

API Examples for Postman

- [Introduction](#)
- [Logon](#)
 - [Request](#)
 - [Response](#)
- [Read Devices](#)
 - [Request](#)
 - [Response](#)
- [Create Discovery](#)
 - [Request](#)
 - [Response](#)
- [Update Discovery](#)
 - [Request](#)
 - [Response](#)
- [Delete Discovery](#)
 - [Request](#)
 - [Response](#)

Introduction

Here are some examples for using the Open-Audit API via Postman.

When beginning a new request, we always logon and store the returned cookie for future use. In addition to the cookie, if we want to create a resource (Orgs, Locations, Credentials, Discoveries, et al) we need to provide an access token. An access token is generated with every request (except logon) and any of the last 20 (by default, settable in the configuration) will be accepted. You should always aim to use the last access token issued. An example token is in the Get Device List response, below.

Updated for Open-Audit 3.5.4 onward on 2021-11-29.

Logon

Request

Section			
URL	POST	http://localhost/omk/open-audit/logon	
Headers	Accept	application/json	
Body	Type	form-data	
	Key	username	admin
	Key	password	password

Response

```
{
  "message": "Authenticated as user admin",
  "ok": 1
}
```

Read Devices

Logon as above, then.

Request

Section		
---------	--	--

URL	GET	http://localhost/omk/open-audit/devices
Headers	Accept	application/json

Response

Note - restricted to one item in the data array, normally you will retrieve all items.

```
{
  "data": [
    {
      "attributes": {
        "locations.id": 1,
        "orgs.id": 1,
        "orgs.name": "Default Organisation",
        "system.class": "virtual server",
        "system.dbus_identifier": "",
        "system.description": "win 2008r2 with iis",
        "system.dns_domain": "",
        "system.dns_fqdn": "",
        "system.dns_hostname": "",
        "system.domain": "open-audit.local",
        "system.environment": "production",
        "system.first_seen": "2020-03-19 11:47:50",
        "system.form_factor": "Virtual",
        "system.fqdn": "win2012r2_web02.open-audit.local",
        "system.function": "",
        "system.hostname": "win2012r2_web02",
        "system.icon": "windows",
        "system.id": 19,
        "system.identification": "Virtual server from VMware, Inc.",
        "system.ip": "192.168.1.138",
        "system.ip_padded": "192.168.001.138",
        "system.last_seen": "2020-03-19 11:48:42",
        "system.last_seen_by": "audit",
        "system.location_id": 1,
        "system.manufacturer": "VMware, Inc.",
        "system.model": "VMware Virtual Platform",
        "system.name": "win2012r2_web02",
        "system.org_id": 1,
        "system.os_family": "Windows 2008",
        "system.os_group": "Windows",
        "system.os_name": "Microsoft Windows Server 2008 R2 Standard",
        "system.os_version": "6.1.7601",
        "system.serial": "VMware-56 4d 3a 1e b9 d5 13 17-fc 68 fb 3d e5 5a b6 77",
        "system.snmp_oid": "",
        "system.status": "production",
        "system.sysContact": "",
        "system.sysDescr": "",
        "system.sysLocation": "",
        "system.sysName": "",
        "system.sysObjectID": "",
        "system.sysUpTime": "",
        "system.type": "computer",
        "system.uuid": "1E3A4D56-D5B9-1713-FC68-FB3DE55AB677"
      },
      "id": 19,
      "links": {
        "self": "http://localhost/omk/open-audit/system/19"
      },
      "type": "system"
    }
  ],
  "included": [],
  "links": {
    "first": "http://localhost/omk/open-audit/devices?properties=default",
    "last": "http://localhost/omk/open-audit/devices?properties=default",
    "next": "http://localhost/omk/open-audit/devices?properties=default",
    "prev": "http://localhost/omk/open-audit/devices?properties=default",
  }
}
```

```

    "self": "http://localhost/omk/open-audit/devices"
  },
  "meta": {
    "access_token": "23652075c7660006c281bf33589620dc093bdbedf8eb7ed1223449a95748",
    "action": "collection",
    "baseurl": "http://localhost/omk/open-audit",
    "collection": "devices",
    "current": "y",
    "data_order": [
      "system.id",
      "system.uuid",
      "system.name",
      "system.ip",
      "system.hostname",
      "system.dns_hostname",
      "system.domain",
      "system.dns_domain",
      "system.dbus_identifier",
      "system.fqdn",
      "system.dns_fqdn",
      "system.description",
      "system.type",
      "system.icon",
      "system.os_group",
      "system.os_family",
      "system.os_name",
      "system.os_version",
      "system.manufacturer",
      "system.model",
      "system.serial",
      "system.form_factor",
      "system.status",
      "system.environment",
      "system.class",
      "system.function",
      "system.org_id",
      "system.location_id",
      "system.snmp_oid",
      "system.sysDescr",
      "system.sysObjectID",
      "system.sysUpTime",
      "system.sysContact",
      "system.sysName",
      "system.sysLocation",
      "system.first_seen",
      "system.last_seen",
      "system.last_seen_by",
      "system.identification",
      "orgs.name",
      "system.ip_padded",
      "orgs.id",
      "locations.id"
    ],
    "debug": false,
    "filter": [],
    "filtered": 19,
    "format": "json",
    "groupby": "",
    "header": "HTTP/1.1 200 OK",
    "heading": "Devices",
    "id": null,
    "ids": 0,
    "include": "",
    "limit": 1000,
    "offset": 0,
    "properties": "system.id,system.uuid,system.name,system.ip,system.hostname,system.dns_hostname,system.
domain,system.dns_domain,system.dbus_identifier,system.fqdn,system.dns_fqdn,system.description,system.type,
system.icon,system.os_group,system.os_family,system.os_name,system.os_version,system.manufacturer,system.model,
system.serial,system.form_factor,system.status,system.environment,system.class,system.function,system.org_id,
system.location_id,system.snmp_oid,system.sysDescr,system.sysObjectID,system.sysUpTime,system.sysContact,system.
sysName,system.sysLocation,system.first_seen,system.last_seen,system.last_seen_by,system.identification",

```

```

"query_parameters": [
  {
    "name": "properties",
    "operator": "",
    "value": "default"
  }
],
"query_string": "properties=default",
"received_data": [],
"request_method": "GET",
"requestor": "commercial",
"sort": "",
"sub_resource": "",
"sub_resource_id": 0,
"timestamp": "2020-03-24 13:47:56",
"timezone": "UTC +1000",
"total": 19,
"version": 1
}

```

Create Discovery

Logon as above, then request list of devices (or any available endpoint) so we can use the meta access_token in our request (see above response).

Request

Section			
URL	POST	http://localhost/omk/open-audit/discoveries	
Headers	Accept	application/json	
Body	Type	form-data	
	Key	data	<pre> { "access_token": "bcb3f959c14f0daf959e3de92e4213201a56bc205e31b63f35c3f9299670", "type": "discoveries", "attributes": { "description": "Subnet - 192.168.1.0/24", "match_options": "{\\"match_dbus\\":\\"\\",\\"match_dns_fgdn\\":\\"\\",\\"match_dns_hostname\\":\\"\\",\\"match_fgdn\\":\\"\\",\\"match_hostname\\":\\"\\",\\"match_hostname_dbus\\":\\"\\",\\"match_hostname_serial\\":\\"\\",\\"match_hostname_uuid\\":\\"\\",\\"match_ip\\":\\"\\",\\"match_ip_no_data\\":\\"\\",\\"match_mac\\":\\"\\",\\"match_mac_vmware\\":\\"\\",\\"match_serial\\":\\"\\",\\"match_serial_type\\":\\"\\",\\"match_sysname\\":\\"\\",\\"match_sysname_serial\\":\\"\\",\\"match_uuid\\":\\"\\"}", "name": "My Testing Discovery", "org_id": 1, "scan_options": "{\\"exclude_ip\\":\\"\\",\\"exclude_tcp_ports\\":\\"\\",\\"exclude_udp_ports\\":\\"\\",\\"filtered\\":\\"\\",\\"id\\":\\"1\\",\\"nmap_tcp_ports\\":\\"\\",\\"nmap_udp_ports\\":\\"\\",\\"open filtered\\":\\"\\",\\"ping\\":\\"\\",\\"service_version\\":\\"\\",\\"ssh_ports\\":\\"\\",\\"tcp_ports\\":\\"\\",\\"timeout\\":\\"\\",\\"timing\\":\\"\\",\\"udp_ports\\":\\"\\",\\"script_timeout\\":\\"\\",\\"snmp_timeout\\":\\"\\",\\"ssh_timeout\\":\\"\\",\\"wmi_timeout\\":\\"\\"}", "subnet": "192.168.1.0/24", "type": "subnet" } } </pre>

Response

Note, generated from a discoveries read. The actual output should be almost identical.

```

{
  "data":
  [

```

```

{
  "attributes":
  {
    "ad_domain": "",
    "ad_server": "",
    "cloud_id": 1,
    "cloud_name": "",
    "command_options": "",
    "description": "Subnet - 192.168.1.0/24",
    "devices_assigned_to_location": null,
    "devices_assigned_to_org": null,
    "discard": "n",
    "duration": "00:00:00",
    "edited_by": "Administrator",
    "edited_date": "2021-11-29 13:16:53",
    "id": 3,
    "ip_all_count": 0,
    "ip_audited_count": 0,
    "ip_discovered_count": 0,
    "ip_responding_count": 0,
    "ip_scanned_count": 0,
    "last_finished": "2000-01-01 00:00:00",
    "last_run": "2000-01-01 00:00:00",
    "match_options":
    {
      "match_dbus": "",
      "match_dns_fqdn": "",
      "match_dns_hostname": "",
      "match_fqdn": "",
      "match_hostname": "",
      "match_hostname_dbus": "",
      "match_hostname_serial": "",
      "match_hostname_uuid": "",
      "match_ip": "",
      "match_ip_no_data": "",
      "match_mac": "",
      "match_mac_vmware": "",
      "match_serial": "",
      "match_serial_type": "",
      "match_sysname": "",
      "match_sysname_serial": "",
      "match_uuid": ""
    },
    "name": "My Testing Discovery",
    "network_address": "",
    "org_id": 1,
    "orgs.id": 1,
    "scan_options":
    {
      "exclude_ip": "",
      "exclude_tcp_ports": "",
      "exclude_udp_ports": "",
      "filtered": "",
      "id": "1",
      "nmap_tcp_ports": "",
      "nmap_udp_ports": "",
      "open|filtered": "",
      "ping": "",
      "script_timeout": "",
      "service_version": "",
      "snmp_timeout": "",
      "ssh_ports": "",
      "ssh_timeout": "",
      "tcp_ports": "",
      "timeout": "",
      "timing": "",
      "udp_ports": "",
      "wmi_timeout": ""
    },
    "seed_ip": "",
    "seed_ping": "y",

```

```

        "seed_restrict_to_private": "y",
        "seed_restrict_to_subnet": "y",
        "status": "",
        "subnet": "192.168.1.0/24",
        "system.id": 0,
        "system_id": 0,
        "type": "subnet"
    },
    "id": 3,
    "links":
    {
        "self": "http://dev.local/omk/open-audit/discoveries/3"
    },
    "type": "discoveries"
}
],
"included": [],
"issues": [],
"meta":
{
    "access_token": "ef4421add7e6f2741a2830a1b0262d3b678cc33efdacdd9442d5a871f474",
    "action": "read",
    "as_at": "",
    "baseurl": "http://dev.local/omk/open-audit",
    "collection": "discoveries",
    "current": "y",
    "data_order":
    [
        "discoveries.id",
        "discoveries.name",
        "discoveries.org_id",
        "discoveries.description",
        "discoveries.type",
        "discoveries.subnet",
        "discoveries.seed_ip",
        "discoveries.seed_restrict_to_subnet",
        "discoveries.seed_restrict_to_private",
        "discoveries.seed_ping",
        "discoveries.ad_domain",
        "discoveries.ad_server",
        "discoveries.devices_assigned_to_org",
        "discoveries.devices_assigned_to_location",
        "discoveries.network_address",
        "discoveries.system_id",
        "discoveries.scan_options",
        "discoveries.match_options",
        "discoveries.command_options",
        "discoveries.discard",
        "discoveries.last_run",
        "discoveries.last_finished",
        "discoveries.duration",
        "discoveries.status",
        "discoveries.ip_all_count",
        "discoveries.ip_responding_count",
        "discoveries.ip_scanned_count",
        "discoveries.ip_discovered_count",
        "discoveries.ip_audited_count",
        "discoveries.cloud_id",
        "discoveries.cloud_name",
        "discoveries.edited_by",
        "discoveries.edited_date",
        "orgs.id",
        "system.id"
    ],
    "debug": false,
    "filter": [],
    "filtered": 1,
    "format": "json",
    "groupby": "",
    "header": "HTTP/1.1 200 OK",
    "heading": "Discoveries",

```

```

    "id": 3,
    "include": "",
    "limit": 1000,
    "nmap_version": 7,
    "offset": 0,
    "properties": ".*",
    "query_parameters": [],
    "query_string": "",
    "received_data": [],
    "request_method": "GET",
    "requestor": "commercial",
    "server_app_version": "4.3.0",
    "server_platform": "Debian GNU/Linux 9 (stretch)",
    "sort": "",
    "sub_resource": "",
    "timestamp": "2021-11-29 13:24:45",
    "timezone": "UTC +1000",
    "total": 1,
    "version": 1
  }
}

```

Update Discovery

Logon as above, then.

Request

Section			
URL	PATCH	http://localhost/omk/open-audit/discoveries/5	
Headers	Accept	application/json	
Body	Type	x-www-form-urlencoded	
	Key	data	<pre> { "id": 5, "type": "discoveries", "attributes": { "name": "My New Name OMK" } } </pre>

Response

Note - generated from pre 3.5.4. Attribute outputs will be as above for 3.5.4 onward.

```

{
  "data": [
    {
      "attributes": {
        "description": "Subnet - 192.169.1.0/24",
        "devices_assigned_to_location": null,
        "devices_assigned_to_org": null,
        "discard": "n",
        "duration": "00:00:00",
        "edited_by": "Administrator",
        "edited_date": "2020-03-24 14:13:36",
        "id": 5,
        "ip_all_count": 0,
        "ip_audited_count": 0,
        "ip_discovered_count": 0,
        "ip_responding_count": 0,
        "ip_scanned_count": 0,
        "last_finished": "2000-01-01 00:00:00",

```

```

        "last_run": "2000-01-01 00:00:00",
        "name": "My New Name OMK",
        "network_address": "http://127.0.0.1/open-audit/",
        "options": "",
        "org_id": 1,
        "orgs.id": 1,
        "other": {
            "nmap": {
                "discovery_scan_option_id": "1",
                "exclude_ip": "",
                "exclude_tcp_ports": "",
                "exclude_udp_ports": "",
                "filtered": "n",
                "nmap_tcp_ports": "0",
                "nmap_udp_ports": "0",
                "ping": "y",
                "service_version": "n",
                "ssh_ports": "22",
                "tcp_ports": "22,135,62078",
                "timeout": "0",
                "timing": "4",
                "udp_ports": "161"
            },
            "subnet": "192.169.1.0/24"
        },
        "status": "",
        "system.id": 0,
        "system_id": 0,
        "type": "subnet"
    },
    "id": 5,
    "links": {
        "self": "/omk/open-audit/discoveries/5"
    },
    "type": "discoveries"
}
],
"errors": [],
"included": [],
"links": {
    "first": null,
    "last": null,
    "next": null,
    "prev": null,
    "self": "http://localhost/omk/open-audit/discoveries/5"
},
"meta": {
    "access_token": "47049142d113e4e316ae4219afdf54d6a6d034ff779a42fd5198a720da2e",
    "action": "update",
    "baseurl": "http://localhost/omk/open-audit",
    "collection": "discoveries",
    "current": "y",
    "data_order": [
        "discoveries.id",
        "discoveries.name",
        "discoveries.org_id",
        "discoveries.description",
        "discoveries.type",
        "discoveries.devices_assigned_to_org",
        "discoveries.devices_assigned_to_location",
        "discoveries.network_address",
        "discoveries.system_id",
        "discoveries.options",
        "discoveries.discard",
        "discoveries.last_run",
        "discoveries.last_finished",
        "discoveries.duration",
        "discoveries.status",
        "discoveries.ip_all_count",
        "discoveries.ip_responding_count",
        "discoveries.ip_scanned_count",
    ]
}

```



```

        "discoveries.ip_discovered_count",
        "discoveries.ip_audited_count",
        "discoveries.edited_by",
        "discoveries.edited_date",
        "orgs.id",
        "system.id",
        "other.subnet",
        "other.nmap"
    ],
    "debug": false,
    "filter": [],
    "filtered": "",
    "format": "json",
    "groupby": "",
    "header": "HTTP/1.1 200 OK",
    "heading": "Discoveries",
    "id": 5,
    "ids": 0,
    "include": "",
    "limit": 1000,
    "offset": 0,
    "properties": "*",
    "query_parameters": [],
    "query_string": "",
    "received_data": {
        "attributes": {
            "id": 5,
            "name": "My New Name OMK"
        },
        "id": 5,
        "type": "discoveries"
    },
    "request_method": "PATCH",
    "requestor": "",
    "sort": "",
    "sub_resource": "",
    "sub_resource_id": 0,
    "timestamp": "2020-03-24 14:13:36",
    "timezone": "UTC +1000",
    "total": 0,
    "version": 1
}

```

Delete Discovery

Logon as above, then.

Request

Section		
URL	DELETE	http://localhost/omk/open-audit/discoveries/5
Headers	Accept	application/json

Response

```
{
  "meta": {
    "access_token": "530d34dc6304ebd361d088d7831e4ce9d276ac8a4826837bdf36e8e84c87",
    "action": "delete",
    "baseurl": "http://localhost/open-audit/",
    "collection": "discoveries",
    "current": "Y",
    "debug": false,
    "filtered": "",
    "format": "json",
    "groupby": "",
    "header": "HTTP/1.1 200 OK",
    "id": 5,
    "ids": 0,
    "include": "",
    "limit": 1000,
    "offset": 0,
    "properties": "*",
    "query_string": "",
    "request_method": "DELETE",
    "requestor": "",
    "sort": "",
    "sub_resource": "",
    "sub_resource_id": 0,
    "total": 0,
    "timestamp": "2020-03-24 14:22:38",
    "timezone": "UTC +1000",
    "version": 1,
    "filter": [],
    "query_parameters": [],
    "received_data": [],
    "heading": "Discoveries",
    "data_order": []
  },
  "links": {
    "self": "http://localhost/open-audit/index.php/discoveries/5",
    "first": null,
    "last": null,
    "next": null,
    "prev": null
  },
  "included": [],
  "data": [
    {
      "type": "discoveries"
    }
  ]
}
```