ninja

Public API *beta*

Ver. 0.1.2

Table of Contents

6. Appendix

6.1 Enumerations

7. Changelog

7.1 v0.1.2

1. Introduction

1.1 REST

The NinjaRMM API is a REST API which uses the already existing HTTP methods to create (POST), read (GET), change (PUT) or delete (DELETE) single items or a collection of items. The following table shows the general use cases for these HTTP methods.

	GET	PUT	POST	DELETE
Collection	retrieve list	-	-	-
Single Item	retrieve item	create item	update item	delete item

1.2 Date format

All dates must be in one of the RFC 2616 formats (http://www.ietf.org/rfc/rfc2616.txt).

Example

```
Sun, 01 May 2016 06:51:10 GMT
```

1.3 API Hostnames

The NinjaRMM API is available at the following hostnames depending on your location:

Location	Preferred Hostname
US	api.ninjarmm.com
EU	eu-api.ninjarmm.com

2. Authentication

2.1 Overview

Authentication is the process of proving your identity to the system. Requests are allowed or denied in part based on the identity of the requester. As a developer, you'll be making requests that invoke these privileges, so you'll need to prove your identity to the system by authenticating your requests. This section shows you how.

The NinjaRMM REST API uses a custom HTTP scheme based on a keyed-HMAC (Hash Message Authentication Code) for authentication. To authenticate a request, you first concatenate selected elements of the request to form a string. You then use your API secret access key to calculate the HMAC of that string. Informally, we call this process "signing the request," and we call the output of the HMAC algorithm the signature, because it simulates the security properties of a real signature. Finally, you add this signature as a parameter of the request by using the syntax described in this section.

When the system receives an authenticated request, it fetches the API secret access key that you claim to have and uses it in the same way to compute a signature for the message it received. It then compares the signature it calculated against the signature presented by the requester. If the two signatures match, the system concludes that the requester must have access to the API secret access key and therefore acts with the authority of the principal to whom the key was issued. If the two signatures do not match, the request is dropped and the system responds with an error message.

Example Authenticated Request

```
GET /v1/customers HTTP/1.1
Host: api.ninjarmm.com
Date: Sun, 01 May 2016 06:51:10 GMT
Authorization: NJ TF4STGMDR4H7AEXAMPLE:rEZWuXR0X1wX3autLTHIl2zX98I=
```

2.2 The Authentication Header

Using the HTTP `Authorization` header is the most common method of providing authentication information. All object operations use the `Authorization` request header to provide authentication information.

The NinjaRMM REST API uses the standard HTTP `Authorization` header to pass authentication information. (The name of the standard header is unfortunate because it carries authentication information, not authorization.) Under the NinjaRMM authentication scheme, the Authorization header has the following form:

```
Authorization: NJ AccessKeyId:Signature
```

Developers are issued an access key ID and secret access key when they register. For request authentication, the *`AccessKeyId`* element identifies the access key ID that was used to compute the signature and, indirectly, the developer making the request.

The *`Signature`* element is the RFC 2104 HMAC-SHA1 of selected elements from the request, and so the *`Signature`* part of the Authorization header will vary from request to request. If the request signature calculated by the system matches the *`Signature`* included with the request, the requester will have demonstrated possession of the secret access key. The request will then be processed under the identity, and with the authority, of the developer to whom the key was issued.

Following is pseudogrammar that illustrates the construction of the request *`Signature`*. (In the example, `\n` means the Unicode code point `U+000A`, commonly called newline).

```
Signature = Base64( HMAC-SHA1( YourSecretAccessKeyID, Base64( UTF-8-Encoding-
Of( StringToSign ) ) ) );

StringToSign = HTTP-Verb + "\n" +
               Content-MD5 + "\n" +
               Content-Type + "\n" +
               Date + "\n" +
               CanonicalizedResource;
```

HMAC-SHA1 is an algorithm defined by RFC 2104 - Keyed-Hashing for Message Authentication . The algorithm takes as input two byte-strings, a key and a message. For NinjaRMM API request authentication, use your secret access key (*YourSecretAccessKeyID*) as the key, and the UTF-8 encoding of the *StringToSign* as the message. The output of HMAC-SHA1 is also a byte string, called the digest. The *Signature* request parameter is constructed by Base64 encoding this digest.

2.3 Time Stamp Requirement

A valid time stamp (using either the HTTP `Date` header or an *x-nj-date* alternative) is mandatory for authenticated requests. Furthermore, the client timestamp included with an authenticated request must be within 15 minutes of the NinjaRMM system time when the request is received. If not, the request will fail with the *RequestTimeTooSkewed* error code. The intention of these restrictions is to limit the possibility that intercepted requests could be replayed by an adversary. For stronger protection against eavesdropping, use the HTTPS transport for authenticated requests.

Some HTTP client libraries do not expose the ability to set the `Date` header for a request. If you have trouble including the value of the 'Date' header in the canonicalized headers, you can set the timestamp for the request by using an `'x-nj-date'` header instead. The value of the `x-nj-date` header must be in one of the RFC 2616 formats (http://www.ietf.org/rfc/rfc2616.txt). When an `x-nj-date` header is present in a request, the system will ignore any `Date` header when computing the request signature. Therefore, if you include the `x-nj-date` header, use the empty string for the Date when constructing the *StringToSign*. See the next section for an example.

2.4 Authentication Example

The examples in this section use the (non-working) credentials in the following table.

Parameter	Value
AccessKeyId	TF4STGMDR4H7AEXAMPLE
SecretAccessKey	eh14c4ngchhu6283he03j6o7ar2fcuca0example

In the example *`StringToSign`*, formatting is not significant, and `\n` means the Unicode code point `U+000A`, commonly called newline.

Example Authenticated Request

Request

```
GET /v1/customers HTTP/1.1
Host: api.ninjarmm.com
Date: Sun, 01 May 2016 06:51:10 GMT
Authorization: NJ TF4STGMDR4H7AEXAMPLE:rEZWuXR0X1wX3autLTHIl2zX98I=
```

StringToSign

```
GET\n
\n
\n
Sun, 01 May 2016 06:51:10 GMT\n
/v1/customers
```

3. API Functions

3.1 Ping

Check API availability and verify your request credentials. Returns a 204 HTTP status code for a valid request.

3.2 Customers

3.2.1 GET /v1/customers

Retrieve a list of all available customers.

Example Response


```
[{
        "id": 1,
        "name": "ABC Consultants",
        "description": "IT repair shop"
}, {
        "id": 2,
        "name": "Magic IT People",
        "description": "Quick IT Helpdesk"
}]
```


3.2.2 GET /v1/customers/<id>

Retrieve a specific customer.

Example Response


```
{
        "id": 1,
        "name": "ABC Consultants",
        "description": "IT repair shop"
}
```

3.3 Devices

3.3.1 GET /v1/devices

Retrieve a list of all available devices.

Example Response


```
 [
  {
    "id": 4460,
    "type": "AGENT",
    "sub_type": "AGENT_GENERAL",
    "role": "WINDOWS_WORKSTATION",
    "customer_id": 357,
    "parent_device_id": null,
    "display_name": "REBEL-ALIEN",
    "dns_name": "rebel-alien",
    "system_name": "REBEL-ALIEN",
    "netbios_name": "REBEL-ALIEN",
    "last_online": "Wed, 01 Jun 2016 08:23:31 GMT",
    "last_update": "Wed, 01 Jun 2016 08:23:29 GMT",
    "last_logged_in_user": "REBEL-ALIEN\\the_r_000",
    "ninja_url": "https://app.ninjarmm.com/#/deviceDashboard/4460/overview",
    "remote_control_url":
"teamviewer10://control?device=d123456789&authorization=password",
    "ip_addresses": [
      "192.168.142.1",
      "fe80::6d58:dd4e:313d:436b",
      "192.168.116.1",
      "fe80::24cd:799c:afe8:5190",
      "192.168.1.71",
      "fe80::48a7:9c5c:a2a3:33e9",
      "2602:30a:c7e9:a120:e4f0:4be:c13a:242b",
      "2602:30a:c7e9:a120:48a7:9c5c:a2a3:33e9"
    ],
    "mac_addresses": [
      "00:50:56:C0:00:08",
      "00:50:56:C0:00:01",
      "20:47:47:C5:23:33"
    ],
    "memory": {
      "capacity": 17179869184
    },
    "os": {
      "manufacturer": "Microsoft Corporation",
      "name": "Microsoft Windows 10 Home",
      "os_architecture": "64-bit",
      "last_boot_time": "Tue, 31 May 2016 18:36:52 GMT"
    },
    "system": {
      "manufacturer": "Alienware",
```

```
      "name": "REBEL-ALIEN",
      "model": "Alienware 15",
      "dns_host_name": "rebel-alien",
      "bios_serial_number": "9547Z52",
      "domain": "WORKGROUP"
    },
    "processor": {
      "name": "Intel(R) Core(TM) i7-4720HQ CPU @ 2.60GHz",
      "architecture": "x64",
      "num_cores": 4,
      "num_logical_cores": 8,
      "current_clock_speed": 2601000000,
      "max_clock_speed": 2601000000
    },
    "disks": [{
      "name": "C:",
      "type": "Local Disk",
      "file_system": "NTFS",
      "serial_number": "876457785",
      "volume_label": "",
      "capacity": 42842714112,
      "free_space": 3738173440
    }]
  },
  {
    "id": 4823,
    "type": "NMS_TARGET",
    "sub_type": "NMS_TARGET_GENERAL",
    "role": "NMS_PRINTER",
    "customer_id": 435,
    "parent_device_id": 4822,
    "display_name": "172.16.1.20",
    "dns_name": null,
    "system_name": null,
    "netbios_name": null,
    "last_online": "Tue, 10 May 2016 22:58:24 GMT",
    "last_update": "Tue, 10 May 2016 22:58:24 GMT",
    "ninja_url": "https://app.ninjarmm.com/#/nmsDashboard/4823/overview",
    "ip_addresses": [
      "172.16.1.20"
    ],
    "mac_addresses": [
      "00:F0:56:C0:AB:08",
    ]
  },
  {
    "id": 4847,
    "type": "NMS_SERVER",
    "sub_type": "NMS_SERVER_GENERAL",
    "role": "NMS_NETWORK_MANAGEMENT_AGENT",
    "customer_id": 434,
    "parent_device_id": null,
    "display_name": "JERRYPC",
    "dns_name": null,
    "system_name": "JERRYPC",
    "netbios_name": null,
    "last_online": "Mon, 16 May 2016 19:08:42 GMT",
```

```
    "last_update": "Mon, 16 May 2016 19:08:42 GMT",
    "ninja_url": "https://app.ninjarmm.com/#/nmsDashboard/4847/overview",
    "remote_control_url":
"teamviewer10://control?device=d123456789&authorization=password",
    "ip_addresses": [
      "172.16.1.24"
    ],
    "mac_addresses": [
      "01:F0:56:C0:FB:08",
    ]
  },
  {
    "id": 4342,
    "type": "MONITOR_SERVER",
    "sub_type": "MONITOR_SERVER_GENERAL",
    "role": null,
    "customer_id": 368,
    "parent_device_id": null,
    "display_name": "Ping Test",
    "dns_name": null,
    "system_name": "Ping Test",
    "netbios_name": "Ping Test",
    "last_online": "Mon, 16 May 2016 19:03:52 GMT",
    "last_update": "Mon, 16 May 2016 19:03:52 GMT",
    "ninja_url": "https://app.ninjarmm.com/#/cloudMonitorDashboard/4342"
  }
]
```


3.3.2 GET /v1/devices/<id>

Retrieve a specific device.

Example Response


```
{
    "id": 4460,
    "type": "AGENT",
    "sub_type": "AGENT_GENERAL",
    "role": "WINDOWS_WORKSTATION",
    "customer_id": 357,
    "parent_device_id": null,
    "display_name": "REBEL-ALIEN",
    "dns_name": "rebel-alien",
    "system_name": "REBEL-ALIEN",
    "netbios_name": "REBEL-ALIEN",
    "last_online": "Wed, 01 Jun 2016 08:23:31 GMT",
    "last_update": "Wed, 01 Jun 2016 08:23:29 GMT",
    "last_logged_in_user": "REBEL-ALIEN\\the_r_000",
    "ninja_url": "https://app.ninjarmm.com/#/deviceDashboard/4460/overview",
    "ip_addresses": [
      "192.168.142.1",
```

```
      "fe80::6d58:dd4e:313d:436b",
      "192.168.116.1",
      "fe80::24cd:799c:afe8:5190",
      "192.168.1.71",
      "fe80::48a7:9c5c:a2a3:33e9",
      "2602:30a:c7e9:a120:e4f0:4be:c13a:242b",
      "2602:30a:c7e9:a120:48a7:9c5c:a2a3:33e9"
    ],
    "mac_addresses": [
      "00:50:56:C0:00:08",
      "00:50:56:C0:00:01",
      "20:47:47:C5:23:33"
    ],
    "memory": {
      "capacity": 17179869184
    },
    "os": {
      "manufacturer": "Microsoft Corporation",
      "name": "Microsoft Windows 10 Home",
      "os_architecture": "64-bit",
      "last_boot_time": "Tue, 31 May 2016 18:36:52 GMT"
    },
    "system": {
      "manufacturer": "Alienware",
      "name": "REBEL-ALIEN",
      "model": "Alienware 15",
      "dns_host_name": "rebel-alien",
      "bios_serial_number": "9547Z52",
      "domain": "WORKGROUP"
    },
    "processor": {
      "name": "Intel(R) Core(TM) i7-4720HQ CPU @ 2.60GHz",
      "architecture": "x64",
      "num_cores": 4,
      "num_logical_cores": 8,
      "current_clock_speed": 2601000000,
      "max_clock_speed": 2601000000
    },
    "disks": [{
      "name": "C:",
      "type": "Local Disk",
      "file_system": "NTFS",
      "serial_number": "876457785",
      "volume_label": "",
      "capacity": 42842714112,
      "free_space": 3738173440
    }],
    "software": [{
      "name": "Mozilla Firefox 45.0.1 (x86 en-US)",
      "publisher": "Mozilla",
      "version": "45.0.1",
      "install_date": "20160410",
      "size": 92580864
    }, {
      "name": "Google Chrome",
      "publisher": "Google, Inc.",
      "version": "49.0.2623.112",
```

```
      "install_date": "20160410",
      "size": 53498880
    }, {
      "name": "Microsoft .NET Framework 4.5.2",
      "publisher": "Microsoft Corporation",
      "version": "4.5.51209",
      "install_date": "20160229",
      "size": 40685568
    }]
}
```


3.4 Alerts

3.4.1 GET /v1/alerts

Retrieve list of alerts. Alert responses will contain both device and customer information.


```
[
  {
    "id": 457115,
    "type": "MONITOR",
    "status": "WINDOWS_SERVICE_STOPPED",
    "message": "'WinDefend':'Windows Defender Service' stopped.",
    "severity": null,
    "result": null,
    "source": null,
    "os_user_name": null,
    "timestamp": "Sun, 15 May 2016 22:11:39 GMT",
    "can_reset": false,
    "device": {
      "id": 1743,
      "type": "AGENT",
      "sub_type": "AGENT_GENERAL",
      "role": "WINDOWS_WORKSTATION",
      "customer_id": 107,
      "parent_device_id": null,
      "display_name": "DESKTOP1",
      "dns_name": "DESKTOP-MHOMN54",
      "system_name": "DESKTOP-MHOMN54",
      "netbios_name": "DESKTOP-MHOMN54",
      "last_online": "Wed, 18 May 2016 17:07:19 GMT",
      "last_update": "Wed, 18 May 2016 17:07:19 GMT"
    },
    "customer": {
```

```
      "id": 107,
      "name": "Ninja TEST",
      "description": "Test customer"
    }
  }
]
```

3.4.2 GET /v1/alerts/since/<id>

Retrieve alerts since last known alert ID (<id>). Same schema as **/v1/alerts**

3.4.3 DELETE /v1/alerts/<id>

Reset an alert. Only alerts with `can_reset` can be deleted. Returns a 204 HTTP status code for a successful request.

4. Limits

4.1 List API

All list APIs will be limited to 10 requests for every 10-minute interval.

4.2 Entity API

All entity APIs will be limited to not less than 10 requests per minute.

5. Errors

5.1 Error Responses

The server will return an `error` with a descriptive `error_message` if it is unable to process your request successfully. The error message will be accompanied with an appropriate 4xx/5xx HTTP status code.

Response Fields

- error – A short string for each error type
- error_description – A human readable description of the error with details
- error_code – A unique numeric code for each error type

Types of Errors

- invalid_header – A syntactically incorrect request header was found
- missing_header – Request is missing a required header
- skewed_time – Request date is too far from current time
- not_authenticated – Invalid *`AccessKeyId`* or incorrect *`Signature`*
- invalid_id – Requested entity does not exist
- rate_limit_exceeded – A resource has been requested beyond its allowed limits

6. Appendix

6.1 Enumerations

All devices have a *type* and a *sub_type*. An optional *role* may be present where applicable. The possible values for these properties and their descriptions are listed below.

Type

- AGENT – All Windows and Mac devices
- MONITOR_SERVER – All cloud monitor devices
- NMS_SERVER – Network Management Agent responsible for monitoring your network endpoints
- NMS_TARGET – Network endpoints monitored by the Network Management Agent

SubType

- AGENT_GENERAL – All AGENT `type` devices will have a `sub_type` value of `AGENT_GENERAL`
- MONITOR_SERVER_GENERAL – All cloud monitor devices excluding email monitors
- MONITOR_SERVER_EMAIL – All Email cloud monitor devices
- NMS_SERVER_GENERAL – All NMS_SERVER `type` devices will have a `sub_type` value of `NMS_SERVER_GENERAL`
- NMS_TARGET_GENERAL – All NMS_TARGET `type` devices will have a `sub_type` value of `NMS_TARGET_GENERAL`

Role

All `AGENT` devices will have their *role* set to one of the following values based upon their operating system and device role.

- WINDOWS_SERVER
- WINDOWS_WORKSTATION
- MAC
- EFOLDER_IMAGEMANAGER_SERVICE

All `NMS_SERVER` devices will have their *role* set to the following.

- NMS_NETWORK_MANAGEMENT_AGENT

All `NMS_TARGET` devices will have their *role* set to one of the following values based upon device role.

- NMS_SWITCH
- NMS_ROUTER
- NMS_FIREWALL
- NMS_PRIVATE_NETWORK_GATEWAY
- NMS_PRINTER
- NMS_SCANNER
- NMS_DIAL_MANAGER
- NMS_WAP
- NMS_IPSLA
- NMS_COMPUTER
- NMS_VM_HOST
- NMS_APPLIANCE
- NMS_OTHER
- NMS_SERVER
- NMS_PHONE
- NMS_VIRTUAL_MACHINE

7. Changelog

7.1 v0.1.2

- Device APIs now return *disks*
- Alert APIs was added