StrandVision.com

API 1.0

Documentation

Tuesday, April 18, 2023

Table of Contents

Revision History

4/18/2023.....Initial Release

Overview

Questions / Behavior

We saw this from the Varnish developer's guide and feel it fits our API developers as well…

- Be sensible.
- If in doubt, think.
- If still in doubt, ask.
- Admit your mistakes, it's faster that way.
- Thou SHALL not paint bikesheds.

Making A Request

REST requests must usually be made via HTTPS by using the headers, authentication, data types, and methods specified below. When HTTP requests are not allowed, the HTTP 400 – Bad Request response is returned. Please be aware that the HTTPS certificate may be self-signed so when using curl, set CURLOPT_SSL_VERIFYPEER and CURLOPT_SSL_VERIFYHOST to 0. The current endpoint for the API is available at:

https://api.StrandVision.com/v1.0/

Rate Limiting

To prevent unwanted flooding of the API system, there is a maximum number of requests that can be sent in a given time period. This limit is 30 requests per 5 minute and 5,000 requests per 24 hour scrolling period which can be retrieved via the api/read/limits method. This limit is tracked per API key and all requests count toward this limit. Refer to the x-requestLimit and x-requestsRemaining header responses for values related to this limit. It is also possible to have these limits adjusted per API key by contacting a StrandVision representative.

Supported Data Formats

The StrandVision API supports both XML and JSON data formats, specified by using the x-apiResponse field or using the content-type and accept HTTP Keys. If no format is specified, JSON will be used as the default.

Authentication

Authentication with the StrandVision API is done using the API keys given on a per-account basis. Some functions that require additional security will also require a matching secret key. The values for these keys can be found under on the Signage Pages, API area of the StrandVision.com web site once you have logged in. If the function only required the API Key, you can simply read from the api url with &apiKey=<key> added as a parameter. To make an authenticated request using your Secret key, follow these steps:

- Create the string representation of the current GMT / UTC date and time in HTTP RFC 7231 format. In php, this is created with gmdate("D, d M Y H:i:s T", $date). Example: Sun, 02 Apr 2023 08:02:03 GMT
- Calculate the hexadecimal HMAC SHA256 hash of that string using your Secret key as the hash key. In php, this is created with hash_hmac('sha256', $date, $secret). If using the above date and secret key of JHRF18Y4PCH4BLXRLKN0QCTXH9GKOC17, the resulting HMAC hash to send is 05632e27359d2170ee67a8b8bdd6c44f8cfc18f1376c22b918c444b29a204d0a

- Set the values for the request headers using your API key, the current date and time, and the HMAC
- hash that you calculated. This example was created using a Secret key of c9b5625f-9834-4ff8-baba-
- 4ed5f32cae55:
- x-apiKey: JHRF18Y4PCH4BLXRLKN0QCTXH9GKOC17
- x-apiDate: Sun, 02 Apr 2023 08:02:03 GMT
- x-apiHmac: 05632e27359d2170ee67a8b8bdd6c44f8cfc18f1376c22b918c444b29a204d0a

Requests are not case sensitive and must be sent shortly after these headers are generated. If too much time has passed between when the x-apiDate and x-apiHmac strings were created and when the request is received by the StrandVision API servers, then the request will be denied. Note that the API Create, Update and Delete functions must also have the additional security password properly passed via GET. Since this additional security password changes frequently, if it fails, try the call again in 10 seconds.

If your application has difficulties sending headers to the API server, the same key / value pairs can also be sent via GET or POST. If you are unable to get SHA256 working, call us and we can set your individual access key to use a different hash creation method.

Requests made with missing credentials will receive an HTTP 401 – Unauthorized response. Invalid credentials or x-apiDate value will receive an HTTP 403 - Forbidden response. When an invalid API endpoint is accessed, the HTTP 404 – Not Found response will be returned. If there is an issue with the server, an HTTP 500 – Internal Server Error:<abbreviated codes> response will be returned. Our technicians are notified of these errors via email. If it is not corrected within 30 minutes or you need urgent assistance, please call us.

Common Key Fields

The StrandVision API includes several custom HTTP Keys that contain information about the requests and responses that are sent. These headers fields are:

Request Keys

Field name	Description
x-apiKey	The API Key for your account. Refer to the Config - Account Information menu once logged in to find this value.
x-apiDate	Standard HTTP-formatted date. This date is used to protect against falsified requests
x-apiHmac	HMAC hash of value of the x- aouDate field. Refer to the StrandVision REST API Documentation v1.0 Authentication section for more details on how to generate this value.
x-apiResponse	Whether the response should be formatted differently than your default response method. Valid options are ‘json’ and ‘xml’.
x-apiConsolidate	Optional to consolidate response (reduce bandwidth) by removing empty response values along with other information that can be gathered elsewhere. Valid options are 0 and 1.
x-LogLevel	Specify the log level for this call. This defaults to 0 which reduces the information that is stored for each call. Set to 1 to store server name, user agent and request url. Set to 2 or higher to save raw request and response information. This is used

Response Keys

Field name	Description
x-RequestId	A unique identifier of the API call that was sent. Use the value of this header to help identify your request for your own purposes or when contacting StrandVision support.
x-RequestLimit	If your account is rate limited, this is returned with the maximum number of requests that can be sent before the rate limit is exceeded.
x-RequestRemain	If rate limited, this is returned with the number of requests remaining before the rate limit is exceeded.
x-RequestReset	If rate limited, this is when the counter will be reset.
x-PagesMax	If there are more than one page of information, this provides the total number of pages.

API List Call

Each section has a List API call which will list all of the calls available for that section. For example, the Api/Read/List function will return all of the Api/Read/* calls and a short description of each as an array.

Additional API Needs

From time to time, this document will be updated to include new API calls. The latest version is at www.StrandVision.com/api.pdf. Not seeing a specific example API call you are looking for or you identify additional calls that this service could provide? Please contact us to request it to be added.

General API Calls

The following is a detailed listing of the data types used for requests and responses for the overall system with the StrandVision API.

Get API Servers - api/read/servers (Secret Optional)

This process returns a list of StrandVision servers that are available to be read from. Since the strandvision api servers are load balanced, this will typically only contain one server. It is recommended that this be called once per week in case the DefaultServer needs to be used for future calls. Note that if the primary or default servers are offline, you can use the FailServerList to get read only access to your signage content.

Response Keys

Field Name	Type	Description
PrimaryServer	Url	The primary server for all future calls (or at a minimum all future calls for this session).
DefaultServer	Url	The default server for all future calls. If different, this must be stored as part of the API configuration.
FailServerList	Array	Array of server urls in priority order

Get API Call Limits - api/read/limits (Secret Required)

This process returns information about your call limits. The following fields are returned if no parameter is passed:

Field Name	Type	Description
Limit5Min	Number	Maximum 5 minute requests, -1=unlimited
Remain5Min	Number	Requests left in the 5 minute period, -
ResetDate5Mi	Date	Date/Time that the 5 minute period will reset
Limit1Day	Number	Maximum requests perday, -1=unlimited
Remain1Day	Number	Requests left in the 24 hour period, -1=unlimited
ResetDate1Da	Date	Date/Time that the day period

Get API ACL - api/read/acl (Secret Required)

This process returns the functions that your acl allows you to call. Note that API Access Control Lists are always manually created by the system administrator.

If the parameter Path is passed in, this process returns the following:

Field Name	Type	Description
AclAllowed	Number	1 if allowed and 0 if not

The following fields are returned as an array if no parameter is passed:

Field Name	Type	Description
Path	**Text**	**Path that is allowed (* = wildcard from that level on)**
Display_Name	Text	Name of the access control list
Id	Number	The ID of the access control list
Require_Https	Number	1 if requires https, 0 if http is allowed
Require_Hash	Number	0 for no date checksum required. 1=md5, 2=sha1, 3=sha256, 4=sha384, 5=sha512 hash of the date is required

Get API Groups - api/read/groups (Secret Required)

This process returns the groups that your acl has access to. Note that API Groups are always manually created by the system administrator.

The following fields are returned as an array if no parameter is passed:

Field Name	Type	Description
Id	Number	Id Number for the group
Name	Text	Descriptive Name of the group
Is_Enabled	Text	Whether this group is allowed to be processed - Yes or No
Is_Public	Text	Whether this group is automatically assigned to everyone - Yes or No
Created	Date	HTTP-formatted GMT/UTC date/time for when this key was created

Get API Key - api/read/keys (Secret Required)

This process returns the details about your api key and all keys you created. You can pass an optional KeyId parameter to return a single one. The following fields are returned as an array of all keys:

Field Name	Type	Description
Id	Number	The Id of this key
Display_Name	Text	The display name for this key
Email	Text	Optional Email address
Phone	Text	Optional Phone
CreatedBy	Number	The Key Id that created this key
Created	Date	HTTP-formatted GMT/UTC date/time for when this key was created
Modified	Date	HTTP-formatted GMT/UTC date/time for when this key was last modified
StartDate	Date	If filled in, the first HTTP-formatted GMT/UTC date/time that this key is available
EndDate	Date	If filled in, last HTTP-formatted GMT/UTC date/time that this key is available
Is_Enabled	Number	If the key is enabled (0 if not)
DayPass	Number	If the server day password is required (changes multiple times per day)
Require_Https	Number	If HTTPS protocol is required for this key (note that the ACL can require HTTPS for some functions)
Require_Hash	Number	0 for no date checksum required. 1=md5, 2=sha1, 3=sha256, 4=sha384, 5=sha512 hash of the date is required
AllowHours	Number	The number of hours that the remote computer clock can be different than the server clock. 0 ignores the x-ApiDate entirely and can be skipped.
ResponseFormat	Text	The default response format that is assigned to this key. Current options are csv, json or xml.
LogLevel	Number	The default logging level for this key. 0=minimal, 1=medium, 2+=high
LogRaw	Number	The number of days to allow raw log details to be stored and accessed
Api_Key	Text	The API Key
Api_Secret	Text	The API Secret Key
MaxHits	Text	The maximum number of hits allowed per sec, min, hr, day, wk, mon. 0=unlimited and multiple limits are allowed when comma
GroupId	Number	Group id this key is assigned to. If there are multiple groups, this is returned as an array of group id's

Get API Log Details - api/read/log (Secret Required)

This process returns the following log details that are available for the RequestId passed in with parameter LogRequestId:

Field Name	Type	Description
Request_Time	DateTime	Date/Time call was made (in GMT / UTC)
Http_Host	Text	Host that was called

Server_Name	Text	Server name that processed the request
Server_Addr	IP	IP Address of the responding server
Server_Port	Number	Server port used
Remote_Addr	IP	IP Address of the calling computer
Request_Scheme	Text	Http or Https
Request_Metho	Text	Get or Post
Api_Acl	Number	ACL id that was selected for the call
Api_Function	Text	The API function called
Request_Url	Text	Request url (if stored)
Http_User_Agen	Text	User Agent (if stored)
Raw_Request	Text	Json encoded raw request (if stored)
Response_Code	Number	HTTP Response Code
Response	Text	Response sent (if stored)
Bandwidth	Number	Bandwidth used by the call

To store all details during a call, pass the key LogLevel with a value of 2 on the initial request, then call this process with the RequestID returned to get the details back. Note that the RequestId must have been called with the same apiKey. A week after the log record is created, extra details are removed and they are removed entirely after a month.

Create API Key - api/create/key (Secret/Daily Required)

This process creates a new key and assigns it to manually configured acl group ids that you have access to (see api/read/groups). Your primary access group that allows key creation cannot be allocated to new access keys. Only the GroupId and Display_Name key are required and the others are optional. Note that if the Display_Name is already found, the key will not be created and an HTTP 400 – Bad Request will be returned.

Get/Post Request Keys

Field Name	Type	Description
GroupId	Number	A required Group id to assign this user to. If multiple groups are to be added, pass an array of group id's
Display_Name	Text	The display name for this key
Email	Text	Optional Email address
Phone	Text	Optional Phone
StartDate	Date	Optional HTTP-formatted GMT/UTC starting date/time defaults to now
EndDate	Date	Optional HTTP-formatted GMT/UTC ending date/time
DayPass	Number	Defaults to 0 - 1 if the server day password is required (changes multiple times per day)
Require_Https	Number	Defaults to 1 – Set if HTTPS protocol is required for this key
Require_Hash	Number	Defaults to 3 - 0 for no date checksum required. 1=md5, 2=sha1, 3=sha256, 4=sha384, 5=sha512 hash of the date is required
AllowHours	Number	Defaults to 5 minutes - The number of hours that the remote computer clock can be different than the server clock. 0 ignores the x-ApiDate entirely and can be skipped.
ResponseFormat	Text	The default response format that is assigned to this key. Current options are csv, json or xml and the default is json.

LogLevel	Number	The default logging level for this key. 0=minimal, 1=medium, 2+=high. Default=0
LogRaw	Number	The number of days to allow raw log details to be stored and accessed. Default=0
MaxHits	Text	The maximum number of hits allowed per sec, min, hr, day, wk, mon. 0=unlimited and multiple limits are allowed when comma separated. Default=5/sec, 100k/mon.
Defaults	Array	Key => Value array to store in defaults table

Response Keys

Field Name	Type	Description
Id	Number	The Id of this key
Api_Key	Text	The API Key
Api_Secret	Text	The API Secret

Edit API Key - api/edit/key (Secret/Daily Required)

This process edits an existing key if it was created by your access key and it is not your own. The Key Id or ApiKey must be passed and if both are passed, they must match the same record. The other parameters are optional. If GroupId is passed, it assigns the manually configured acl group ids that you have access to (see api/read/groups). Your primary access group that allows key creation cannot be allocated to new access keys. Note that if the Display_Name is passed and matches another key, the key will not be updated and an HTTP 400 – Bad Request will be returned.

Get/Post Request Keys

Field Name	Type	Description
KeyId	Number	Optional Key Id to edit
Api_Key	Text	Optional API Key to edit
GroupId	Number	A required Group id to assign this user to. If multiple groups are to be added, pass an array of group id's
Display_Name	Text	The display name for this key
Email	Text	Optional Email address
Phone	Text	Optional Phone
StartDate	Date	Optional HTTP-formatted GMT/UTC starting date/time
EndDate	Date	Optional HTTP-formatted GMT/UTC ending date/time
DayPass	Number	Defaults to 0 - 1 if the server day password is required (changes multiple times per day)
Require_Https	Number	Defaults to 1 – Set if HTTPS protocol is required for this key
Require_Hash	Number	Defaults to 3 - 0 for no date checksum required. 1=md5, 2=sha1, 3=sha256, 4=sha384, 5=sha512 hash of the date is required
AllowHours	Number	Defaults to 12 - The number of hours that the remote computer clock can be different than the server clock. 0 ignores the x-ApiDate entirely and can be skipped.
ResponseFormat	Text	The default response format that is assigned to this key. Current options are csv, json or xml and the default is json.

LogLevel	Number	The default logging level for this key. 0=minimal, 1=medium, 2+=high. Default=0
LogRaw	Number	The number of days to allow raw log details to be stored and accessed. Default=0
MaxHits	Text	The maximum number of hits allowed per sec, min, hr, day, wk, mon. 0=unlimited and multiple limits are allowed when comma separated. Example=1k/sec, 100k/mon.
Defaults	Array	Key => Value array to store in defaults table

Response Keys

Field Name	Type	Description
Id	Number	The Id of this key
Change Field	Variable	The updated field value
Change Field	Variable	The updated field value

Create API Defaults - api/create/defaults (Secret Required)

This process creates or updates the default values for the specified access key. The Key Id or ApiKey must be passed and if both are passed, they must match the same record. Note that only the Access Key / Id is validated to ensure that at least one is passed, the values are found / active and you created it. Other parameters are not validated and must have lower case field names in the default table. If the default record is already here for this access key, the fields sent will be updated. If there are any issues with the parameters, the sql query and error message will be returned with an HTTP 400 – Bad Request header. The other parameters are shown in the "Common Get/Post Request Keys" section on page 17 (excluding ModDate).

Get/Post Request Keys

Field Name	Type	Description
Key_Id	Number	Optional Key Id to assign the default values.
Api_Key	Text	Optional API Key to assign the default values.
Parent	Number(8)	Parent ID for your account
Custno	Number(8)	Customer Number for your account
DispGroup	Number	Display Group for your account
Language	Number	Language number, 0=English
Show_Delete	Number	If should show deleted information 0 (default)=no,

Response Keys

This returns the complete default record on success otherwise a failure error message.

Delete API Key - api/delete/key (Secret/Daily Required)

This process disables an active key and sets the end date to now if it was created by your access key and it is not your own. The Key Id or ApiKey must be passed and if both are passed, they must match the same record.

Get/Post Request Keys

Field	Type	Description
KeyId	Number	Optional Key Id to delete
Api_Key	Text	Optional API Key to delete

Response Keys

Field Name	Type	Description
DeleteDate	Date	The date that this key was deleted