T06:35:54.363594+00:00",
        "match_detail": {
          "details": "Security content versions mismatching",
          "match": true,
          "message": "IPS configurations matching"
        },
```

```
          "nxha_name": "6500-HA",
          "nxha_peer": "65HA-2-150",
          "out_of_sync": false,
          "product_type_lc": "wmps",
          "reason": "",
          "software_version": "9.0.0",
          "status": "success"
        }
      },
      "a4aa440fc72b7939653889710e2f47f56a8c005466c63c8b531f81b8f605df8e": {
        "65HA-2-150": {
          "appliance": "65HA-2-150",
          "appliance_id": "0025908517FC",
          "content_version": "1.0",
          "fetch_time": 1580366153.183817,
          "fetch_time_iso": "2020-01-30T06:35:53.183817+00:00",
          "hash":
"a4aa440fc72b7939653889710e2f47f56a8c005466c63c8b531f81b8f605df8e",
          "last_updated_time": 1580366153.183817,
          "last_updated_time_iso": "2020-01-30T06:35:53.183817+00:00",
          "match_detail": {
            "details": "Configuration of custom rules are different",
            "match": false,
            "message": "Custom rules mismatch"
          },
          "nxha_name": "6500-HA",
          "nxha_peer": "65HA-1-148",
          "out_of_sync": true,
          "product_type_lc": "wmps",
          "reason": "",
          "software_version": "9.0.0",
          "status": "success"
        }
      }
    },
    "group": "sysgroup.web_MPS",
    "last_insync_time": 0.0,
    "last_insync_time_iso": "1970-01-01T00:00:00+00:00",
    "match_time": 1580366163.9055443,
    "match_time_iso": "2020-01-30T06:36:03.905544+00:00",
    "out_of_sync": true,
    "ref_hash":
"4789ac8fdd1c546372dfddcbb9ebef518b1ec6d791185059aa35cf4725ec18cb"
}
```


Response Code

- 200
- 400
- 404
- 503

Create Policy Reference Group

Description

Fetch an IPS policy configuration from a given appliance and save it as reference for the given group.

- `appliance (required)` appliance does not need to belong to group
- `group (required)` set the fetched IPS policy config as the reference for the given group

Curl Sample

```
curl -v -H 'Content-Type: application/json'
https://<cmshost>/wsapis/v2.0.0/proxy/ipsgroup/reference --data '
{"appliance": "dsg74", "group": "sysgroup.Web_MPS"}'
```

Method

POST

Request

```
{
"appliance": "dsg73",
"group": "sysgroup.Web_MPS"
}
```

Response Code

- 200
- 400
- 503

Metadata For Reference Policy Configurations

Description

Return the metadata of all cached reference IPS policy configurations.

Curl Sample

```
curl -v https://<cmshost>/wsapis/v2.0.0/proxy/ipsgroup/reference
```

Method

GET

Request


```
[
  {
    "appliance_id": "0CC47AFB1E7C",
    "appliance_name": "65HA-2-150",
    "fetch_time": 1587177550.9625492,
    "fetch_time_iso": "2020-04-18T02:39:10.962549+00:00",
    "group": "6500-HA",
    "group_type": "nxha",
    "hash":
"334fcd5c57aa26c14842e721f63d1522cfad049a05417e2b11dfed00e5621abd"
  },
  {
    "appliance_id": "002590867E62",
    "appliance_name": "dsg74",
    "fetch_time": 1587177552.1536264,
    "fetch_time_iso": "2020-04-18T02:39:12.153626+00:00",
    "group": "sysgroup.Web_MPS",
    "group_type": "system",
    "hash":
"79cdd33ff1cf32fb6c1a6ee6996ae70eb3511b12612b0adebe2c463c5d9f8f31"
  }
]
```


Response Code

- 200
- 503

Reference Policy Configurations For Group

Description

Return the saved reference IPS policy configuration for the given group from CMS cache.

Curl Sample

```
curl -v
https://<cmshost>/wsapis/v2.0.0/proxy/ipsgroups/reference/sysgroup.Web_MPS
```

Method

GET

Response

```
<JSON IPS POLICY CONFIG>
```

Response Code

- 200
- 404
- 503

Sync Policy Configuration To Group

Description

Sync IPS policy configuration to a group.

- src_group (required)
- dst_appl_list or dst_group (required either one but not both)
- use_cache (required)
- src_id (required only when use_cache is false)

Curl Sample

```
curl -v -H 'Content-Type: application/json'
https://<cmshost>/wsapis/v2.0.0/proxy/ipsgroup/sync_job -XPOST --data '{
"src_group": "sysgroup.Web_MPS", "dst_appl_list": ["dsg74", "dsg80",
"dsg81"], "use_cache": false, "src_id": "dsg73"}'
```

Method

POST

Request

```
{
  "src_group": "sysgroup.Web_MPS",
  "dst_appl_list": [
    "dsg74"
  ],
  "use_cache": false,
  "src_id": "dsg73"
}
```

Response

```
{
  "_create_time": "2019-12-19 06:10:56.133414+00:00",
  "_last_updated_time": "2019-12-19 06:10:56.133414+00:00",
  "create_time": 1576735856.1334136,
  "detailed_status": {
    "dsg74": {
      "_last_updated_time": "2019-12-19 06:10:56.133450+00:00",
      "appl": "dsg74",
      "last_updated_time": 1576735856.1334503,
      "reason": "",
      "status": "queued",
      "sync_req_id": "",
      "tries": 0
    }
  },
  "job_id": "5845cbac-7b6a-4f90-be42-4643c0938636",
```

```
  "job_request": {
    "dst_appl_list": [
      "dsg74"
    ],
    "src_group": "sysgroup.Web_MPS",
    "src_id": "dsg73",
    "use_cache": false
  },
  "job_type": "ips-sync",
  "owner_type": "external",
  "last_updated_time": 1576735856.1334136,
  "reason": "",
  "status": "queued",
  "tries": 0
}
```


Response Code

- 200
- 400
- 503

Policy Sync Status History

Description

Get IPS policy sync status history. URL parameters:

- `status` - filter; can be "queued", "in-progress", "failed", "success", "partial-complete"; for filtering multiple `status`, use a comma-separated list which will return jobs with status that match any of the specified `statuses`
- `create_time (int64)` - filter; if specified, it will filter out jobs that has a job create time less than the specified `create_time`
- `create_time_end (int64)` - filter; if specified, it will filter out jobs that has a job create time greater than the specified `create_time_end`
- `create_time_iso (string)` - filter; if specified, it will filter out jobs that has a job create time less than the specified `create_time_iso`
- `create_time_iso_end (string)` - filter; if specified, it will filter out jobs that has a job create time greater than the specified `create_time_iso_end`
- `last_updated_time (int64)` - filter; if specified, it will filter out jobs that has a job last updated time less than the specified `last_updated_time` in the url parameter
- `last_updated_time_end (int64)` - filter; if specified, it will filter out jobs that has a job last updated time larger than the specified `last_updated_time_end` in the url parameter
- `last_updated_time_iso (string)` - filter; if specified, it will filter out jobs that has a job last updated time less than the specified `last_updated_time_iso` in the url parameter
- `last_updated_time_iso_end (string)` - filter; if specified, it will filter out jobs that has a job last updated time larger than the specified `last_updated_time_iso_end` in the url parameter
- `src_id` - filter; note that the field `src_id` in the **original sync job request** is optional, so any job without `src_id` will be filtered out if `src_id` is specified in the url parameter
- `dst_id` - filter; job is returned **only** if the specified `dst_id` in the url parameter is found in the `dst_appl_list` in the **original sync job response**; for filtering multiple `dst_id`, use a comma-separated list which will return jobs will **all** the `dst_ids` specified
- `dst_group` - filter; note that the field `dst_group` in the **original sync job request** is optional, so any job without `dst_group` will be filtered out if `dst_group` is specified in the url parameter

- owner_type - filter; job initiator. Any job initiated via the API endpoint sync_job is of type external. Any job started by the nxha-sync daemon is of type internal-nxha. Possible values are "internal-nxha", "external"

Curl Sample

```
curl -v https://<cmshost>/wsapis/v2.0.0/proxy/ipsgroup/sync_job
```

Method

GET

Response


```
[
  {
    "create_time": 1587166682.2256286,
    "create_time_iso": "2020-04-17T23:38:02.225629+00:00",
    "detailed_status": {
      "65HA-2-150": {
        "appl": "65HA-2-150",
        "last_updated_time": 1587166692.9575257,
        "last_updated_time_iso": "2020-04-17T23:38:12.957526+00:00",
        "reason": "",
        "status": "in-progress",
        "sync_req_id": "8e555d7b-80fb-4d41-896c-dea3d0b97856",
        "tries": 1
      }
    },
    "job_id": "d7dbc8cd-5383-4ff2-a456-b573b9f64391",
    "job_request": {
      "dst_appl_list": [
        "65HA-2-150"
      ],
      "src_group": "6500-HA",
      "src_id": "65HA-1-148",
      "use_cache": false
    },
    "job_type": "ips-sync",
    "last_updated_time": 1587166690.1601624,
    "last_updated_time_iso": "2020-04-17T23:38:10.160162+00:00",
    "owner_type": "internal-nxha",
    "reason": "",
    "status": "in-progress",
    "tries": 1
  },
  {
    "_create_time": "2019-12-19 06:18:09.354060+00:00",
    "_last_updated_time": "2019-12-19 06:18:09.354060+00:00",
    "create_time": 1576736289.35406,
    "detailed_status": {
      "dsg74": {
        "_last_updated_time": "2019-12-19 06:18:09.354076+00:00",
        "appl": "dsg74",
        "last_updated_time": 1576736289.354076,
        "reason": "",
        "status": "queued",
        "sync_req_id": "",
```

```
        "tries": 0
      }
    },
    "job_id": "2b743755-2392-49d9-be9a-5c7060a8fe68",
    "job_request": {
      "dst_appl_list": [
        "dsg74"
      ],
      "src_group": "sysgroup.Web_MPS",
      "use_cache": true
    },
    "job_type": "ips-sync",
    "owner_type": "external",
    "last_updated_time": 1576736289.35406,
    "reason": "",
    "status": "queued",
    "tries": 0
  }
]
```


Response Code

- 200
- 503

Policy Sync Status

Description

Get IPS policy sync status for a given job ID.

Curl Sample

```
curl -v https://<cmshost>/wsapis/v2.0.0/proxy/ipsgroup/sync_job/2b743755-
2392-49d9-be9a-5c7060a8fe68
```

Method

GET

Response


```
{
  "_create_time": "2019-12-19 06:18:09.354060+00:00",
  "_last_updated_time": "2019-12-19 06:18:09.354060+00:00",
  "create_time": 1576736289.35406,
  "detailed_status": {
    "dsg74": {
      "_last_updated_time": "2019-12-19 06:18:09.354076+00:00",
      "appl": "dsg74",
      "last_updated_time": 1576736289.354076,
      "reason": "",
      "status": "queued",
      "sync_req_id": "",
      "tries": 0
    }
  },
  "job_id": "2b743755-2392-49d9-be9a-5c7060a8fe68",
  "job_request": {
    "dst_appl_list": [
      "dsg74"
    ],
    "src_group": "sysgroup.Web_MPS",
    "use_cache": true
  },
  "job_type": "ips-sync",
  "owner_type": "external",
  "last_updated_time": 1576736289.35406,
  "reason": "",
  "status": "queued",
  "tries": 0
}
```


Response Code

- 200
- 404

- 503

Group Policy Configuration Status

Description

Retrieve group status of IPS policy configurations.

Curl Sample

```
curl -v https://<cmshost>/wsapis/v2.0.0/proxy/ ipsgroup/group_
matching/sysgroup.Web_MPS
```

Method

GET

Response


```
{
  "buckets": {
    "4789ac8fdd1c546372dfddcbb9ebef518b1ec6d791185059aa35cf4725ec18cb": {
      "dsg74": {
        "appliance": "dsg74",
        "appliance_id": "002590867E62",
        "fetch_time": 1576736508.6168592,
        "hash":
"4789ac8fdd1c546372dfddcbb9ebef518b1ec6d791185059aa35cf4725ec18cb",
        "last_updated_time": 1576736508.6168592,
        "out_of_sync": true,
        "match_detail": {
          "details": "Number of rules are 0 v/s 1",
          "match": false,
          "message": "Custom rules mismatch"
        },
        "product_type_lc": "wmps",
        "reason": "",
        "status": "success"
      }
    },
    "a4aa440fc72b7939653889710e2f47f56a8c005466c63c8b531f81b8f605df8e": {
      "dsg73": {
        "appliance": "dsg73",
        "appliance_id": "0025908517FC",
        "fetch_time": 1576736520.0709522,
        "hash":
"a4aa440fc72b7939653889710e2f47f56a8c005466c63c8b531f81b8f605df8e",
        "last_updated_time": 1576736520.0709522,
        "out_of_sync": false,
        "match_detail": {
          "details": "",
          "match": true,
          "message": "IPS configurations matching"
        },
        "product_type_lc": "wmps",
        "reason": "",
        "status": "success"
```

```
        }
      }
    },
    "group": "sysgroup.Web_MPS",
    "out_of_sync": true,
    "last_insync_time": 0.0,
    "match_time": 1576736520.2212718,
    "ref_hash":
"a4aa440fc72b7939653889710e2f47f56a8c005466c63c8b531f81b8f605df8e"
    "unsupported_appls": [
      {
        "appliance": "nx-10550",
        "appliance_id": "0CC47AFC69F6",
        "content_version": "1012.120",
        "fetch_time": 1587531519.0067,
        "fetch_time_iso": "2020-04-22T04:58:39.006700+00:00",
        "last_updated_time": 1587531519.0067,
        "last_updated_time_iso": "2020-04-22T04:58:39.006700+00:00",
        "product_type_lc": "wmps",
        "reason": "Source appliance is running a version of FEOS lower than
configured min.",
        "software_version": "8.3.2",
        "status": "failed"
      }
    ]
}
```


Response Code

- 200
- 404
- 503

Notification Suppression Settings

Description

Get notification suppression settings for a given group.

Curl Sample

```
curl -v https://<cmshost>/wsapis/v2.0.0/proxy/ipsgroup/sysgroup.Web_
MPS/config
```

Method

GET

Response

```
{
  "appliances": [
    {
      "appliance": "dsg73",
      "suppress_warning": true
    },
    {
      "appliance": "dsg74",
      "suppress_warning": true
    }
  ],
  "group": "sysgroup.Web_MPS",
  "suppress_warning": false
}
```

Response Code

- 200
- 404
- 503

Suppress or Unsupress Notification

Description

Suppress/Unsuppress notification.

- `group (required)`
- `suppress_warning (optional)` - suppress/unsuppress warning for the group
- `appliances (optional)` - suppress/unsuppress warning for a list of appliance withing the given group

Curl Sample

```
curl -v -H 'Content-Type: application/json'
https://<cmshost>/wsapis/v2.0.0/proxy/ipsgroup/sysgroup.Web_MPS/config --data
'{"group":"sysgroup.Web_MPS", "appliances": [ {"appliance": "dsg73",
"suppress_warning": true}, {"appliance": "dsg74", "suppress_warning": true}
]}'
```

Method

POST

Request

```
{
  "group": "sysgroup.Web_MPS",
  "suppress_warning": false,
  "appliances": [
    {
      "appliance": "dsg73",
      "suppress_warning": true
    },
    {
      "appliance": "dsg74",
      "suppress_warning": true
    }
  ]
}
```

Response Code

- 200
- 404
- 503

Network Security with IPS

API Definitions

The commands are available on the following appliance:

- Network Security
- Version supported is 2.0.0
- The IPS API base URI is https://<host>/wsapis/v2.0.0/ips. (represented as <ips-api-base> in the table)
- Standard WSAPI authentication and RBAC are used

Asynchronous API response format

Some of the APIs are asynchronous in nature. After validating the input data, these APIs schedule a background worker to perform the operation.
Following is the expected response:

Error Code	Meaning	Response Payload
200	Input is valid, background job scheduled	`{"job_code" : "<operation>", "ips_job_status" : "<workState>", "ips_job_id" : "<job uuid>"}`
400	Invalid input	JSON document with a human-readable message and error code

Async Job Status

API URL

`<ips-api-base>/job/status`

Sample Curl Request

- `curl -gsvk -H "<token>" "https://<host>/wsapis/v2.0.0/ips/job/status?uuid=97492efa-5167-470d-944f-6d2a1848967b"`
- `curl -gsvk -H "<token>" "https://<host>/wsapis/v2.0.0/ips/job/status?operation=upload_rules"`
- `curl -gsvk -H "<token>" "https://<host>/wsapis/v2.0.0/ips/job/status?workState=SUCCESS"`
- `curl -gsvk -H "<token>" "https://<host>/wsapis/v2.0.0/ips/job/status"`

Authentication

Standard WSAPI authentication

Method

`GET - fetch asyn job status`

Query Params (all optional)

uuid: UUID of a job
Operation: one of the following (case insensitive) Valid operations:

SECURITY_CONTENT_UPDATE,

SYNC,

MODIFY_POLICY,

ADD_POLICY,

RULE_UPLOAD,

UPDATE_GEN_CONFIG,

MODIFY_INTERFACES,

DISABLE_POLICIES,

UPLOAD_RULES,

DELETE_CUSTOM_RULES,

APPLY_CUSTOM_RULES,

ADD_POLICY_EXCEPTION,

MODIFY_POLICY_EXCEPTION,

DELETE_POLICY_EXCEPTION

WorkState: one of the follwing (case insensitive)
Valid operations:

SUCCESS,

FAILED,

RUNNING

Response

HTTP OK(200) with JSON representation of the job statuses.

```
When IpsPolicyDaemon starts up, the initial work status info is set to
default params.
{
"workState":"READY",
"operation":"NONE"
}
Once an operation is running
{
"msg": "Updating data base with new changes and recalcuating hash",
"workState": "RUNNING",
"uuid": "97492efa-5167-470d-944f-6d2a1848967b",
"operation": "UPDATE_GEN_CONFIG"
}
once the operation is complete
{
"msg": "Sync operation succesful",
"workState": "SUCCESS",
"uuid": "19571627-1a58-4196-8d7f-35cd822005c8", #last processed reqUuid
"operation": "SYNC"
}
In case of failure.
{
"upload_rules":{
"msg":"Invalid Rules Found",
"workState":"FAILED",
"details":{
"invalid_rules":[
{
"valid":false,
"ruleText":"alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS msg:\"APP-
DETECT Absolute Software Computrace outbound connection -
search.namequery.com\"; flow:to_server,established; content:\"Host|3A|
search.namequery.com|0D 0A|\"; fast_pattern:only; http_header;
content:\"TagId: \"; http_header; metadata:policy max-detect-ips drop, policy
security-ips drop, ruleset community, service http;
reference:url,absolute.com/support/consumer/technology_computrace;
reference:url,attack.mitre.org/techniques/T1014;
reference:url,www.blackhat.com/presentations/bh-usa-09/ORTEGA/BHUSA09-Ortega-
DeactivateRootkit-PAPER.pdf; classtype:misc-activity; sid:85000000; rev:6;)",
"id":85000000,
"errorMsg":"Optional fields doesn't start with a '('"
}
]
},
"uuid":"e743ceab-9dec-4c11-bd0d-84b428553c02",
```

```
"operation":"UPLOAD_RULES"
}
```

Response Mime Type

`application/json`

HTTP Response Codes

- 200 - if there are no errors
- 401 - auth failure
- 500 - if there are any errors

General Configuration

API URL

<ips-api-base>/global/config

Sample Curl Request

```
curl -gsvk -H "$c" "https://<host>/wsapis/v2.0.0/ips/global/config"

curl -gsvk -H "$c" --header "Content-Type: application/json" --data '{"ips_
feature_license_required":false,

"auto_rules_update_enabled":true,"ips_feature_licensed":false,"feature_
adware_supported":false,

"ips_enabled":false,"recon_rules_enabled":false,"ips_feature_
active":false,"riskware_enabled":false,

"blockmode_enabled":false}' "https://<host>/wsapis/v2.0.0/ips/global/config"
```

Authentication

Standard WSAPI authentication

Method

GET - fetch asyn job status

POST - update config

Response

```
HTTP OK with JSON representation of general config
{
"ips_feature_license_required": false,
"auto_rules_update_enabled": true,
"ips_feature_licensed": false,
"feature_adware_supported": false,
"ips_enabled": false,
"recon_rules_enabled": false,
"ips_feature_active": false,
"riskware_enabled": false,
"blockmode_enabled": false
}
```

Response Mime Type

application/json

HTTP Response Codes

- 200 - no errors
- 401 - auth error
- 400 - invalid data
- 429 - system busy, try after some time
- 500 - internal error

Policy Information

API URL

```
<ips-api-base>/policies?<filters
ips-api-base>/policies/<policy-name>?<filters
```

URL Parameters

```
concise_info: (optional) - true(default)|false
policy_type: (mandatory)- ips_default|ips_custom
```

Sample Curl Request

1. Fetch ALL policies
   ```
   curl -gsvk -H "$c" --header "Accept: application/json" "https://<host>/
    wsapis/v2.0.0/ips/policies
   ```
2. Fetch ALL Default policies
   ```
   curl -gsvk -H "$c" --header "Accept: application/json" "https://<host>/
    wsapis/v2.0.0/ips/policies?policy_type=ips_default"
   ```
3. Fetch ALL Custom policies
   ```
   curl -gsvk -H "$c" --header "Accept: application/json" "https://<host>/
    wsapis/v2.0.0/ips/policies?policy_type=ips_custom"
   ```
4. Fetch a single Default policy
   ```
   curl -gsvk -H "$c" --header "Accept: application/json" "https://<host>/
    wsapis/v2.0.0/ips/policies/Comprehensive?policy_type=ips_
   default"<code?
   ```
5. Fetch a single custom policy
   ```
   curl -gsvk -H "$c" --header "Accept: application/json" "https://<host>/
    wsapis/v2.0.0/ips/policies/MyPolicy?policy_type=ips_custom"
   ```

Authentication

Standard WSAPI authentication

Method

GET

Response

HTTP OK with JSON representation of policy

```
{
"match_criteria": {
"max_confidence": 10,
"max_severity": 10,
"attack_target": [
"client",
```

```
"server"
],
"min_confidence": 0,
"min_severity": 0,
"hash": "8292f7028a7c4e07765fc45000fb1aa1b44954292d2fe673bef8f324d1f547b2"
},
"interfaces": [
{
"name": "A",
"state": "applied"
},
{
"name": "B",
"state": "empty"
}
],
"last_updated": "2014/04/25",
"is_active": true,
"ruleset": {
"custom": {
"block_count": 10,
"active_count": 0,
"hash": "76e8430845b848ea9a61dad6a5d22f710096e56ce25694353ac3313cef30f2ee",
"rule_count": 10
},
"hash": "d52df14ae5c086e3102c832bd6b2714cea2c3a3d0940e039871cb7a9e9a119d8",
"content": {
"block_count": 8128,
"version": "1025.242",
"rule_count": 8263
}
},
"policy_name": "ComprehensiveClone",
"insert_time": "2020-06-11T17:55:41.553101",
"is_writable": false,
"is_default": false,
"policy_version": 2,
"policy_type": "ips_custom",
"inclusion_list": {},
"update_time": "2020-06-12T18:29:47.813948",
"exclusion_list": {
"rules": []
},
"hash": "acd9882335d0ca0ca3b485b3b0ecb5fa5cf90cedde02dc87454c4a6a83ecce36"
}
```


Response Mime Type

application/json

Add or Modify Policies

API URL

```
add/clone policy POST - <ips-api-base>/policies
modify policy POST - <ips-api-base>/policies/<policy-name>/modify
```

Sample Curl Request

```
curl -gsvk -X POST --header "$c" --header "Content-Type: application/json" --
data @custom_policy.json "https://<host>/wsapis/v2.0.0/ips/policies"
```

Authentication

Standard WSAPI authentication

Method

```
POST - add/clone policy
POST - modify policy
```

Request

```
{
"inclusion_list": {
"rules" : [
{
"rule_id":85300112,
"rule_revision":12,
"action":"block"
},
{
"rule_id":85300113,
"rule_revision":13,
"action":"noblock"
}
]
},
"exclusion_list":{
"rules" : [
{
"rule_id":85000001,
"rule_revision":12,
"action":"block"
},
{
"rule_id":85300007,
"rule_revision":13,
"action":"block"
}
]
},
"interfaces":[
"A",
```

```
"B"
],
"policy_name":"Custom-Policy_cloned_from_FireEye_Default",
"cloned_policy":"FireEye_Default",
"cloned_policy_type":"ips_default",
"block_all":false
}
```


HTTP Response Codes

- 200 - no errors
- 401 - auth error
- 400 - invalid data
- 429 - system busy, try after some time
- 500 - internal error

Disable Policies

API URL

```
POST <ips-api-base>/policies/disable
```

Sample Curl Request

```
curl -gsvk -H "$c" -X POST "https://<host>/wsapis/v2.0.0/ips/policies/
disable"
```

Authentication

Standard WSAPI authentication

HTTP Response Codes

- 200 - no errors
- 401 - auth error
- 429 - system busy, try after some time
- 500 - internal error

Manage Policy Interfaces

API URL

`GET -<ips-api-base>/interfaces` - all interfaces on an appliance

`GET/POSTPOST - <ips-api-base>/policies/<policy-name>/interfaces` - get/update interfaces for a given policy

URL Parameters

`policy_type (mandatory): ips_custom|ips_default`

Sample Curl Request

```
curl -gsvk --header "$c" "https://<host>/wsapis/v2.0.0/ips/policies/Custom-Policy_cloned_from_FireEye_Default/interfaces"
```

```
curl -gsvk --header "$c" "https://<host>/wsapis/v2.0.0/ips/interfaces"
```

```
curl -gsvk -X POST -H "$c" -H "Content-Type: application/json" --data '["A", "B"]' "https://<host>/wsapis/v2.0.0/ips/policies/FireEye_Default/interfaces?policy_type=ips_default"
```

```
curl -gsvk -X POST -H "$c" -H "Content-Type: application/json" --data '[]' "https://<host>/wsapis/v2.0.0/ips/policies/FireEye_Default/interfaces?policy_type=ips_default"
```

Authentication

Standard WSAPI authentication

Method

```
GET - fetch interface/s
POST - add/modify interface/s
```

`application/json`

Request Body

JSON Array of valid interfaces: example ["A", "B"]

Request Mime Type

`application/json`

HTTP Response Codes

- 200 - no errors
- 401 - auth error

- 429 - system busy, try after some time
- 500 - internal error

Delete Policies

API URL

`<ips-api-base>/policies/delete` - Delete all custom policies

`<ips-api-base>/policies/<policy-name>/delete` - Delete a given custom policy

Sample Curl Request

Delete all custom policies -

```
curl -gsvk -X POST --header "$c" "https://<host>/wsapis/v2.0.0/ips/
policies/delete"
```

Delete a particular custom policy -

```
curl -gsvk -X POST --header "$c" "https://<host>/wsapis/v2.0.0/ips/
policies/Custom-Policy_cloned_from_FireEye_Default/delete"
```

Authentication

Standard WSAPI authentication

Method

`POST`

Response Mime Type

`application/json`

HTTP Response Codes

- 200 - no errors
- 401 - auth error
- 429 - system busy, try after some time
- 500 - internal error

List Policy Rules

API URL

```
<ips-api-base>/policies/<policy-name>/rules
```

URL Parameters

```
policy_type (mandatory) : ips_custom | ips_default
offset, limit (optional): for pagination
```

Sample Curl Request

```
curl -gsvk -H "$c" --header "Accept: application/json" "https://<host>/
wsapis/v2.0.0/ips/policies/FireEye_Default/rules?
policy_type=ips_default&limit=5&offset=10" | jq "."
```

Authentication

Standard WSAPI authentication

Method

GET

Response


```
[
{
"severity": "7",
"reference": "CVE-2011-0611,BID-47314",
"signature_iden": 85300010,
"protocol": "http",
"block_status": 0,
"blocked": "blockable",
"rule_name": "Adobe Flash Player ActionScript callMethod Type Confusion Code
Execution",
"is_custom": false,
"created_at": "2013-09-30T00:00:00",
"category": "exploit",
"enabled": true,
"direction": "from_server"
},
{
"severity": "7",
"reference": "CVE-2007-0015,BID-21829,SECUNIA-SA23540",
"signature_iden": 85300011,
"protocol": "http",
"block_status": 0,
"blocked": "blockable",
"rule_name": "Apple QuickTime RTSP URL Buffer Overflow",
"is_custom": false,
"created_at": "2013-09-30T00:00:00",
"category": "exploit",
```

```
"enabled": true,
"direction": "to_client"
},
{
"severity": "7",
"reference": "CVE-2007-0015",
"signature_iden": 85300012,
"protocol": "http",
"block_status": 0,
"blocked": "blockable",
"rule_name": "Apple QuickTime RTSP URL Buffer Overflow",
"is_custom": false,
"created_at": "2013-09-30T00:00:00",
"category": "exploit",
"enabled": true,
"direction": "to_client"
}
]
```


Response Mime Type

`application/json`

Response Codes

- 200 - no errors
- 401 - auth error
- 500 - internal error

HTTP Response Codes

- 200 - no errors
- 401 - auth error
- 429 - system busy, try after some time
- 500 - internal error

Manage Custom Rules

API URL

```
<ips-api-base>/custom_rules
```

Sample Curl Request

```
curl -gsvk -X POST -H "$c" --header "Content-Type: multipart/form-data" -F
filename=@custom_rule
"https://<host>/wsapis/v2.0.0/ips/custom_rules"
```

Authentication

Standard WSAPI authentication

Method

```
POST - add custom rule
```

Request Payload Samples

File upload sample:

```
"alert tcp any $HTTP_PORTS -> any any ( msg:
\"Mozilla Firefox Cross Domain Information Disclosure\"; attack_
target:client; flow:from_
server; file_data; content:\"alert('Hello
'+/^https\\:\\\\/\\\\/twitter.com\\\\/([^/]
+)/.exec(win.locati     on)[1])\"; rule_format:
2; is_ips:yes; action:blockable; vm_verify:no; protocol:http;
category:exploit; sub_categ
ory:information_leakage; severity:7; confidence:8; release_date:09-30-2013;
modify_date:
01-27-2016;  reference:cve,     CVE-2012-4192; reference:osvdb,OSVDB-86126;
metadata:qual
ity null; sid:85000001; rev:12; )",
"alert tcp any $HTTP_PORTS -> any any ( msg:
\"Mozilla Firefox Cross Domain Information Disclosure\"; attack_
target:client; flow:from_
server; file_data; content:\"alert('Hello
'+/^https\\:\\\\/\\\\/twitter.com\\\\/([^/]
+)/.exec(win.locati     on)[1])\"; rule_format:
2; is_ips:yes; action:blockable; vm_verify:no; protocol:http;
category:exploit; sub_categ
ory:information_leakage; severity:7; confidence:8; release_date:09-30-2013;
modify_date:
01-27-2016;  reference:cve,     CVE-2012-4192; reference:osvdb,OSVDB-86126;
metadata:qual
ity null; sid:85000002; rev:12; )"
```

JSON upload (application/json)

Json sample:

```
[
"alert tcp any $HTTP_PORTS -> any any ( msg:\"Mozilla Firefox Cross Domain
Information
Disclosure\"; attack_target:client; flow:from_server; file_data;
content:\"alert('Hello
'+/^https\\:\\\\/\\\\/twitter.com\\\\/([^/]+)/.exec(win.locati on)[1])\";
rule_format:2;
is_ips:yes; action:blockable; vm_verify:no; protocol:http; category:exploit;
sub_category:information_leakage; severity:7; confidence:8; release_date:09-
30-2013;
modify_date:01-27-2016; reference:cve, CVE-2012-4192; reference:osvdb,OSVDB-
86126;
metadata:quality null; sid:85000008; rev:12; )"
]
```

Response

For JSON upload:

The validation results are returned if there are errors (as follows). If no errors, then the Async API response format is returned.

For file upload:

Async API response format is returned.

Sample responses:

```
[
{
"valid":true,
"ruleText":"alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:
\"APP-DETECT Absolute Software Computrace outbound connection - search.nam
equery.com2\"; flow:to_server,established; content:\"Host|3A| search.namequ
ery.com3|0D 0A|\"; fast_pattern:only; http_header; content:
\"TagId: \"; http_header; metadata:policy max-detectips drop, policy
securityips drop, ruleset community, service http;
reference:url,absolute.com/
support/consumer/technology_computrace4; reference:url,attack.mitre.org/
techniques/T10145; reference:url,www.blackhat.com/presentations/bh-usa-09/
ORTEGA/BHUSA09-Ortega-DeactivateRootkit-PAPER.pdf6; classtype:miscactivity;
sid:85000000; rev:6;)",
"id":85000000
},
{
"valid":false,
"ruleText":"alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS msg:
\"APP-DETECT Absolute Software Computrace outbound connection - search.nam
equery.com7\"; flow:to_server,established; content:\"Host|3A| search.namequ
ery.com8|0D 0A|\"; fast_pattern:only; http_header; content:
\"TagId: \"; http_header; metadata:policy max-detect-
ips drop, policy securityips drop, ruleset community, service http;
reference:url,absolute.com/
support/consumer/technology_computrace9; reference:url,attack.mitre.org/
techniques/T101410; reference:url,www.blackhat.com/presentations/bh-usa-09/
ORTEGA/BHUSA09-Ortega-DeactivateRootkit-PAPER.pdf11; classtype:miscactivity;
sid:85000001; rev:6;)",
"id":85000001,
"errorMsg":"Optional fields doesn't start with a '('"
}
]
```

List Custom Rules

API URL

<ips-api-base>/custom_rules

URL Parameters

is_concise (optional): true(default)/false . is_concise=false will include rule_text as well in the response

offset/limit (optional): for pagination

Sample Curl Request

```
curl -gsvk -H "$c" --header "Accept: application/json"
"https://<host>/wsapis/v2.0.0/ips/ custom_rules?limit=5&offset=10&is_
concise=true" | jq "."
```

Authentication

Standard WSAPI authentication

Method

GET

Response


```
[
{
"severity": "7",
"reference": "CVE-2011-0611,BID-47314",
"signature_iden": 85300010,
"protocol": "http",
"block_status": 0,
"blocked": "blockable",
"rule_name": "Adobe Flash Player ActionScript callMethod Type Confusion Code
Execution",
"is_custom": false,
"created_at": "2013-09-30T00:00:00",
"category": "exploit",
"enabled": true,
"direction": "from_server"
},
{
"severity": "7",
"reference": "CVE-2007-0015,BID-21829,SECUNIA-SA23540",
"signature_iden": 85300011,
"protocol": "http",
"block_status": 0,
"blocked": "blockable",
"rule_name": "Apple QuickTime RTSP URL Buffer Overflow",
"is_custom": false,
```

```
"created_at": "2013-09-30T00:00:00",
"category": "exploit",
"enabled": true,
"direction": "to_client"
},
{
"severity": "7",
"reference": "CVE-2007-0015",
"signature_iden": 85300012,
"protocol": "http",
"block_status": 0,
"blocked": "blockable",
"rule_name": "Apple QuickTime RTSP URL Buffer Overflow",
"is_custom": false,
"created_at": "2013-09-30T00:00:00",
"category": "exploit",
"enabled": true,
"direction": "to_client"
}
]
```


HTTP Response Codes

- 200 - no errors
- 401 - auth error
- 500 - internal error

Apply Custom Rules

API URL

```
<ips-api-base>/custom_rules/apply
```

Sample Curl Request

```
curl -gsvk -X POST --header "$c" "https://<host>/wsapis/v2.0.0/ips/ custom_
rules/apply"
```

Authentication

Standard WSAPI authentication

Method

POST

Custom Rule Information

API URL

<ips-api-base>/custom_rules/info

Sample Curl Request

```
curl -gsvk -X GET --header "$c" "https://<host>/wsapis/v2.0.0/ips/ custom_
rules/info"
```

Authentication

Standard WSAPI authentication

Method

GET

Response

```
{
"block_count": 0,
"active_count": 0,
"hash": "d55a490c2f2655f8bae6519bff919061f9831821d83cf9b9daf7f41181f73be7",
"rule_count": 100
}
```

Delete Custom Rules

API URL

```
<ips-api-base>/custom_rules/delete
```

Sample Curl Request

```
curl -gsvk -X POST --header "$c" --header "Content-Type: application/json" --
data '[85000001, 85000002]' "https://<host>/wsapis/v2.0.0/ips/custom_
rules/delete"
curl -gsvk -X POST -H "$c" "https://<host>/wsapis/v2.0.0/ips/custom_
rules/delete"
```

Authentication

Standard WSAPI authentication

Method

POST

Request Body

JSON array: [85000001, 85000002] - deletes rules which match the id's provided
If no request body/empty array is provided - deletes all the custom rules

Response Mime Type

```
application/json
```

Export CustomRules

API URL

```
<ips-api-base>/custom_rules/export
```

Sample Curl Request

```
curl -gsvk --header "$c" "https://<host>/wsapis/v2.0.0/ips/custom_
rules/export"
```

Authentication

Standard WSAPI authentication

Method

GET

Response

A simple text file which contains uploaded custom rules

Response Codes

- 200 - no errors
- 401 - auth error
- 500 - internal error

List Policy Exceptions

API URL

<ips-api-base>/policy_exceptions

URL Parameters

All filters can be passed as optional query params. Supported ones are listed below:

signature - "test-1" / 1234 (takes both signature_id and signature_name)
interface - "A","B","ALL"
victim_ip - ipv4 address/sub_net
attacker_ip- ipv4 address/sub_net
action - "block","suppress","unblock","suppress_unblock"

Sample Curl Request

```
curl -gsvk "https://<host>/wsapis/v2.0.0/ips/policy_exceptions"
curl -gsvk -H "$c" "https://<host>/wsapis/v2.0.0/ips/policy_exceptions?
interface=A&signature=test-1&action=block"
curl -gsvk -H "$c" "https://<host>/wsapis/v2.0.0/ips/policy_exceptions?
interface=A&signature=123&action=block"
```

Authentication

Standard WSAPI authentication

Method

GET

Response

```
{
"hash": "584d701b524763af7f5236f0e3a83baa",
"signatures": [
{
"id": "1111",
"interface": "A",
"srcip": "172.16.45.34",
"destip": "10.9.3.4",
"action": "noblock"
},
{
"name": ""<sig-name1>",
"interface": "A",
"srcip": "172.16.45.34",
"destip": "10.9.3.4",
"action": "noblock"
}
...
]
}
```

Response Codes

- 200 - no errors
- 401 - auth error
- 500 - internal error

Add Policy Exceptions

API URL

<ips-api-base>/policy_exceptions

Sample Curl Request

```
curl -gsvk -X POST --header "$c" --header "Content-Type: application/ json" --data12 '{"name":"<sig name1>","interface":"A","victim_ip":"172.16.45.34/24","attacker_ip":"10.9.3.4/24","action":"noblock"}'
"https://<host>/wsapis/v2.0.0/ips/policy_exceptions"
```

Authentication

Standard WSAPI authentication

Method

POST – add policy exception – one exception at a time

Request Body

```
{
"original_signature":{
"victim_ip":"172.16.45.34/24",
"attacker_ip":"10.9.3.4/24",
"name":"test-1",
"action":"noblock",
"interface":"A"
},
"modified_signature":{
"name":"test-1",
"interface":"A",
"victim_ip":"172.16.45.34/22",
"attacker_ip":"10.9.3.4/22",
"action":"block"
}
}
```

Response Mime Type

application/json

Update Policy Exceptions

API URL

<ips-api-base>/policy_exceptions/modify

Sample Curl Request

```
curl -gsvk -X POST -H "Content-Type: application/json" -H "$c"
 --data '{"original_signature":{"victim_ip":"172.16.45.34/24","attacker_
ip":"10.9.3.4/24","name":"test-
1","action":"noblock","interface":"A"},"modified_signature":{"victim_
ip":"172.16.45.34/22","attacker_ip":"10.9.3.4/22","name":"test-
1","action":"block","interface":"A"}}'
 "https://<host>/wsapis/v2.0.0/ips/policy_exceptions/modify"
```

Authentication

Standard WSAPI authentication

Method

POST - modify policy exception - one exception at a time

Request Body

```
{
"original_signature":{
"victim_ip":"172.16.45.34/24",
"attacker_ip":"10.9.3.4/24",
"name":"test-1",
"action":"noblock",
"interface":"A"
},
"modified_signature":{
"name":"test-1",
"interface":"A",
"victim_ip":"172.16.45.34/22",
"attacker_ip":"10.9.3.4/22",
"action":"block"
}
}
```

Response Mime Type

application/json

Delete Policy Exceptions

API URL

<ips-api-base>/policy_exceptions/delete

Sample Curl Request

```
curl -gsvk -X POST --header "$c" --header "Content-Type: application/ json" --data13 '{"name":"<sig name1>","interface":"A","victim_ip":"172.16.45.34/24","attacker_ip":"10.9.3.4/24","action":"noblock"}'
"https://<host>/wsapis/v2.0.0/ips/policy_exceptions/delete"
```

Authentication

Standard WSAPI authentication

Method

POST – delete policy exception – one exception at a time

Request Body

```
{
"name": "<signame1>",
"interface": "A",
"victim_ip": "172.16.45.34/24",
"attacker_ip": "10.9.3.4/24",
"action": "noblock"
}
```

Even grouping is supported
If input = {"id" : 345} , then all the signatures which has id =345 are deleted
If input = {"id" : 123, "interface": A} , then all the signatures **with** id=123 and
interface=A are deleted

Response Mime Type

application/json

List Global Information

API URL

`<ips-api-base>/global - Config + policies`

URL Parameters

All filters are passed as optional query params. Supported ones are listed below:
is_concise = true/false

Sample Curl Request

```
curl -gsvk -H "$c" "https://<host>/wsapis/v2.0.0/ips/global"
```

Authentication

Standard WSAPI authentication

Method

`GET`

Response

`application/json`

The JSON structure is shown in the IPSManagement Redesign FS page

Response Codes

- 200 - no errors
- 401 - auth error
- 500 - internal error

View Global Information

API URL

<ips-api-base>/global/config - Config only

Sample Curl Request

```
curl -gsvk -H "$c" "https://<host>/wsapis/v2.0.0/ips/global/config"
```

Authentication

Standard WSAPI authentication

Method

GET

Response

application/json

Response Sample

```
{
"ips_feature_license_required": false,
"auto_rules_update_enabled": true,
"ips_feature_licensed": false,
"feature_adware_supported": false,
"ips_enabled": false,
"recon_rules_enabled": false,
"ips_feature_active": false,
"riskware_enabled": false,
"blockmode_enabled": false
}
```

Response Codes

- 200 - no errors
- 401 - auth error
- 500 - internal error

Sync Global Configuration

API URL

```
<ips-api-base>/global/sync
```

Sample Curl Request

```
curl -gsvk -X POST -H "Content-Type: application/json" -H "$c" --data
@globalConfig.json "https://<host>/wsapis/v2.0.0/ips/global/sync"
```

Authentication

Standard WSAPI authentication

Method

```
POST
```

Response

```
application/json
```

Request

```
mime-type - application/json
```

Response

```
application/json
 {"sync_req_id":"6252b6ab-b62c-4077-a4f9-892eff436020"}
```

Global Configuration Sync Status

API URL

```
<ips-api-base>/global/sync/<sync-uuid>/status
```

Sample Curl Request

```
curl -gsvk -H "$c" "https://<host>/wsapis/v2.0.0/ips/global/sync/ 6252b6ab-b62c-4077-a4f9-892eff436020/status"
```

Authentication

Standard WSAPI authentication

Method

GET

Response

```
application/json
 {"status_message":"sync sucessfull","status_code":2,"search_id":"6252b6ab-b62c-4077- a4f9-892eff436020"}
```

Response Codes

- 200 - no errors
- 401 - auth error
- 500 - internal error

Logging Out

After you have completed your requests, you should log out using the `logout` command. This command ends the session between the remote server and your appliance and disables the session token.

The Web Services API has a default limit of 100 concurrent open sessions. FireEye highly recommends that you close any session you open after you have finished.

Log Out Request

```
POST https://<address>/wsapis/[v1.2.0|v2.0.0]/auth/logout
```

This command is available on the following appliances:

- Central Management
- Malware Analysis
- Email Security — Server Edition
- File Protect
- Network Security
- VX Series

Required headers:

```
X-FeApi-Token: [API-Token]
X-FeClient-Token: [Client-Token]
```

Parameters

- address—The IP address of the appliance running the Web Services API.
- API-Token—This token authenticates the session. By default, the session times out after 15 minutes of inactivity.
- Client-Token—(Optional) This client token is provided by FireEye. For more information about the client token, contact your sales representative.

Example

```
https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/auth/logout
```

Request headers:

```
X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
X-FeClient-Token: BigDataInc
```

Log Out Response

```
HTTP/1.1 [Response Code] [Response Message]
Date: [Date]
```

Response Fields

- Response Code—A standard HTML response code.
  - 204—Logout successful.
  - 304—Request unsuccessful because the session token was missing.
- Response Message—A standard HTML response message.
  - No Content—Logout successful.
  - Not Modified—Request unsuccessful because the session token was missing.
- Date—Standard ISO-8601 date format.

Example

```
HTTP/1.1 200 OK
Date: Fri, 20 Sep 2015 08:00:00 GMT
```

cURL Code Sample: Logging Out

The following code sample can be copied and executed from any command-line interface that includes the cURL library. This sample builds on the authentication cURL code sample.

In this sample, line breaks are added for readability. These line breaks must be removed before you paste the code sample into your command-line tool.

```
curl -qgsSkH --no-progress-bar
--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
-F form=:https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/logout
```

This cURL sample performs the following tasks:

- `-q`—This option specifies that the `curlrc` config file is not read or used. Although this is an optional setting, FireEye recommends that you include this option.
- `-g`—This option turns off the URL globbing parser. Although this is an optional setting, FireEye recommends that you include this option.
- `-s`—This option turns off the progress meter and error message. Although this is an optional setting, FireEye recommends that you include this option.
- `-S`—When used with the `-s` option, this option shows error messages if your cURL switch fails. Although this is an optional setting, FireEye recommends that you include this option.
- `-k`—This option explicitly allows cURL to perform insecure SSL connections and transfers. This allows you to test your SSL connection without installing a CA certificate.

- `-H`—This header allows you to specify a custom header with the `--header` switch.
- `--no-progress-bar`—No progress bar suppresses the cURL download progress bar, which can interfere with the request.
- `--header "X-FeApi-Token: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"`—This custom header provides the API-Token that was returned during the authentication request. In the authentication cURL code sample, this token was included in the `auth.txt` file. Replace the token value in the code sample with the token value received in response to your authentication request.

  By default, the X-FeApi-Token times out after 15 minutes of inactivity.

- `-F form=:`— The -F switch and the subsequent empty form force cURL to use the HTTP POST request.
- `https://xxx.xxx.xxx.xxx:443/wsapis/v2.0.0/logout`—The logout request URL. Replace the IP address `xxx.xxx.xxx.xxx` with the IP address of your appliance.

Results

If executed properly, this code will log you off your appliance. You will not see any response from your appliance. However, if you attempt to use the session key again to perform a new request, you will get the following message:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<fireeyeapis version="v1.2.0">
  <description>Please check if the cookie has expired and retry</description>
  <errorCode>FEAUTH1001</errorCode>
  <httpStatus>401</httpStatus>
  <message>Unauthorized</message>
</fireeyeapis>
```

PART III: Example: Using the Web Services API

In the following code example, a Python script is used to authenticate to the Central Management appliance and then to request a report from the Central Management appliance.

```
#!/usr/bin/env python2.7


import urllib2, base64, ssl
import sys
import argparse

ctx = ssl.create_default_context()
ctx.check_hostname = False
ctx.verify_mode = ssl.CERT_NONE

class WsConnection:
   def __init__(self, urlIn, username, password):
       url = urlIn + "/auth/login"
       print("Authenticating: %s %s %s" % (url, username, password))
       request = urllib2.Request(url, "test")
       base64string = base64.encodestring('%s:%s' % (username, password)).replace
('\n', '')
       request.add_header("Authorization", "Basic %s" % base64string)
       request.add_header("X-FeClient-Token", "test")
       result = urllib2.urlopen(request,context=ctx)
       headers = result.info().dict
       print "Authenticated. Token:" + headers["x-feapi-token"]
       self.auth_token = headers["x-feapi-token"];

   def send_request(self, url):
       print "SEND_REQUEST:" + url
       request = urllib2.Request(url)
       request.add_header("X-FeClient-Token", "test")
       request.add_header("X-FeApi-Token", self.auth_token)
       result = urllib2.urlopen(request, context=ctx)
       return result.read()

def getAlerts(connection, baseurl, argsList):
   url = baseurl + "/alerts?"
   for arg in argList:
       url += arg[0] + "=" + arg[1] + "&"
   print connection.send_request(url)

def getReports(connection, baseurl, args):
   url = baseurl + "/reports/report?module=eMPS&command=
empsEmailAVReport&frame=pastWeek&type=csv"
   print connection.send_request(url)

def logout(token, ip, port):
   url = "https://%s:%s/wsapis/v1.2.0/auth/logout" % (ip, port)
   print "calling logout:" + url
```

```
    request = urllib2.Request(url, "test")
    request.add_header("X-FeClient-Token", "test")
    request.add_header("X-FeApi-Token", token)
    result = urllib2.urlopen(request, context=ctx)
    return result.info()

def usage_exit():
   print "python api_client.py cms={cms address} port={port} user={user}
pass={pass} [{filter=value}]"
   exit(1)

cmsAddr = False
cmsPort = False
username = False
password = False
api = "alerts"
argList = []

if __name__ == "__main__":
   skipOnce = True
   for arg in sys.argv:
       if skipOnce:
          skipOnce = False
          continue
       key,value = arg.split("=")
       #print key, value
       if key == "cms":
          cmsAddr = value
          continue
       if key == "port":
          cmsPort = value
          continue
       if key == "user":
          username = value
          continue
       if key == "pass":
          password = value
          continue
       if key == "api":
          api = value
       tpl = []
       tpl.append(key)
       tpl.append(value)
       rgList.append(tpl)

   if cmsAddr and cmsPort and username and password:
          baseurl = "https://" + cmsAddr + ":" + cmsPort + "/wsapis/v1.0.0"
          conn = WsConnection(baseurl, username, password)
          if api == "alerts":
               print "Calling alerts API"
               getAlerts(conn, baseurl, argList)
   else:
          usage_exit()
```


Technical Support

For technical support, contact FireEye through the Support portal:

csportal.fireeye.com

Documentation

Documentation for all FireEye products is available on the FireEye Documentation Portal (login required):

https://docs.fireeye.com/

FireEye, Inc. | 601 McCarthy Blvd. | Milpitas, CA | 1.408.321.6300 | 1.877.FIREEYE | www.fireeye.com/company/contact-us.html