EXHIBIT 13

password	Password for the new user
csrf_token	unique token ID for the new user
remote_authentication	Valid values are true or false.This key determines whether the user being created will be authenticated using the remote system or not.
remote_authorization	Valid values are true or false.This key determines whether the user being created will be authorized using the remote system or not.

Example

```
curl -k -H "Authorization:d7e6d14140fc944fc4ba287f88f42d45"
"https://10.2.20.107/admin/api.php?op=add_user" -d user_name=test2 -d
full_name=test2 -d role_name='Default Admin Role' -d
generate_api_key=0 -d api_key_is_disabled=0 -d password=JATP1z2 -d
remote_authentication=false -d remote_authorization=false
```

Authorization - The device user API key.
Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

Sample Response

There is no response from this API call.

analysis_details

Use the analysis_details API to retrieve the analysis details associated with a particular file object. The analysis_details API takes either an event_id, md5sum or sha1sum as a parameter.

> TIP As of Release 4.1.1 and later, Juniper ATP Appliance now limits the upload to the actual processing limit and throws an error if the file is greater than 16MB.

Unlike the “event” API, analysis_details does not return any context about how and when the file object was discovered.

An additional boolean parameter “get_components” set to 1 will cause the return of all the components of the specified file. This option is only meaningful if the md5sum/sha1sum corresponds to a zip, tar, or other archive.

```
https://HOST/admin/api.php?op=analysis_details
```

.

HTTP Post Parameters	Description
event_id or md5sum/ sha1sum	[Required] Unique identifier for this event. One of these parameters is a mandatory parameter. Get this from the output of the API https://<Host>/admin/api.php?op=events The md5sum & sha1sum are the hashes of the objects.

get_components	1 indicates components are available. When the get_components value is set, analysis details for all the sub-components are also returned.

API Access: To demonstrate the analysis_details API from the Central Manager Web UI Incidents page: select an incident from the Incidents table then scroll down the page and click Downloads or Uploads tab. Expand the row to view details and with this action, you will see a call to the analysis_details API.
See also behavior_details on page 10

Example

```
curl -k -H "Authorization:7c71c218662411a5c857042053acca8f"
"https://10.2.20.37/admin/api.php?op=analysis_details" -d
event_id=672
```

Authorization - The device user API key.
Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

NOTE The request should include one of event-id or md5 or sha1. If both are specified, then the server only considers the event-id.

Sample Response

```
{
      analysis_array:
      [
      1]
            0:
            {
                  local_path: "/var/spool/c-icap/download/CI_TMPFP9jYz"
                  file_md5_string: "7be866d691c3da79f51240bf8963e210"
                  file_sha1_string:
                  "1f707b2fe77691ee91aa5da0a326aec40182bb0d"
                  file_sha256_string:
                  "fada509542437360aeaa73a6256a9f1c8
                  8764e823f0f0a6a78fb66e419b5f389"
                  file_size: "893977"
                  file_type_string: "PE32 executable (GUI) Intel 80386,
                  for MS Windows"
                  file_suffix: "exe"
                  mime_type_string: "FILE_UPLOAD"
                  has_components: null
                  packer_name: null
                  malware_name: "TROJAN_YAKES.CY"
                  malware_severity: "0.75"
                  malware_category: "Trojan_Generic"
                  malware_classname: "malware"
                  has_static_detection: "1"
                  has_behavioral_detection: "0"
```

```
                user_whitelisted: null
                JATP_whitelisted: null
                has_cnc: null
                dig_cert_name: null
                analysis_start_time: "2016-06-02 08:34:40.513488+00"
                analysis_done_time: "2016-06-02 08:35:03.877626+00"
                source_url_rank: "-1"
                reputation_score: "35"
                microsoft_name: "None"
                has_behavior_log: "1"
                screen_shots:
                [
                3]
                      0:  "/analysis/897/qemu-results/screenshots-
                      winxp/screenshot_00.jpg"
                      1:  "/analysis/897/qemu-results/screenshots-
                      winxp/screenshot_01.jpg"
                      2:  "/analysis/897/qemu-results/screenshots-
                      winxp/screenshot_02.jpg"
                -
          }
          -
-
analysis_details:
{
          local_path: "/var/spool/c-icap/download/CI_TMPFP9jYz"
          file_md5_string: "7be866d691c3da79f51240bf8963e210"
          file_sha1_string: "1f707b2fe77691ee91aa5da0a326aec40182bb0d"
          file_sha256_string: "fada509542437360aeaa73a6256a9f1c88
          764e823f0f0a6a78fb66e419b5f389"
          file_size: "893977"
          file_type_string: "PE32 executable (GUI) Intel 80386, for MS
          Windows"
          file_suffix: "exe"
          mime_type_string: "FILE_UPLOAD"
          has_components: null
          packer_name: null
          malware_name: "TROJAN_YAKES.CY"
          malware_severity: "0.75"
          malware_category: "Trojan_Generic"
          malware_classname: "malware"
          has_static_detection: "1"
          has_behavioral_detection: "0"
          user_whitelisted: null
          JATP_whitelisted: null
          has_cnc: null
          dig_cert_name: null
          analysis_start_time: "2016-06-02 08:34:40.513488+00"
          analysis_done_time: "2016-06-02 08:35:03.877626+00"
          source_url_rank: "-1"
```

collector_id	ID of the Collector that processed the malicious traffic.

API Access: To demonstrate the behavior_details API from the Central Manager Web UI Incidents page: select an incident from the Incidents table then scroll down the page and click Downloads or Uploads tab. Expand the row to view details and with this action, you will see a call to the behavior_details API.
See also analysis_details on page 7

Example

```
curl -k -H "Authorization:7c71c218662411a5c857042053acca8f"
"https://10.2.20.37/admin/api.php?op=behavior_details" -d
event_id=672&collector_id=aaaa-bbbb-cccc-ddddd”
```

Authorization - The device user API key.
Obtain from Config > System Profiles > Users > Click on any User to obtain an API Key.

NEW: Additional JSON objects are available for obtaining third party ingestion vendor information:

memory_artifact_details This contains all the memory artifact strings that are recognized for the executable from which Juniper ATP Appliance is able to take a memory dump when certain Windows API calls are used. This corresponds to Memory Artifacts information displayed in the Juniper ATP Appliance Central Manager Web UI incident displays.

behavior_details uses an object called malware_actions that lists all the actions exhibited by detected malware. This corresponds to the Malware Traits information displayed in the Juniper ATP Appliance Central Manager Web UI incident displays.

Sample Output

```
curl  'https://10.2.25.21/admin/
api.php?op=behavior_details&sha1sum=c174ed87d658110b1596e30a827a810f0
e1bc102' -H 'Host: 10.2.25.24' -H
"Authorization:292fef0472b25dd9e1c032c69a4c9a18"  --insecure |
json_pp


{
  "behavior_details": {
"has_ivp": true,
"cnc_array": [
  {
    "host": "teredo.ipv6.microsoft.com",
    "string": "port 53 DNS",
    "response": ""
  }
],
"registry_changes": [
```

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.