API REQUEST APPROVAL

How to retrieve and approve requests through the API

Table of Contents

Introduction

The purpose of this document is to demonstrate, how requests can be retrieved and approve from an external system. The goal is to empty the request queue on an interval and approve or deny requests that are already stored in the external system. The scenario could be to make a recurring job in ServiceNOW and then add buttons on tickets to approve or deny requests.

The public REST API is explained on this page: https://www.adminbyrequest.com/PublicAPI

The API exposes the same features as you can find in the portal and the mobile app. There are three areas: Auditlog, Requests and Inventory. The details and fields of each API can be found here:
https://www.adminbyrequest.com/Docs/API/Auditlog.aspx
https://www.adminbyrequest.com/Docs/API/Requests.aspx
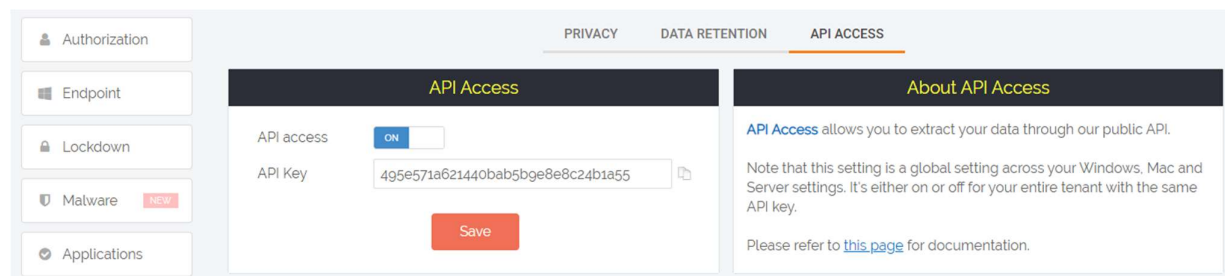https://www.adminbyrequest.com/Docs/API/Inventory.aspx

Set up

The first step is to generate an API key. By default, your tenant data are not exposed to the public API. You have to generate a new key and use to get the data. Note that the API has brute force protections in place, so it's safe to open the API.

Once we have this key, we can make a call to the API using the API key as the "apikey" header. We will be using the free Postman (https://www.postman.com/) to demonstrate the use. Here we have called the Auditlog API to get entries.

```
206      "ElevatedApplications": [
207          {
208              "Path": "C:\\Program Files\\totalcmd",
209              "File": "TOTALCMD64.EXE",
210              "Name": "Total Commander"
211          }
212      ],
213      "ScanResults": [],
214      "ID": 51134241,
215      "Type": "Run As Admin",
216      "TypeCode": 0,
217      "Status": "Finished",
218      "StatusCode": 2,
219      "Application": {
220          "File": "TOTALCMD64.EXE",
221          "Name": "Total Commander",
222          "Vendor": "Ghisler Software GmbH",
223          "Version": "9.22a",
224          "SHA256": "600D3BF7766EF846DB0B8C17971FC5C77D5B37F7B3AE77220E20E752624EF4EF",
225          "ScanResult": "Clean",
226          "ScanResultCode": 0,
227          "Threat": null,
228          "VirusTotalLink": "https://www.virustotal.com/latest-scan/600D3BF7766EF846DB0B8C17971FC5C77D5B37F7B3AE77220E20E752624EF4EF",
229          "Preapproved": false
230      },
```

Getting requests

Requests will appear in the "Requests" top menu in the portal as shown here:

To get a list of pending requests for approval, we need to call the Requests API indicating that we are only interested in "Pending" states. The URL is then (dc1api for Europe and dc2api for US tenants):
https://dc1api.adminbyrequest.com/requests?status=pending

This will give us a list in json format with all the same information that is shown in the portal:

GET ∨ https://dc1api.adminbyrequest.com/requests?status=pending **Send**

Params ● Auth ● Headers (7) Body Pre-req. Tests Settings Cookies

Headers 👁 6 hidden

	KEY	VALUE	DESCRIP ○○○	Bulk Edit	Presets ∨
☑	apikey	b863e0ffc89948f98415e2622afa66f3			
	Key	Value	Description		

Body Cookies Headers (9) Test Results 🌐🔒 200 OK 519 ms 1.31 KB Save Response ∨

Pretty Raw Preview Visualize JSON ∨

```
1   [
2       {
3           "scanResults": [],
4           "id": 65430027,
5           "traceNo": "46142793",
6           "settingsName": "Global",
7           "type": "Run As Admin",
8           "typeCode": 0,
9           "status": "Pending approval",
10          "statusCode": 4,
11          "application": {
12              "file": "cmd.exe",
13              "name": "Windows Command Processor",
14              "vendor": "Microsoft Corporation",
15              "version": "10.0.21390.1 (WinBuild.160101.0800)",
16              "sha256": "61B4C38792F586995F8E1B8E935B2DE1D6C7941A71A57FC1A1269D2E1E3164CD",
17              "scanResult": "Clean",
18              "scanResultCode": 0,
19              "threat": null,
20              "virustotalLink": "https://www.virustotal.com/latest-scan/
                    61B4C38792F586995F8E1B8E935B2DE1D6C7941A71A57FC1A1269D2E1E3164CD"
21          },
22          "user": {
23              "account": "AZUREAD\\FASTTRACKSOFTWARESUP",
24              "fullName": "FastTrack Software Support",
25              "email": "support@fasttracksoftware.com",
26              "phone": "333.333.3333"
27          },
```

Approving requests

Notice that each request has an "id" field. This field is used to perform an approve or deny request as explained in the documentation here: https://www.adminbyrequest.com/RequestsAPI

Resources

https://dc1api.adminbyrequest.com/requests	🗋	Returns an array of requests	GET
https://dc1api.adminbyrequest.com/requests/{id}	🗋	Returns one request	GET
https://dc1api.adminbyrequest.com/requests/{id}	🗋	Approve request. If request is already approved or started, nothing happens	PUT
https://dc1api.adminbyrequest.com/requests/{id}	🗋	Deny request. If request is already approved or started, nothing happens	DELETE

So all we have to do is to make a simple PUT request with the ID:

| PUT ⌄ | https://dc1api.adminbyrequest.com/requests/65430027 | **Send** ⌄ |

... and the request is now approved and the user is notified accordingly. It's that simple!

Pending Approval Requests

Users will be notified by email of approval or denial. Requests will drop out of the list after two weeks. If the user doesn't use an approve request within two weeks, the approval will also expire. You can approve or deny requests using the mobile app also.

| PENDING (0) | APPROVED (1) | DENIED (1) | QUARANTINED (0) |

08-06-2021 11:25:27 • FastTrack Software Support
Email: support@fasttracksoftware.com • Phone: 333,333,3333 • Computer: FTWIN10-AALBORG-DENMARK
• Requesting to run Windows Command Processor 10.0.21390.1 (WinBuild.160101.0800) from Microsoft Corporation
• File: cmd.exe • Metadefender: Clean • Virustotal: Run check
• Reason: Need to run a cmd

Deny

Keeping state

So how do you only get new requests? The easiest way is to store the highest id you have received before and use this for the next calls. Here are the filters for the Requests API:

Filters (query string parameters)		
status	Only get request of a certain type (possible values: Pending, Denied, Approved, Quarantined)	int
startid	The starting ID you wish to receive. Can be used for incremental offload of data to your own system	int
take	Maximum number of resources to return. Default is 50 to preserve bandwidth, maximum is 1000. For queries with more than 1000 records, pagination is mandatory	int
last	Entries are retrieve in ascending order. Last returns the latest X number of entries in descending order. Maximum is 1000. Take and startid cannot be combined with last.	int
wantscandetails	Use this filter, if you wish to receive detailed lists of scan results. The default is to give you the overall result only	bit
reason	Can be passed when denying a request	string
deniedby	Can be passed when denying a request - this has to be an email address that matches a portal user, otherwise it will be ignored	string
approvedby	Can be passed when approving a request - this has to be an email address that matches a portal user, otherwise it will be ignored	string

- Example url to get one pending request: https://dc1api.adminbyrequest.com/requests?status=pending&take=1&wantscandetails=1
- Pagination works by using the last id in the list and feeding it as startid in the next query
- To copy new data to your own system, we recommend to store the highest id (last entry in list) you have retrieved from a previous call and pass this number plus 1 as "startid"

Let's say the last request we received was 65430930. Then we add one (since we already received 65430930) and use as startid, meaning that we only want to see any requests with an id higher than 65430930:

| GET ⌄ | https://dc1api.adminbyrequest.com/requests?startid=65430931 | **Send** ⌄ |

Questions?

Feel free to contact us. If you do not have a direct contact at FastTrack Software, feel free to create a support ticket at https://www.adminbyrequest.com/Support