Bit9 Platform API, Version 1.0

This document is intended for programmers who want to write code to interact with the Bit9 Platform using custom scripts or integrate with other applications. The Bit9 API is a RESTful API that can be consumed over the HTTPS protocol using any language that can issue GET/POST/PUT URI requests and interpret JSON responses.

Disclaimer

By accessing and/or using the API and Documentation provided on this site, you hereby agree to the following terms:

You may access and use the API and Documentation only for your own internal business purposes and in connection with your authorized use of Bit9 software.

Title to the API and the Documentation, and all intellectual property rights applicable thereto, shall at all times remain solely and exclusively with Bit9 and Bit9's licensors, and you shall not take any action inconsistent with such title.

THE API AND RELATED DOCUMENTATION ARE PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED.

IN NO EVENT SHALL BIT9 BE LIABLE FOR SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER INDIRECT DAMAGES OR FOR DIRECT DAMAGES ARISING OUT OF OR RESULTING FROM YOUR ACCESS OR USE OF THE API AND DOCUMENTATION, EVEN IF BIT9 IS ADVISED OF OR AWARE OF THE POSSIBILITY OF SUCH DAMAGES.

Versioning

Current version of Bit9 API is v1. All API calls are based in address `https://<your server name>/api/bit9platform/v1`

Authentication

Bit9 APIs are authenticated through the API token. This token has to be placed inside each HTTP request `'X-Auth-Token'` header. The API token is tied to the console user. To obtain the API token, ask the Bit9 Server administrator to generate special user and token for you. A good practice is to have separate console users with minimum required access controls for each API client.

Access Controls

An API client has the same access level as its corresponding console user. For example, in order to get access to the 'event' object, the user associated with API token will need permission to view events. Required permissions are listed with each API in this document. If caller lacks the required permissions, `HTTP error 401 - Unauthorized` will be returned.

Responses

Successful calls will return either `HTTP 200 - OK` or `HTTP 201 - Created`, depending if request modified/deleted an existing object or created a new object, respectively.
In case of POST and PUT, the response will contain the body of the modified or created object in the content, and the URI of the created or modified object in URL property of the response.
In the case of GET, the response will contain the body of the searched object(s) in the content.
Failed calls will return errors in the range 400-599. This is usually one of the following:
`HTTP 400 - Bad request` - Usually means that request contains unexpected parameters. More details about error can be found in the response content.
`HTTP 401 - Unauthorized` - Either authentication (invalid token) or access control (missing RBAC) error.
`HTTP 403 - Forbidden` - Specified object cannot be accessed or changed.
`HTTP 404 - Not found` - Object referenced in the request cannot be found.
`HTTP 503 - Service unavailable` - Cannot return object at this moment because service is unavailable. This can happen if too many file downloads are happening at the same time. You can try later.

Searching

Searching is done through the GET request, by passing search elements as URL query parts:
`v1/computer?q=<query condition 1>&q=<query condition 1>...&group=<optional group term>&sort=<optional sort term>&offset=<optional offset>&offset=<optional limit>`
The following sections describe these query parts.

Query Condition

Multiple conditions can be added, and each has to be satisfied for the result set.
Individual conditions can have one or multiple subconditions, separated with '|' (pipe) symbol.

A condition contains three parts: name, operator and value.

- Name is any valid field in the object that is being queried.
- Operator is any of valid operators (see below). All operators consist of a single character.
- Value is compared with operator and depends on field type.

Possible operators are:

- **:** results in LIKE comparison for strings, and = comparisons for other types. Note that LIKE comparison for strings results in '=' comparison if the string doesn't contain wildchars. String comparison is case insensitive.
- **!** results in NOT LIKE comparison for strings, and <> comparison for other types. Note that NOT LIKE comparison for strings results in '<>' comparison if the string doesn't contain wildchars. String comparison is case insensitive.

- **<** Less than - can be used for both strings and numerical values
- **>** Greater than - can be used for both strings and numerical values
- **+** logical AND operation (valid only for numerical values). True if value has all bits set as in operand. This can be used to check existence of given flag in a field
- **-** logical NAND operation (valid only for numerical values). True if value has none of the bits in the operand. This can be used to check non-existence of given flag in a field
- **|** separating values with | (pipe) symbol will cause both values to be included in the condition. Example "q=fileName:test1.exe|test2.exe" will match all objects where filename is either test1.exe or test2.exe. Note that negative conditions (- and !) will exclude entries that match either of included values.

Example of valid filter segment:

```
# Request:
[GET]
https://myServer/api/bit9platform/v1/Computer?q=ipAddress:fe00*|ff00*&q=computerTag!&q=dateCre
ated>-10h

# Resulting SQL query condition evaluated:
... WHERE (ipAddress LIKE 'fe00%' OR ipAddress LIKE 'ff00%')
AND computerTag NOT LIKE ''
AND dateCreated>DATEADD(HOUR, -10, GETUTCDATE())
```

Note: All string matching will be case insensitive

Limiting Results and Getting Result Count

Attributes: &offset=x&limit=y, where x is offset in data set, and y is maximum number of results to retrieve

Special values for limit are:

- If not specified: First 1000 results will be returned.
- If set to -1: Only result count will be returned, without actual results. Offset parameter is ignored in this case.
- If set to 0: All results will be returned. Offset parameter is ignored in this case.
  Note that some result sets could be very large, resulting in query timeout. Therefore, unless you know that query will not return more than 1000 results, it is recommended to retrieve data in chunks using offset and limit.

Here is an example on how to get result count from a query:

```
# Request:
[GET] https://myServer/api/bit9platform/computer?limit=-1

# Response:
{"count": 1284}
```

Sorting

Sorting is optional and can be defined with a single attribute: *&sort=xyz [ASC|DESC]*

- There can be only one sorting field
- Default sort order (if omitted) is ASC
- xyz is field name from the result set

Grouping

Grouping is optional and can be defined with a single attribute: *&group=xyz*

- There can be only one grouping field
- When grouping is specified, sorting is ignored – output is automatically sorted by grouping field

Output of grouping is always array of objects with value and count fields. "Value" is group field value, and "count" is number of rows that have that name for the grouped field. Here is example:

```
# Request:
[GET] https://myServer/api/bit9platform/v1/Computer?group=osShortName

# Response:
[
{"value": "CentOS 5","count": 53},
{"value": "CentOS 6","count": 826},
{"value": "Mac","count": 2311},
{"value": "Windows 7","count": 1330}
]
```

Code Examples

Here are several code examples, written in Python 3, using requests and JSON libraries.

Approve Publisher

This code approves publisher with id=12 for all policies

```
import requests, json

# --- Prepare our request header and url ---
authJson={
'X-Auth-Token': '8F97E8CB-1DCD-40D2-817B-7CECDD79CA67',  # replace with actual user token
'content-type': 'application/json'
}
b9StrongCert = True  # Set to False if your Server has self-signed IIS certificate
```

```
url = 'https://myserver/api/bit9platform/v1/publisher/12'  # replace with actual server
address

# --- Here is our request ---
data = {'publisherState': 2}  # 2 means 'approved'
r = requests.put(url, json.dumps(data), headers=authJson, verify=b9StrongCert)
r.raise_for_status()  # Make sure the call succeeded
publisher = r.json()  # get resulting publisher object
```

Ban File per Policy

This code bans file with Md5 hash '64a4f54d6863d59f1121a91554b55e9a' for policies id 10 and 11

```
import requests, json

# --- Prepare our request header and url ---
authJson={
'X-Auth-Token': '8F97E8CB-1DCD-40D2-817B-7CECDD79CA67',  # replace with actual user token
'content-type': 'application/json'
}
b9StrongCert = True  # Set to False if your Server has self-signed IIS certificate
url = 'https://myserver/api/bit9platform/v1/fileRule'  # replace with actual server address

# --- Here is our request ---
data = {'hash': '64a4f54d6863d59f1121a91554b55e9a', 'fileState': 3,  # 3 means 'banned'
'policyIds': '10,11'}
r = requests.post(url, json.dumps(data), headers=authJson, verify=b9StrongCert)
r.raise_for_status()  # Make sure the call succeeded
fileRule = r.json()  # get resulting file rule object
```

Disable Tamper Protection for Computers

This code disables tamper protection for computers with IP address starting with 10.201.2, and moves them into policy 8

```
import requests, json

# --- Prepare our request header and url ---
authJson={
'X-Auth-Token': '8F97E8CB-1DCD-40D2-817B-7CECDD79CA67',  # replace with actual user token
'content-type': 'application/json'
}
apiUrl = 'https://myserver/api/bit9platform' # replace with actual server address
b9StrongCert = True  # Set to False if your Server has self-signed IIS certificate

# Get computers. Here we assume that count is reasonable and we ca get all of them at once (no
limit specified)
comps = requests.get(
    apiUrl + '/v1/computer?q=ipAddress:10.201.2.*',
    headers=authJson, verify=b9StrongCert).json()

for c in comps:  # For each returned computer...
c['policyId'] = 8  # Move to policy 8
# Tamper protection can be disabled only through URI:
requests.post(
        apiUrl+'/v1/computer?newTamperProtectionActive=false',
        json.dumps(c), headers=authJson, verify=b9StrongCert)
```

Locally Approve Files

This code locally approves all unapproved files for Windows computer in policy 8, if file prevalence is 10 or greater

```
import requests, json

# --- Prepare our request header and url ---
authJson={
'X-Auth-Token': '8F97E8CB-1DCD-40D2-817B-7CECDD79CA67',  # replace with actual user token
'content-type': 'application/json'
}
apiUrl = 'https://myserver/api/bit9platform' # replace with actual server address
b9StrongCert = True  # Set to False if your Server has self-signed IIS certificate

# Get all Windows computers in policy 8
comps = requests.get(
    apiUrl + '/v1/computer?q=policyId:8&q=platformId:1',
    headers=authJson, verify=b9StrongCert).json()

for c in comps:  # For each returned computer, get list of locally unapproved files
files = requests.get(
        apiUrl + '/v1/fileInstance?q=computerId:'+ str(c['id']) + '&q=localState:1',
        headers=authJson, verify=b9StrongCert).json()

for finst in files:  # For each returned file...
    # Get its file catalog entry to get prevalence
    fcat = requests.get(
            apiUrl + '/v1/fileCatalog/'+str(finst['fileCatalogId']),
            headers=authJson, verify=b9StrongCert).json()

    if fcat['prevalence']>=10:  # if prevalent enough...
        finst['localState'] = 2  # Approve locally
        requests.post(
                apiUrl + '/v1/fileInstance',
                json.dumps(finst), headers=authJson, verify=b9StrongCert)
```

API Reference

This section lists all API objects and their properties that are listed in table with each object. Some subset of properties for each object are modifiable through POST/PUT requests and those are called in a separate table.

Each API object can have associated GET, PUT, POST or DELETE requests with their individual parameters.
GET and DELETE request parameters are entirely passed in the request URI.
POST and PUT request parameters accept entire object that is passed in the body of the request (as JSON), and some additional parameters that are passed through the request URI.

» approvalRequest

v1/approvalRequest object exposes workflow for approval requests and justifications.

All Object Properties for approvalRequest

Name	Type	Property Description
id	Int32	Unique approvalRequestId
fileCatalogId	Int32	Id of fileCatalog entry associated with file for this request
installerFileCatalogId	Int32	Id of fileCatalog entry associated with installer for this request
processFileCatalogId	Int32	Id of fileCatalog entry associated with process for this request
computerId	Int32	Id of computer where request originated
computerName	String	Name of computer where request originated
dateCreated	DateTime	Date/time when this request was created (UTC)
createdBy	String	User that created request on the agent
dateModified	DateTime	Date/time when this request was last modified (UTC)
modifiedBy	Int32	User that last modified this request
enforcementLevel	Int32	Enforcement level of agent at the time of request. Can be one of: 20=High (Block Unapproved) 30=Medium (Prompt Unapproved) 40=Low (Monitor Unapproved) 60=None (Visibility) 80=None (Disabled)

resolution	Int32	Resolution of request. Can be one of: 0=Not Resolved 1=Rejected 2=Resolved - Approved 3=Resolved - Rule Change 4=Resolved - Installer 5=Resolved - Updater 6=Resolved - Publisher 7=Resolved - Other
requestType	Int32	Type of request. One if: 1=Approval 2=Justification
requestorComments	String	Comments by user that created this request
requestorEmail	String	Email of user that created this request
priority	Int32	Priority of this request. Can be one of: 0=High 1=Medium 2=Low
resolutionComments	String	Comments by request resolver
status	Int32	Request status. Can be one of: 1=Submitted 2=Open 3=Closed
policyId	Int32	Id of policy for computer at the time when request arrived to the server
multipleBlocks	Boolean	True if file referenced by this request had multiple blocks
fileName	String	Name of file on the agent
pathName	String	Path of the file on the agent
process	String	Process that attempted to execute file on the agent. This is full process path
customRuleId	Int32	Id of the customRule that caused the file block on the agent

Properties modifiable Using PUT/POST Request for approvalRequest

Name	Type	Property Description
`resolution`	`Int32`	Resolution of request. Resolution can be changed for open requests or closed requests only. It can be one of: 0=Not Resolved 1=Rejected 2=Resolved - Approved 3=Resolved - Rule Change 4=Resolved - Installer 5=Resolved - Updater 6=Resolved - Publisher 7=Resolved - Other
`requestorEmail`	`String`	Email of user that created this request
`resolutionComments`	`String`	Comments by request resolver
`status`	`Int32`	Request status. Can be one of: 1=Submitted 2=Open 3=Closed. Allowed transitions are 1->2, 1->3, 2->3.

POST Request for approvalRequest

Description: Updates approval request

Required permissions: 'View approval requests', 'Manage approval requests'

Call syntax: `bit9platform/v1/approvalRequest`

Name	Source	Type	Description
`value`	FromBody	approvalRequest	Updated approval request object

PUT Request for approvalRequest

Description: Updates approval request

Required permissions: 'View approval requests', 'Manage approval requests'

Call syntax: `bit9platform/v1/approvalRequest/{id}`

Name	Source	Type	Description
`id`	FromUri	Int32	Id of file rule to create or update
`value`	FromBody	approvalRequest	Updated approval request object

GET Request for approvalRequest

Description: Returns object instance of this class

Required permissions: 'View approval requests'

Call syntax: `bit9platform/v1/approvalRequest/{id}`

Name	Source	Type	Description
`id`	FromUri	Int64	id of a requested object

GET Request for approvalRequest

Description: Returns objects that match given criteria

Required permissions: 'View approval requests'

Call syntax: `bit9platform/v1/approvalRequest?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}`

Name	Source	Type	Description
`q`	FromUri	List`1	Query condition (Optional - multiple query conditions are supported)
`group`	FromUri	String	Field name to group by (Optional)
`sort`	FromUri	String	Field name to sort by (Optional)
`offset`	FromUri	Int32	Offset in query results (Optional)
`limit`	FromUri	Int32	Maximum number of results to return. When 0 or not present, all results will be returned. When -1, only count will be returned.

» certificate

`v1/certificate` object exposes certificates found on endpoints and allows changing certificate state.

All Object Properties for certificate

Name	Type	Property Description
`id`	`Int32`	Unique certificate id
`parentCertificateId`	`Int32`	Id of a parent `certificate` in a certificate chain
`publisherId`	`Int32`	Id of `publisher` for this certificates
`thumbprint`	`String`	Thumbprint hash of the certificate

`thumbprintAlgorithm`	`String`	Algorithm used to calculate thumbprint of the certificate
`subjectName`	`String`	Certificate subject name
`signatureAlgorithm`	`String`	Certificate signature algorithm
`serialNumber`	`String`	Certificate serial number
`validFrom`	`DateTime`	Certificate valid from date (UTC)
`validTo`	`DateTime`	Certificate valid to date (UTC)
`publicKeyAlgorithm`	`String`	Certificate public key algorithm
`publicKeySize`	`Int32`	Certificate public key size in bits
`firstSeenComputerId`	`Int32`	Id of `computer` where this certificate was first seen
`description`	`String`	Description of certificate given by the user
`sourceType`	`Int32`	Mechanism that changed publisher state. Can be one of: 1 = Manual 5 = External (API)
`dateCreated`	`DateTime`	Date/time certificate was first seen (UTC)
`dateModified`	`DateTime`	Date/time certificate state or description was modified (UTC)
`modifiedByUser`	`String`	User that last modified certificate state or description
`intermediary`	`Boolean`	True if certificate is intermediary certificate in the chain
`valid`	`Boolean`	True if certificate is valid
`embedded`	`Boolean`	True if certificate was seen as embedded signer of a file
`detached`	`Boolean`	True if certificate was seen as detached signer of a file
`signer`	`Boolean`	True if certificate was seen signing a file
`cosigner`	`Boolean`	True if certificate was seen counter-signing a file

certificateState	Int32	One of assigned states: 1=Unapproved 2=Approved 3=Banned
certificateEffectiveState	Int32	One of effective states (taking into account other certificate in the chain): 1=Unapproved 2=Approved 3=Banned 4=Mixed (mix of approved and banned based on policy)
clVersion	Int64	CL version associated with this certificate

Properties modifiable Using PUT/POST Request for certificate

Name	Type	Property Description
description	String	New certificate description
certificateState	Int32	New state of the certificate. Valid states are: 1=Unapproved 2=Approved 3=Banned

POST Request for certificate

Description: Change certificate state

Required permissions: 'View software rules pages', 'Manage publisher rules'

Call syntax: `bit9platform/v1/certificate`

Name	Source	Type	Description
value	FromBody	certificate	Certificate object with desired parameters

PUT Request for certificate

Description: Change certificate state

Required permissions: 'View software rules pages', 'Manage publisher rules'

Call syntax: `bit9platform/v1/certificate/{id}`

Name	Source	Type	Description
`id`	FromUri	Int32	id of certificate to change
`value`	FromBody	certificate	Certificate object with desired parameters

DELETE Request for certificate

Description: Delete certificate approval

Required permissions: 'View software rules pages', 'Manage publisher rules'

Call syntax: `bit9platform/v1/certificate/{id}`

Name	Source	Type	Description
`id`	FromUri	Int32	id of certificate for which to delete approval

GET Request for certificate

Description: Returns object instance of this class

Required permissions: 'View software rules pages'

Call syntax: `bit9platform/v1/certificate/{id}`

Name	Source	Type	Description
`id`	FromUri	Int64	id of a requested object

GET Request for certificate

Description: Returns objects that match given criteria

Required permissions: 'View software rules pages'

Call syntax: `bit9platform/v1/certificate?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}`

Name	Source	Type	Description
`q`	FromUri	List`1	Query condition (Optional - multiple query conditions are supported)
`group`	FromUri	String	Field name to group by (Optional)
`sort`	FromUri	String	Field name to sort by (Optional)
`offset`	FromUri	Int32	Offset in query results (Optional)
`limit`	FromUri	Int32	Maximum number of results to return. When 0 or not present, all results will be returned. When -1, only count will be returned.

» computer

v1/computer object exposes computer-related properties for Bit9 Agent. It allows following modifications:

- Moving computers to different policies
- Upgrading Bit9 Agent
- Templating computers for VDI
- Changing debugging properties of computers
- Requesting advanced computer actions

All Object Properties for computer

Name	Type	Property Description
id	Int32	Unique computer id
name	String	Computer name
policyId	Int32	Id of policy this computer belongs to
policyName	String	Name of the policy this computer belongs to
policyDescription	String	Description of the policy this computer belongs to
automaticPolicy	Boolean	True if this computer's policy is assigned automatically through AD
localApproval	Boolean	True if this computer is in local approval mode
users	String	List of last logged in users
ipAddress	String	Last known IP address of this computer
connected	Boolean	True if this computer is connected
enforcementLevel	Int32	Current enforcement level. Can be one of: 20=High (Block Unapproved) 30=Medium (Prompt Unapproved) 35=Local approval 40=Low (Monitor Unapproved)

		60=None (Visibility) 80=None (Disabled)
disconnectedEnforcementLevel	Int32	Current enforcement level for disconnected computers. Can be one of: 20=High (Block Unapproved) 30=Medium (Prompt Unapproved) 35=Local approval 40=Low (Monitor Unapproved) 60=None (Visibility) 80=None (Disabled)
computerTag	String	Custom computer tag
CLIPassword	String	CLI password for this computer. Viewing this field requires 'Manage computers' permission
lastRegisterDate	DateTime	Last date/time this computer registered to the server (UTC)
lastPollDate	DateTime	Last date/time this computer contacted the server (UTC)
osShortName	String	Short OS name
osName	String	Long OS name
platformId	Int32	Platform Id. Can be one of: 1 = Windows 2 = Mac 4 = Linux
virtualized	String	True if computer is virtualized
virtualPlatform	String	If computer is virtualized, this is platform
dateCreated	DateTime	Date this computer was first registered
agentVersion	String	Version of Bit9 Platform agent
daysOffline	Int32	Number of days this computer was offline

uninstalled	Boolean	True if this computer was uninstalled
deleted	Boolean	True if computer is disabled
processorCount	Int32	Number of processor cores on this computer
processorSpeed	Double	Processor speed
processorModel	String	Processor model
machineModel	String	Machine model
memorySize	Int32	Memory size in MB
upgradeStatus	String	Upgrade status
upgradeError	String	Last upgrade error
upgradeErrorTime	DateTime	Last time upgrade error changed
upgradeErrorCount	Int32	Number of times last upgrade error happened so far
syncFlags	Int32	Status of synchronization on this agent. Can be combination of: 0x01=Agent is going through initialization 0x02=Agent is going through full cache re-synch 0x08=Agent config list is out of date 0x10=Agent Enforcement is out of date 0x20=Kernel is not connected to the agent 0x40=Agent events timestamps indicate that system clock is out of synch 0x80=Agent has failed the health check 0x100=This is clone that is tracking only new files 0x200=This version of kernel is not supported by the agent (Linux only)
refreshFlags	Int32	Refresh flags for this agent. Can be combination of: 0x01=Complete resynch of agent NAB and installer table is requested 0x02=Rescan of programs installed on the computer is requested 0x20=Tell agent to refresh config list

		0x40=Force this agent to reregister with new cookie 0x200=Trigger agent Reboot 0x1000=Tell agent to refresh config list from the file 0x4000 Boost the priority of this agent over all others permanently (until it is de-prioritized)
policyStatusDetails	String	Detailed status of policy on this agent
prioritized	Boolean	True if computer is prioritized
macAddress	String	MAC address of adapter used to connect to the Bit9 Server
debugLevel	Int32	Current debug level of agent. Range is from 0 (none) to 8 (verbose)
kernelDebugLevel	Int32	Current kernel debug level of agent. Range is from 0 (none) to 5 (verbose)
debugFlags	Int32	Debug flags. Can be 0 or combination of: 0x01 = Upload debug files now 0x10 = Enable full memory dumps 0x20 = Copy agent cache 0x40 = Delete debug files 0x80 = Upload agent cache 0x200 = Save verbose debug info + counters to the cache when copied/uploaded 0x400 = Generate and upload an analysis.bt9 file that contains various constraint violation analysis information 0x800 = Run a health check and send results to server
debugDuration	Int32	Debug duration in minutes
ccLevel	Int32	Cache consistency check level set for agent. Can be one of: 0 = None 1 = Quick verification 2 = Rescan known files Full scan for new files

ccFlags	Int32	Cache consistency check flags set for agent. Can be 0 or combination of: 0x0001 = Whether this is just a test run or not 0x0002 = Should the state of invalid files be preserved 0x0004 = Should new files found be locally approved or not 0x0008 = Should we re-evaluate whether a file's certificate information is still valid or not 0x0010 = Whether the check was scheduled or not 0x0020 = Whether the agent should run constraint checks to test for invalid results 0x0040 = Whether we are only searching for new script types as a result of a change to what 'IsScript' means 0x0080 = Whether we are doing a level 3 check for initialization 0x0100 = This cache check is to remediate CR# 18041 0x0200 = Force the re-evaluation of the IsCrawlable state and archive type
supportedKernel	Boolean	True if current computer kernel version is supported
forceUpgrade	Boolean	True if upgrade is forced for this computer
hasHealthCheckErrors	Boolean	True if computer has health check errors
clVersion	Int32	Current CL version of this agent
agentMemoryDumps	Int32	True if agent has memory dumps
systemMemoryDumps	Int32	True if agent has system memory dumps
initializing	Boolean	True if agent is initializing
tamperProtectionActive	Boolean	True if agent's tamper protection is active
agentCacheSize	Int32	Number of files that agent is tracking
agentQueueSize	Int32	Number of unsent file operations in agent's queue
syncPercent	Int32	Synchronization percentage for file operations on the agent

tdCount	Int32	Count of Trusted Directories hosted by this agent
template	Boolean	True if computer is a template
templateComputerId	Int32	Id of parent template computer if this is a clone
templateDate	DateTime	Date/time when this computer was templated (UTC)
templateCloneCleanupMode	Int32	Mode of template cleanup. Can be one of: 1=Manual (from console) 2=Automatic, by time (specified by templateCloneCleanupTime and templateCloneCleanupTimeScale) 3=Automatic, when new computer with the same name comes online 4=Automatic, as soon as computer goes offline
templateCloneCleanupTime	Int32	If templateCloneCleanupMode is 2, this is time before clone is cleaned up. Time unit is specified in templateCloneCleanupTimeScale
templateCloneCleanupTimeScale	Int32	Time unit of template cleanup. Can be one of: 1=Hours 2=Days 3=Weeks
templateTrackModsOnly	Boolean	If True, clones of this template will track only new and modified files
cbSensorId	Int32	ID of Carbon Black sensor. If 0, sensor is not installed on this computer
cbSensorVersion	String	Version of Carbon Black sensor if installed
cbSensorFlags	Int32	Carbon Black sensor flags. Can be combination of: 1 = User mode service is running 2 = Kernel driver is running
SCEPStatus	Int32	Status of SCEP protection. Can be one of following values: 0 = Unknown 1 = Not Present

		2 = Disabled 3 = Outdated 2 = Active

Properties modifiable Using PUT/POST Request for computer

Name	Type	Property Description
name	String	Computer name can be changed only if computer is a template
policyId	Int32	New Id of policy for this computer. PolicyId is ignored if either automaticPolicy us True or localApproval is True
automaticPolicy	Boolean	True if this policy is assigned automatically through AD. Has to be False if localApproval is True
localApproval	Boolean	True if this computer is currently in local approval mode. Has to be False if automaticPolicy is True
computerTag	String	Custom computer tag
refreshFlags	Int32	Change refresh flags for this agent. Can be combination of: 0x01=Complete resynch of agent NAB and installer table is requested 0x02=Rescan of programs installed on the computer is requested 0x20=Tell agent to refresh config list 0x40=Force this agent to reregister with new cookie 0x200=Trigger agent Reboot. 0x1000=Tell agent to refresh config list from the file 0x4000 Boost the priority of this agent over all others permanently (until it is de-prioritized)
prioritized	Boolean	True to prioritize this computer
debugLevel	Int32	Current debug level of agent. Range is from 0 (none) to 8 (verbose). This value can be changed only if 'changeDiagnostics' request parameter is set to true.

`kernelDebugLevel`	`Int32`	Current kernel debug level of agent. Range is from 0 (none) to 5 (verbose). This value can be changed only if 'changeDiagnostics' request parameter is set to true.
`debugFlags`	`Int32`	Debug flags. Can be 0 or combination of: 0x01 = Upload debug files now 0x10 = Enable full memory dumps 0x20 = Copy agent cache 0x40 = Delete debug files 0x80 = Upload agent cache 0x200 = Save verbose debug info + counters to the cache when copied/uploaded 0x400 = Generate and upload an analysis.bt9 file that contains various constraint violation analysis information 0x800 = Run a health check and send results to server This value can be changed only if 'changeDiagnostics' request parameter is set to true.
`debugDuration`	`Int32`	Debug duration in minutes. This value can be changed only if 'changeDiagnostics' request parameter is set to true.
`ccLevel`	`Int32`	Cache consistency check level set for agent. Can be one of: 0 = None 1 = Quick verification 2 = Rescan known files Full scan for new files This value can be changed only if 'changeDiagnostics' request parameter is set to true.
`ccFlags`	`Int32`	Cache consistency check flags set for agent. Can be 0 or combination of: 0x0001 = Whether this is just a test run or not 0x0002 = Should the state of invalid files be preserved 0x0004 = Should new files found be locally approved or not 0x0008 = Should we re-evaluate whether a file's certificate information is still valid or not

		0x0010 = Whether the check was scheduled or not 0x0020 = Whether the agent should run constraint checks to test for invalid results 0x0040 = Whether we are only searching for new script types as a result of a change to what 'IsScript' means 0x0080 = Whether we are doing a level 3 check for initialization 0x0100 = This cache check is to remediate CR# 18041 0x0200 = Force the re-evaluation of the IsCrawlable state and archive type This value can be changed only if 'changeDiagnostics' request parameter is set to true.
`forceUpgrade`	`Boolean`	True to force upgrade for this computer
`template`	`Boolean`	True if computer is a VDI template. This value can be changed only if 'changeTemplate' request parameter is set to true.
`templateCloneCleanupMode`	`Int32`	Mode of template cleanup. Can be one of: 1=Manual (from console) 2=Automatic, by time (specified by templateCloneCleanupTime and templateCloneCleanupTimeScale) 3=Automatic, when new computer with the same name comes online 4=Automatic, as soon as computer goes offline This value can be changed only if 'changeTemplate' request parameter is set to true.
`templateCloneCleanupTime`	`Int32`	If templateCloneCleanupMode is 2, this is time before clone is cleaned up. Time unit is specified in templateCloneCleanupTimeScale. This value can be changed only if 'changeTemplate' request parameter is set to true.
`templateCloneCleanupTimeScale`	`Int32`	Time unit of template cleanup. Can be one of: 1=Hours 2=Days 3=Weeks

		This value can be changed only if 'changeTemplate' request parameter is set to true.
`templateTrackModsOnly`	`Boolean`	If True, clones of this template will track only new and modified files. This value can be changed only if 'changeTemplate' request parameter is set to true.

POST Request for computer

Description: Updates computer object. Note that some computer properties can be changed only if specific boolean param is set, as noted below.

Required permissions: 'View computers', 'Manage computers'

Call syntax: `bit9platform/v1/computer?changeDiagnostics={changeDiagnostics}&changeTemplate={changeTemplate}&delete={delete}&resetCLIPassword={resetCLIPassword}&newTamperProtectionActive={newTamperProtectionActive}`

Name	Source	Type	Description
`value`	FromBody	computer	Updated computer object.
`changeDiagnostics`	FromUri	Boolean	Optional flag, defaults to false. If set to true, debug and CC properties of computer will be updated from the object sent in the body the request. This action requires 'Change advanced options' permission.
`changeTemplate`	FromUri	Boolean	Optional flag, defaults to false. If set to true, template settings will be updated from the object sent in the body the request. This action requires 'Change advanced options' permission.
`delete`	FromUri	Boolean	Optional flag, deletes computer entry.

`resetCLIPassword`	FromUri	Boolean	Optional flag to reset CLI password for this computer. This action requires 'Change advanced options' permission.
`newTamperProtectionActive`	FromUri	Nullable`1	Optional boolean to set desired tamper protection. Note that tamper protection cannot be set through the object, and might not be reflected in the object immediately, but only after computer reports back its new tamper protection setting. This action requires 'Change advanced options' permission.

PUT Request for computer

Description: Updates computer object. Note that some computer properties can be changed only if specific boolean param is set, as noted below.

Required permissions: 'View computers', 'Manage computers'

Call syntax: `bit9platform/v1/computer/{id}?changeDiagnostics={changeDiagnostics}&changeTemplate={changeTemplate}&delete={delete}&resetCLIPassword={resetCLIPassword}&newTamperProtectionActive={newTamperProtectionActive}`

Name	Source	Type	Description
`id`	FromUri	Int32	Id of computer to change.
`value`	FromBody	computer	Updated computer object.
`changeDiagnostics`	FromUri	Boolean	Optional flag, defaults to false. If set to true, debug and CC properties of computer will be updated from the object sent in the body the request. This action requires 'Change advanced options' permission.

changeTemplate	FromUri	Boolean	Optional flag, defaults to false. If set to true, template settings will be updated from the object sent in the body the request. This action requires 'Change advanced options' permission.
delete	FromUri	Boolean	Optional flag, deletes computer entry.
resetCLIPassword	FromUri	Boolean	Optional flag to reset CLI password for this computer. Command will clear the password, and it will re-populate with new value the next time computer registers. This action requires 'Change advanced options' permission.
newTamperProtectionActive	FromUri	Nullable`1	Optional boolean to set desired tamper protection. Note that tamper protection cannot be set through the object, and might not be reflected in the object immediately, but only after computer reports back its new tamper protection setting. This action requires 'Change advanced options' permission.

DELETE Request for computer

Description: Delete computer

Required permissions: 'View computers', 'Manage computers'

Call syntax: `bit9platform/v1/computer/{id}`

Name	Source	Type	Description
id	FromUri	Int32	id of computer to delete

GET Request for computer

Description: Returns object instance of this class

Required permissions: 'View computers'

Call syntax: bit9platform/v1/computer/{id}

Name	Source	Type	Description
id	FromUri	Int64	id of a requested object

GET Request for computer

Description: Returns objects that match given criteria

Required permissions: 'View computers'

Call syntax: bit9platform/v1/computer?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}

Name	Source	Type	Description
q	FromUri	List`1	Query condition (Optional - multiple query conditions are supported)
group	FromUri	String	Field name to group by (Optional)
sort	FromUri	String	Field name to sort by (Optional)
offset	FromUri	Int32	Offset in query results (Optional)
limit	FromUri	Int32	Maximum number of results to return. When 0 or not present, all results will be returned. When -1, only count will be returned.

» connector

v1/connector object exposes Network Connectors for Bit9 Platform. Note that internal connectors can only be accessed as read-only (GET requests), while external connectors can also be modified (PUT/POST requests)

All Object Properties for connector

Name	Type	Property Description
id	Int32	Unique connector Id
name	String	Name of the connector
analysisName	String	Name for analysis component of the connector (can be same as the name field)
connectorVersion	String	Version of this connector
canAnalyze	Boolean	True if this connector can analyze files
enabled	Boolean	True if connector is enabled
analysisEnabled	Boolean	True if analysis component of this connector is enabled
isInternal	Boolean	True if this is internal connector
analysisTargets	String[]	Array of possible analysis targets. Analysis targets are required when creating new fileAnalysis. They usualy represent different OS and configurations and are available only for some internal connectors.

Properties modifiable Using PUT/POST Request for connector

Name	Type	Property Description

name	String	Name of the connector. Note that only non-internal connectors can be renamed
analysisName	String	Name for analysis component of the connector (can be same as the name field)
connectorVersion	String	Version of this connector
canAnalyze	Boolean	True if this connector can analyze files
enabled	Boolean	True if connector is enabled
analysisEnabled	Boolean	True if analysis component of this connector is enabled

PUT Request for connector

Description: Updates registration for existing connector

Required permissions: 'View system configuration', 'Extend connectors through API'

Call syntax: `bit9platform/v1/connector/{id}?unregister={unregister}&deleteData={deleteData}`

Name	Source	Type	Description
id	FromUri	Int32	Id of connector object to update
value	FromBody	connector	Connector object to update
unregister	FromUri	Boolean	Optional: whether to unregister this connector. Defaults to false
deleteData	FromUri	Boolean	Optional: whether to delete all analysis results associated with this connector when unregistering. Defaults to true

POST Request for connector

Description: Registers a new connector, or updates registration for existing connector

Required permissions: 'View system configuration', 'Extend connectors through API'

Call syntax: `bit9platform/v1/connector?unregister={unregister}&deleteData={deleteData}`

Name	Source	Type	Description
`connector`	FromBody	connector	Connector object to register
`unregister`	FromUri	Boolean	Optional: whether to unregister this connector. Defaults to false
`deleteData`	FromUri	Boolean	Optional: whether to delete all analysis results associated with this connector when unregistering. Defaults to true

DELETE Request for connector

Description: Unregisters a custom connector

Required permissions: 'View system configuration', 'Extend connectors through API'

Call syntax: `bit9platform/v1/connector/{id}?deleteData={deleteData}`

Name	Source	Type	Description
`id`	FromUri	Int32	Connector id to unregister
`deleteData`	FromUri	Boolean	Optional: whether to delete all analysis results associated with this connector. Defaults to true

GET Request for connector

Description: Returns object instance of this class

Required permissions: 'View system configuration'

Call syntax: `bit9platform/v1/connector/{id}`

Name	Source	Type	Description
`id`	FromUri	Int64	id of a requested object

GET Request for connector

Description: Returns objects that match given criteria

Required permissions: 'View system configuration'

Call syntax: `bit9platform/v1/connector?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}`

Name	Source	Type	Description
`q`	FromUri	List`1	Query condition (Optional - multiple query conditions are supported)
`group`	FromUri	String	Field name to group by (Optional)
`sort`	FromUri	String	Field name to sort by (Optional)
`offset`	FromUri	Int32	Offset in query results (Optional)
`limit`	FromUri	Int32	Maximum number of results to return. When 0 or not present, all results will be returned. When -1, only count will be returned.

» event

v1/event object exposes public events.

All Object Properties for event

Name	Type	Property Description
id	Int64	Unique event Id
timestamp	DateTime	Date/Time when event was created (UTC)
receivedTimestamp	DateTime	Date/Time when event was received by the server (UTC)
description	String	Event description
type	Int32	Event type. Can be one of: 0 = Server Management 1 = Session Management 2 = Computer Management 3 = Policy Management 4 = Policy Enforcement 5 = Discovery 6 = General Management 8 = Internal Events
subtype	Int32	Event subtype. Can be one of event subtype IDs
subtypeName	String	Event subtype as string
ipAddress	String	IP address associated with this event
computerId	Int32	Id of computer associated with this event
computerName	String	Name of computer associated with this event

policyId	Int32	Id of policy where agent was at the time of the event
policyName	String	Name of policy where agent was at the time of the event
fileCatalogId	Int32	Id of fileCatalog entry associated with file for this event
installerFileCatalogId	Int32	Id of fileCatalog entry associated with installer for this event
processFileCatalogId	Int32	Id of fileCatalog entry associated with process for this event
fileName	String	Name of the file associated with this event
pathName	String	Path of the file associated with this event
commandLine	String	Full command line associated with this event. Viewing this field requires 'View process command lines' permission
processPathName	String	Name of the process associated with this event
processFileName	String	Path of the process associated with this event
installerFileName	String	Name of the installer associated with this event
processKey	String	Process key associated with this event. This key uniquely identifies the process in both Bit9 Platform and Carbon Black product
severity	Int32	Event severity. Can be one of: 2 = Critical 3 = Error 4 = Warning 5 = Notice 6 = Info 7 = Debug
userName	String	User name associated with this event
ruleName	String	Rule name associated with this event
banName	String	Ban name associated with this event
updaterName	String	Updater name associated with this event

`indicatorName`	`String`	Advanced threat indicator name associated with this event
`param1`	`String`	Internal string parameter 1
`param2`	`String`	Internal string parameter 2
`param3`	`String`	Internal string parameter 3
`stringId`	`Int32`	Internal string Id used for description

event is a read-only object and has no modifiable properties.

GET Request for event

Description: Returns object instance of this class

Required permissions: 'View events'

Call syntax: `bit9platform/v1/event/{id}`

Name	Source	Type	Description
`id`	FromUri	Int64	id of a requested object

GET Request for event

Description: Returns objects that match given criteria

Required permissions: 'View events'

Call syntax: `bit9platform/v1/event?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}`

Name	Source	Type	Description
q	FromUri	List`1	Query condition (Optional - multiple query conditions are supported)
group	FromUri	String	Field name to group by (Optional)
sort	FromUri	String	Field name to sort by (Optional)
offset	FromUri	Int32	Offset in query results (Optional)
limit	FromUri	Int32	Maximum number of results to return. When 0 or not present, all results will be returned. When -1, only count will be returned.

» fileAnalysis

v1/fileAnalysis object exposes all files sent to analysis with Network Connectors. It also allows requesting or canceling file analysis.

All Object Properties for fileAnalysis

Name	Type	Property Description
id	Int64	Unique fileAnalysis id
computerId	Int32	Id of computer entry associated with this analysis
fileCatalogId	Int32	Id of fileCatalog entry associated with this analysis
connectorId	Int32	Id of connector associated with this analysis
createdBy	String	User that requested this analysis
dateCreated	DateTime	Date/Time when fileAnalysis request was created (UTC)

`dateModified`	`DateTime`	Date/Time when fileAnalysis request was last modified (UTC)
`fileName`	`String`	Name of the file where file exists on the endpoint
`pathName`	`String`	Path of the file where file exists on the endpoint
`priority`	`Int32`	File analysis priority in range [-2, 2], where 2 is highest priority. Default priority is 0
`analysisStatus`	`Int32`	Status of analysis. Can be one of: 0 = scheduled 1 = submitted (file is sent for analysis) 2 = processed (file is processed but results are not available yet) 3 = analyzed (file is processed and results are available) 4 = error 5 = cancelled
`analysisResult`	`Int32`	Result of the analysis. Can be one of: 0 = Not yet available 1 = File is clean 2 = File is a potential threat 3 = File is malicious
`analysisTarget`	`String`	Target of the analysis (Connector-dependent)

Properties modifiable Using PUT/POST Request for fileAnalysis

Name	Type	Property Description
`computerId`	`Int32`	Id of `computer` from which to upload the file. If 0, system will find best computer to get the file from
`fileCatalogId`	`Int32`	Id of `fileCatalog` entry for which analysis is requested
`connectorId`	`Int32`	Id of target `connector` for the analysis
`priority`	`Int32`	Analysis priority in range [-2, 2], where 2 is highest priority. Default priority is 0
`analysisStatus`	`Int32`	Status of analysis. Status of analysis in progress can be changed to 5 (Cancelled)

analysisTarget	String	Target of the analysis (Optional). It has to be one of possible analysisTarget options defined for the givenconnector object, or empty for connectors without defined analysisTargets.

POST Request for fileAnalysis

Description: Creates or updates file analysis request

Required permissions: 'View files', 'Submit files for analysis'

Call syntax: `bit9platform/v1/fileAnalysis`

Name	Source	Type	Description
value	FromBody	fileAnalysis	New fileAnalysis object

PUT Request for fileAnalysis

Description: Updates existing file analysis request

Required permissions: 'View files', 'Submit files for analysis'

Call syntax: `bit9platform/v1/fileAnalysis/{id}`

Name	Source	Type	Description
id	FromUri	Int32	Id of file rule to create or update
value	FromBody	fileAnalysis	New fileAnalysis object

GET Request for fileAnalysis

Description: Returns object instance of this class

Required permissions: 'View files'

Call syntax: `bit9platform/v1/fileAnalysis/{id}`

Name	Source	Type	Description
id	FromUri	Int64	id of a requested object

GET Request for fileAnalysis

Description: Returns objects that match given criteria

Required permissions: 'View files'

Call syntax: `bit9platform/v1/fileAnalysis?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}`

Name	Source	Type	Description
q	FromUri	List`1	Query condition (Optional - multiple query conditions are supported)
group	FromUri	String	Field name to group by (Optional)
sort	FromUri	String	Field name to sort by (Optional)
offset	FromUri	Int32	Offset in query results (Optional)
limit	FromUri	Int32	Maximum number of results to return. When 0 or not present, all results will be returned. When -1, only count will be returned.

» fileCatalog

`v1/fileCatalog` object exposes all unique files found by Bit9 Agents and metadata related to files. Note that this is read-only API. In order to change state of the file, you need to use fileRule object.

All Object Properties for fileCatalog

Name	Type	Property Description
`id`	`Int32`	Unique fileCatalog Id
`dateCreated`	`DateTime`	Date/Time when this unique hash was first seen (Database local time)
`pathName`	`String`	Name of the path where this unique hash was first seen
`fileName`	`String`	Name of the file under which this unique hash was first seen
`fileExtension`	`String`	Extension of the file under which this unique hash was first seen
`computerId`	`Int32`	Id of `computer` where this file was first seen
`md5`	`String`	Md5 hash
`sha1`	`String`	Sha-1 hash
`sha256`	`String`	Sha-256 hash
`sha256HashType`	`Int32`	Can be one of: 5:Regular hash 6:Fuzzy hash for MSI installers
`fileType`	`String`	Type of the file
`fileSize`	`Int64`	Size of the file in bytes

productName	String	Name of the product associated with this file in the VERSIONINFO resource
publisher	String	Subject name of the certificate that signed this file
company	String	Name of the company associated with this file in the VERSIONINFO resource
publisherOrCompany	String	Publisher name of the file if it exist. If file is not signed, this will be a company name from the VERSIONINFO resource
productVersion	String	Version of the file in the VERSIONINFO resource
installedProgramName	String	Name of the product associated with this file in the MSI package
reputationAvailable	Boolean	True if reputation information has arrived for this file
trust	Int32	Trust of this file (0-10). Special value of -1 is reserved for unknown
trustMessages	String	More details about trust of this file
threat	Int16	Threat of this file. Can be one of: -1=Unknown 0=Clean 50=Potential risk 100=Malicious
category	String	Category of this file
fileState	Int32	File state of this hash. Can be one of: 1=Unapproved 2=Approved 3=Banned
publisherState	Int32	Publisher state of this hash. Can be one of: 1=Unapproved 2=Approved 3=Banned
certificateState	Int32	Certificate state of this hash. Can be one of: 1=Unapproved

		2=Approved 3=Banned
effectiveState	String	Effective state of this hash, taking into account publisherState and fileState. Can be one of: Unapproved Approved Banned Approved by Policy Banned by Policy Mixed
approvedByReputation	Boolean	True if this file was approved by reputation
reputationEnabled	Boolean	True if reputation approvals are enabled for this file
prevalence	Int32	Number of endpoints that have this file
fileFlags	Int32	File flags. Can be combination of: 0x00001 = File will report executions as 'report bans' 0x00004 = File is manually marked as installer 0x00010 = File is detected as installer 0x00100 = File was seen as root of installation 0x00200 = File was seen as a child of of installation 0x01000 = File has all needed metadata 0x04000 = File was executed on endpoint 0x10000 = File is manually marked as 'not installer' 0x20000 = Indicate that state we are sending applies to all children if this is a root hash 0x40000 = Indicate that file came from a trusted director 0x80000 = Indicate that file is an msi root file 0x200000 = Indicate that file was seen blocking on at least one endpoint 0x400000 = Indicate that file can be approved by reputation 0x2000000 = Indicates that this is not an 'interesting' file 0x4000000 = Indicate that the signature on this file is invalid 0x8000000 = Indicate that we have all necessary metadata from Macintosh and Linux platforms
publisherId	Int32	Id of publisher that signed this file

`certificateId`	`Int32`	Id of `certificate` that signed this file

fileCatalog is a read-only object and has no modifiable properties.

GET Request for fileCatalog

Description: Returns object instance of this class

Required permissions: 'View files'

Call syntax: `bit9platform/v1/fileCatalog/{id}`

Name	Source	Type	Description
`id`	FromUri	Int64	id of a requested object

GET Request for fileCatalog

Description: Returns objects that match given criteria

Required permissions: 'View files'

Call syntax: `bit9platform/v1/fileCatalog?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}`

Name	Source	Type	Description
`q`	FromUri	List`1	Query condition (Optional - multiple query conditions are supported)
`group`	FromUri	String	Field name to group by (Optional)
`sort`	FromUri	String	Field name to sort by (Optional)

offset	FromUri	Int32	Offset in query results (Optional)
limit	FromUri	Int32	Maximum number of results to return. When 0 or not present, all results will be returned. When -1, only count will be returned.

» fileInstance

v1/fileInstance object exposes live file inventory on all Bit9 Agents. It also allows local approvals of files.

All Object Properties for fileInstance

Name	Type	Property Description
id	Int64	Unique id of this fileInstance
fileCatalogId	Int32	Id of fileCatalog associated with this fileInstance
fileInstanceGroupId	Int64	Id of fileInstanceGroup associated with this fileInstance
computerId	Int32	Id of computer associated with this fileInstance
dateCreated	DateTime	Date/Time when file was was created on agent (UTC)
fileName	String	Name of the file on the agent
pathName	String	Path of the file on the agent
executed	Boolean	True if file was ever executed on the agent
localState	Int32	Local state of the file on the agent. Can be one of: 1=Unapproved 2=Approved 3=Banned

detailedLocalState	Int32	Local state of the file on the agent. Can be one of: 1=Approved (Not Persisted) 2=Unapproved (Persisted) 3=Banned' 4=Locally Approved 5=Banned 6=Banned (Report Only) 7=Locally Approved (Auto) 8=Approved as Installer 11=Approved 12=Approved as Installer (Top Level) 13=Banned (Report Only) 14=Unapproved
detachedPublisherId	Int32	Id of detached `publisher` that signed this file through the catalog
detachedCertificateId	Int32	Id of detached `certificate` that signed this file through the catalog

Properties modifiable Using PUT/POST Request for fileInstance

Name	Type	Property Description
localState	Int32	Target local state for the file on the agent. Can be one of: 1=Unapproved 2=Approved. Note that changed local state might not be reflected in the object immediately, but only after agent reports new state.

POST Request for fileInstance

Description: Change local file instance state

Required permissions: 'View files', 'Change local state'

Call syntax: `bit9platform/v1/fileInstance`

Name	Source	Type	Description

`value`	FromBody	fileInstance	Value of new fileInstance object

PUT Request for fileInstance

Description: Change local file instance state

Required permissions: 'View files', 'Change local state'

Call syntax: `bit9platform/v1/fileInstance/{id}`

Name	Source	Type	Description
`id`	FromUri	Int32	id of fileInstance to change
`value`	FromBody	fileInstance	Value of new fileInstance object

GET Request for fileInstance

Description: Returns object instance of this class

Required permissions: 'View files'

Call syntax: `bit9platform/v1/fileInstance/{id}`

Name	Source	Type	Description
`id`	FromUri	Int64	id of a requested object

GET Request for fileInstance

Description: Returns objects that match given criteria

Required permissions: 'View files'

Call syntax: `bit9platform/v1/fileInstance?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}`

Name	Source	Type	Description
`q`	FromUri	List`1	Query condition (Optional - multiple query conditions are supported)
`group`	FromUri	String	Field name to group by (Optional)
`sort`	FromUri	String	Field name to sort by (Optional)
`offset`	FromUri	Int32	Offset in query results (Optional)
`limit`	FromUri	Int32	Maximum number of results to return. When 0 or not present, all results will be returned. When -1, only count will be returned.

» fileInstanceDeleted

`v1/fileInstanceDeleted` object exposes deleted file inventory on all Bit9 Agents.

All Object Properties for fileInstanceDeleted

Name	Type	Property Description
`id`	`Int64`	Unique id of this fileInstanceDeleted

fileInstanceGroupId	Int64	Id of fileInstanceGroup associated with this fileInstanceDeleted
fileCatalogId	Int32	Id of fileCatalog associated with this fileInstanceDeleted
computerId	Int32	Id of computer associated with this fileInstanceDeleted
dateCreated	DateTime	Date/Time when file was was created on agent (UTC)
dateDeleted	DateTime	Date/Time when file was was deleted on agent (UTC)
fileName	String	Name of the file on the agent
pathName	String	Path of the file on the agent
detachedPublisherId	Int32	Id of detached publisher that signed this file through the catalog
detachedCertificateId	Int32	Id of detached certificate that signed this file through the catalog

fileInstanceDeleted is a read-only object and has no modifiable properties.

GET Request for fileInstanceDeleted

Description: Returns object instance of this class

Required permissions: 'View files'

Call syntax: `bit9platform/v1/fileInstanceDeleted/{id}`

Name	Source	Type	Description
id	FromUri	Int64	id of a requested object

GET Request for fileInstanceDeleted

Description: Returns objects that match given criteria

Required permissions: 'View files'

Call syntax: `bit9platform/v1/fileInstanceDeleted?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}`

Name	Source	Type	Description
q	FromUri	List`1	Query condition (Optional - multiple query conditions are supported)
group	FromUri	String	Field name to group by (Optional)
sort	FromUri	String	Field name to sort by (Optional)
offset	FromUri	Int32	Offset in query results (Optional)
limit	FromUri	Int32	Maximum number of results to return. When 0 or not present, all results will be returned. When -1, only count will be returned.

» fileInstanceGroup

`v1/fileInstanceGroup` object exposes grouping of file inventory from Bit9 Agents. Grouping can be based on installed programs reported by system, or automatic, based on installations seen by the agent.

All Object Properties for fileInstanceGroup

Name	Type	Property Description
id	Int64	Unique id of this fileInstanceGroup

fileCatalogId	Int32	Id of fileCatalog associated with this fileInstanceGroup
computerId	Int32	Id of computer associated with this fileInstanceGroup
dateCreated	DateTime	Date/Time when file was was created on agent (UTC)
fileName	String	Name of the file on the agent
pathName	String	Path of the file on the agent
userName	String	User associated with this group creation on the agent
groupType	Int32	Type of this group. It can be one of: 0=initialization group 1=top level group 2=process group 3=MSI group
installedProgramName	String	User associated with this group creation on the agent

fileInstanceGroup is a read-only object and has no modifiable properties.

GET Request for fileInstanceGroup

Description: Returns object instance of this class

Required permissions: 'View files'

Call syntax: `bit9platform/v1/fileInstanceGroup/{id}`

Name	Source	Type	Description
id	FromUri	Int64	id of a requested object

GET Request for fileInstanceGroup

Description: Returns objects that match given criteria

Required permissions: 'View files'

Call syntax: `bit9platform/v1/fileInstanceGroup?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}`

Name	Source	Type	Description
`q`	FromUri	List`1	Query condition (Optional - multiple query conditions are supported)
`group`	FromUri	String	Field name to group by (Optional)
`sort`	FromUri	String	Field name to sort by (Optional)
`offset`	FromUri	Int32	Offset in query results (Optional)
`limit`	FromUri	Int32	Maximum number of results to return. When 0 or not present, all results will be returned. When -1, only count will be returned.

» fileRule

`v1/fileRule` object exposes rules related to unique files. It allows creation and editing of file Approvals and Bans.

All Object Properties for fileRule

Name	Type	Property Description
`id`	`Int64`	Unique id of this fileRule

fileCatalogId	Int32	Id of fileCatalog entry associated with this fileRule. Can be null if file hasn't been seen on any endpoints yet
name	String	Name of this rule
description	String	Description of this rule
fileState	Int32	File state for this rule. Can be one of: 1=Unapproved 2=Approved 3=Banned
sourceType	Int32	Mechanism that created this rule. Can be one of: 1 = Manual 2 = Trusted Directory 3 = Reputation 4 = Imported 5 = External (API) 6 = Event Rule
sourceId	Int32	Id of source of this rule. Can be event rule id or trusted directory id
reportOnly	Boolean	True if this has a report-only ban
reputationApprovalsEnabled	Boolean	True if reputation approvals are enabled for this file
forceInstaller	Boolean	True if this file is forced to act as installer, even if product detected it as 'not installer'
forceNotInstaller	Boolean	True if this file is forced to act as 'not installer', even if product detected it as installer
policyIds	String	List of IDs of policies where this rule applies. 0 if this is a global rule
hash	String	Hash associated with this rule
platformFlags	Int32	Set of platform flags where this file rule will be valid. combination of: 1 = Windows

		2 = Mac 4 = Linux
dateCreated	DateTime	Date/time when this rule was created (UTC)
createdBy	String	User that created this rule
dateModified	DateTime	Date/time when this rule was last modified (UTC)
modifiedBy	String	User that last modified this rule
clVersion	Int64	CL version associated with this file rule

Properties modifiable Using PUT/POST Request for fileRule

Name	Type	Property Description
fileCatalogId	Int32	Id of fileCatalog entry associated with this fileRule. Can be 0 if creating/modifying rule based on hash or file name
name	String	Name of this rule
description	String	Description of this rule
fileState	Int32	File state for this rule. Can be one of: 1=Unapproved 2=Approved 3=Banned
reportOnly	Boolean	Set to true to create a report-only ban. Note: fileState has to be set to 1 (unapproved) before this flag can be set
reputationApprovalsEnabled	Boolean	True if reputation approvals are enabled for this file
forceInstaller	Boolean	True if this file is forced to act as installer, even if product detected it as 'not installer'
forceNotInstaller	Boolean	True if this file is forced to act as 'not installer', even if product detected it as installer
policyIds	String	List of IDs of policies where this rule applies. 0 if this is a global rule

`hash`	`String`	Hash associated with this rule. This parameter is not required if fileCatalogId is supplied
`platformFlags`	`Int32`	Set of platform flags where this file rule will be valid. combination of: 1 = Windows 2 = Mac 4 = Linux

POST Request for fileRule

Description: Creates or updates file rule

Required permissions: 'View files', 'Manage files'

Call syntax: `bit9platform/v1/fileRule`

Name	Source	Type	Description
`value`	FromBody	fileRule	New file rule object

PUT Request for fileRule

Description: Updates existing file rule

Required permissions: 'View files', 'Manage files'

Call syntax: `bit9platform/v1/fileRule/{id}`

Name	Source	Type	Description
`id`	FromUri	Int32	Id of file rule to create or update
`value`	FromBody	fileRule	New file rule object

DELETE Request for fileRule

Description: Delete file rule

Required permissions: 'View files', 'Manage files'

Call syntax: `bit9platform/v1/fileRule/{id}`

Name	Source	Type	Description
`id`	FromUri	Int32	id of file rule for which to delete ban or approval

GET Request for fileRule

Description: Returns object instance of this class

Required permissions: 'View files'

Call syntax: `bit9platform/v1/fileRule/{id}`

Name	Source	Type	Description
`id`	FromUri	Int64	id of a requested object

GET Request for fileRule

Description: Returns objects that match given criteria

Required permissions: 'View files'

Call syntax: `bit9platform/v1/fileRule?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}`

Name	Source	Type	Description
q	FromUri	List`1	Query condition (Optional - multiple query conditions are supported)
group	FromUri	String	Field name to group by (Optional)
sort	FromUri	String	Field name to sort by (Optional)
offset	FromUri	Int32	Offset in query results (Optional)
limit	FromUri	Int32	Maximum number of results to return. When 0 or not present, all results will be returned. When -1, only count will be returned.

» fileUpload

`v1/fileUpload` object exposes all uploaded files from the Bit9 Agents. It also allows requesting or canceling new uploads. Uploaded files can be accessed through the API.

All Object Properties for fileUpload

Name	Type	Property Description
id	Int32	Unique id of this fileUpload
computerId	Int32	Id of `computer` entry associated with this analysis
fileCatalogId	Int32	Id of `fileCatalog` entry associated with this upload

createdBy	String	User that requested upload
dateCreated	DateTime	Date/time when upload was requested (UTC)
dateModified	DateTime	Date/time when upload was last modified by system (UTC)
fileName	String	Name of the file where file exists on the endpoint
pathName	String	Path of the file where file exists on the endpoint
priority	Int32	Upload priority in range [-2, 2], where 2 is highest priority. Default priority is 0
uploadPath	String	Local upload path for this file on the server (can be a shared network path). Note that file is compressed in a ZIP archive
uploadedFileSize	Int64	Size of uploaded file. This will be 0 unless uploadStatus is 3 (Completed)
uploadStatus	Int32	Status of upload. Can be one of: 0 = Queued 1 = Initiated 2 = Uploading 3 = Completed 4 = Error 5 = Cancelled 6 = Deleted

Properties modifiable Using PUT/POST Request for fileUpload

Name	Type	Property Description
computerId	Int32	Id of computer from which to upload the file. If 0, system will find best computer to get the file from
fileCatalogId	Int32	Id of fileCatalog entry for file to upload
priority	Int32	Upload priority in range [-2, 2], where 2 is highest priority. Default priority is 0
uploadStatus	Int32	Status of upload. Status of upload in progress can be changed to 5 (Cancelled). Any upload can be changed to 6 (Deleted)

GET Request for fileUpload

Description: Returns fileUpload object

Required permissions: 'View file uploads'

Call syntax: `bit9platform/v1/fileUpload/{id}?downloadFile={downloadFile}`

Name	Source	Type	Description
`id`	FromUri	Int64	id of a requested fileUpload
`downloadFile`	FromUri	Boolean	Set to true to get binary file back in the response of the message (valid only if uploadStatus is 3). Can return 503 in case when server is overloaded. In that case try again later.

GET Request for fileUpload

Description: Returns object instance of this class

Required permissions: 'View file uploads'

Call syntax: `bit9platform/v1/fileUpload/{id}`

Name	Source	Type	Description
`id`	FromUri	Int64	id of a requested object

GET Request for fileUpload

Description: Returns objects that match given criteria

Required permissions: 'View file uploads'

Call syntax: `bit9platform/v1/fileUpload?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}`

Name	Source	Type	Description
`q`	FromUri	List`1	Query condition (Optional - multiple query conditions are supported)
`group`	FromUri	String	Field name to group by (Optional)
`sort`	FromUri	String	Field name to sort by (Optional)
`offset`	FromUri	Int32	Offset in query results (Optional)
`limit`	FromUri	Int32	Maximum number of results to return. When 0 or not present, all results will be returned. When -1, only count will be returned.

POST Request for fileUpload

Description: Creates or updates file upload request

Required permissions: 'View file uploads', 'Manage uploads of inventoried files'

Call syntax: `bit9platform/v1/fileUpload`

Name	Source	Type	Description
`value`	FromBody	fileUpload	New fileUpload object

PUT Request for fileUpload

Description: Updates existing file upload request

Required permissions: 'View file uploads', 'Manage uploads of inventoried files'

Call syntax: `bit9platform/v1/fileUpload/{id}`

Name	Source	Type	Description
`id`	FromUri	Int32	Id of file rule to create or update
`value`	FromBody	fileUpload	New fileUpload object

» internalEvent

`v1/internalEvent` object exposes public events.

All Object Properties for internalEvent

Name	Type	Property Description
`id`	`Int64`	Unique event Id
`timestamp`	`DateTime`	Date/Time when event was created (UTC)
`receivedTimestamp`	`DateTime`	Date/Time when event was received by the server (UTC)
`description`	`String`	Event description
`type`	`Int32`	Event type. Can be one of: 0 = Server Management 1 = Session Management 2 = Computer Management

		3 = Policy Management 4 = Policy Enforcement 5 = Discovery 6 = General Management 8 = Internal Events
subtype	Int32	Event subtype. Can be one of event subtype IDs
subtypeName	String	Event subtype as string
ipAddress	String	IP address associated with this event
computerId	Int32	Id of computer associated with this event
computerName	String	Name of computer associated with this event
policyId	Int32	Id of policy where agent was at the time of the event
policyName	String	Name of policy where agent was at the time of the event
fileCatalogId	Int32	Id of fileCatalog entry associated with file for this event
installerFileCatalogId	Int32	Id of fileCatalog entry associated with installer for this event
processFileCatalogId	Int32	Id of fileCatalog entry associated with process for this event
fileName	String	Name of the file associated with this event
pathName	String	Path of the file associated with this event
commandLine	String	Full command line associated with this event. Viewing this field requires 'View process command lines' permission
processPathName	String	Name of the process associated with this event
processFileName	String	Path of the process associated with this event
installerFileName	String	Name of the installer associated with this event
processKey	String	Process key associated with this event. This key uniquely identifies the process in both Bit9 Platform and Carbon Black product

severity	Int32	Event severity. Can be one of: 2 = Critical 3 = Error 4 = Warning 5 = Notice 6 = Info 7 = Debug
userName	String	User name associated with this event
ruleName	String	Rule name associated with this event
banName	String	Ban name associated with this event
updaterName	String	Updater name associated with this event
indicatorName	String	Advanced threat indicator name associated with this event
param1	String	Internal string parameter 1
param2	String	Internal string parameter 2
param3	String	Internal string parameter 3
stringId	Int32	Internal string Id used for description

internalEvent is a read-only object and has no modifiable properties.

GET Request for internalEvent

Description: Returns object instance of this class

Required permissions: 'View events'

Call syntax: `bit9platform/v1/internalEvent/{id}`

Name	Source	Type	Description

`id`	FromUri	Int64	id of a requested object

GET Request for internalEvent

Description: Returns objects that match given criteria

Required permissions: 'View events'

Call syntax: `bit9platform/v1/internalEvent?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}`

Name	Source	Type	Description
`q`	FromUri	List`1	Query condition (Optional - multiple query conditions are supported)
`group`	FromUri	String	Field name to group by (Optional)
`sort`	FromUri	String	Field name to sort by (Optional)
`offset`	FromUri	Int32	Offset in query results (Optional)
`limit`	FromUri	Int32	Maximum number of results to return. When 0 or not present, all results will be returned. When -1, only count will be returned.

» meteredExecution

`v1/meteredExecution` object exposes metered executions. This is a read-only object and can only be configured from the Bit9 Console.

All Object Properties for meteredExecution

Name	Type	Property Description
id	Int32	Unique id of this meteredExecution
meterId	Int32	Id of meter associated with this execution
name	String	Name of meter associated with this execution
description	String	Description of meter associated with this execution
type	Int32	How the meter was defined. Can be one of: 1=md5 hash 2=sha1 hash 4=file name 5=sha-256 hash 6=fuzzy sha-256 hash
data	String	Data from definition of meter. Data depends on type, and can be file name or hash
eventId	Int64	Id of event associated with this execution
computerId	Int32	Id of computer associated with this execution
fileCatalogId	Int32	Id of filecatalog entry associated with this execution
timestamp	DateTime	Date/time associated with this execution (UTC)
userName	String	User name associated with this execution

meteredExecution is a read-only object and has no modifiable properties.

GET Request for meteredExecution

Description: Returns object instance of this class

Required permissions: 'View files'

Call syntax: `bit9platform/v1/meteredExecution/{id}`

Name	Source	Type	Description
`id`	FromUri	Int64	id of a requested object

GET Request for meteredExecution

Description: Returns objects that match given criteria

Required permissions: 'View files'

Call syntax: `bit9platform/v1/meteredExecution?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}`

Name	Source	Type	Description
`q`	FromUri	List`1	Query condition (Optional - multiple query conditions are supported)
`group`	FromUri	String	Field name to group by (Optional)
`sort`	FromUri	String	Field name to sort by (Optional)
`offset`	FromUri	Int32	Offset in query results (Optional)
`limit`	FromUri	Int32	Maximum number of results to return. When 0 or not present, all results will be returned. When -1, only count will be returned.

» notification

v1/notification object allows pushing notifications from the Network Connectors through POST request. These notifications can be based on previously requested file analysis, or can come directly from the network appliance, such as firewall.

Properties modifiable Using PUT/POST Request for notification

Name	Type	Property Description
connectorId	Int64	Id of connector object that sent the notification
time	DateTime	Date/time of the notification (UTC)
analysisResult	Int32	Analysis result. Can be one of: 0 = Unknown 1 = Not malicious 2 = Potential risk 3 = Malicious
fileAnalysisId	Int64	Id of fileAnalysis object associated with the notification. This should be available if notification came as a result of the file analysis
fileName	String	File name (Optional)
md5	String	Md5 hash of the file (Optional)
sha256	String	Sha256 hash of the file (Optional)
sha1	String	Sha-1 hash of the file (Optional)
malwareName	String	Name of malware (Optional)
malwareType	String	Type of malware (Optional)
externalUrl	String	External URL showing more details about the results (Optional)
externalId	Int32	External Id (Optional)
severity	String	Severity of notification (Optional)

`type`	`String`	Type of notification (Optional)
`appliance`	`String`	Name of appliance (Optional)
`product`	`String`	Name of product (Optional)
`version`	`String`	Vesion of the product (Optional)
`srcIp`	`String`	Source IP address (Optional)
`srcHost`	`String`	Source computer name (Optional)
`destIp`	`String`	Destination IP address (Optional)
`msgFormat`	`String`	Message format (Optional)
`anomaly`	`String`	Anomaly detected by the appliance (Optional)
`targetApp`	`String`	Application associated with the notification(Optional)
`targetOS`	`String`	Target OS used when analyzing file (Optional)
`httpHeader`	`String`	Http header associated with the notification (Optional)
`status`	`Int32`	Status associated with the notification (Optional)
`srcUsername`	`String`	Source user name associated with the network traffic (Optional)
`destUsername`	`String`	Destination user name associated with the network traffic (Optional)
`flags`	`Int32`	Flags associated with the notification (Optional)
`files`	`NotificationFile[]`	Optional array of file objects with following fields:
• `md5`		Md5 hash of the file (Optional)
• `sha1`		Sha-1 hash of the file (Optional)

• sha256		Sha-256 hash of the file (Optional)
• fileSize		Size of the file (Optional)
• fileName		Name of the file (Optional)
• filePath		Path of the file (Optional)
• processName		Name of the process that created this directory (Optional)
• processPath		Path of the process that created this directory (Optional)
• operation		Operation associated with this directory (Optional)
• topLevel		True if this is a top-level file (Optional)
regKeys	NotificationRegKey[]	Optional array of regkey objects with following fields:
• regKey		Registry key path (Optional)
• regName		Registry key name (Optional)
• regValue		Registry key value (Optional)
• processMd5		Md5 hash of the process that created this directory (Optional)
• Operation		Operation associated with this registry key (Optional)
directories	NotificationDirectory[]	Optional array of directory objects with following fields:
• dirPath		Path of the created directory (Optional)

POST Request for notification

Description: This method posts a notification object. Notification should contain information about analyzed file If possible, Bit9 will match notification with known file and computer information

Required permissions: 'Extend connectors through API'

Call syntax: `bit9platform/v1/notification`

Name	Source	Type	Description
`value`	FromBody	notification	New notification object

» notifier

`v1/notifier` object exposes notifiers that are used in `customRule` and `fileRule` objects. Notifiers are displayed on the agents when file is blocked because of the rule. This is a read-only object and can only be modified from the Bit9 Console.

All Object Properties for notifier

Name	Type	Property Description
`id`	`Int32`	Unique id of this notifier
`name`	`String`	Name of this notifier
`title`	`String`	Notifier dialog title
`messageText`	`String`	Full message text appearing in notifier dialog
`eventLogText`	`String`	Event log text
`url`	`String`	Url link appearing on notifier dialog
`fgImageLocation`	`String`	Foreground image of notifier dialog
`bgImageLocation`	`String`	Background image of notifier dialog

timeout	Int32	Timeout of notifier in seconds
showLogo	Boolean	True to show logo on notifier dialog
logoUrl	String	Url to the logo image
flags	Int32	Notifier flags. Can be 0 or combination of: 1 = Show approval request fields 2 = Show justification fields
systemNotifier	Boolean	True if this is system notifier
defaultRuleType	Int32	Default customRule type for this notifier
defaultRuleGroupId	Int32	Default customRule group Id for this notifier
createdBy	String	User that created this notifier
dateCreated	DateTime	Date/time when notifier was created (UTC)
modifiedBy	String	User that last modified this notifier
dateModified	DateTime	Date/time when notifier was last modified (UTC)
usageCount	Int32	Number of customRule objects that reference this notifier
clVersion	Int64	CL version associated with this notifier

notifier is a read-only object and has no modifiable properties.

GET Request for notifier

Description: Returns object instance of this class

Required permissions: 'View notifiers'

Call syntax: `bit9platform/v1/notifier/{id}`

Name	Source	Type	Description
`id`	FromUri	Int64	id of a requested object

GET Request for notifier

Description: Returns objects that match given criteria

Required permissions: 'View notifiers'

Call syntax: `bit9platform/v1/notifier?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}`

Name	Source	Type	Description
`q`	FromUri	List`1	Query condition (Optional - multiple query conditions are supported)
`group`	FromUri	String	Field name to group by (Optional)
`sort`	FromUri	String	Field name to sort by (Optional)
`offset`	FromUri	Int32	Offset in query results (Optional)
`limit`	FromUri	Int32	Maximum number of results to return. When 0 or not present, all results will be returned. When -1, only count will be returned.

» pendingAnalysis

`v1/pendingAnalysis` object exposes all pending analysis requests for a given connector. Only external connectors can be accessed. Analyzed files can be accessed through the API.

All Object Properties for pendingAnalysis

Name	Type	Property Description
`id`	`Int64`	Unique fileAnalysis id
`priority`	`Int64`	Priority of this file analysis
`uploaded`	`Boolean`	True if file is available
`fileCatalogId`	`Int32`	Id of `fileCatalog` entry associated with this analysis
`connectorId`	`Int32`	Id of `connector` associated with this analysis
`createdBy`	`String`	User that requested this analysis
`dateCreated`	`DateTime`	Date/Time when fileAnalysis request was created (UTC)
`dateModified`	`DateTime`	Date/Time when fileAnalysis request was last modified (UTC)
`fileName`	`String`	Name of the file where file exists on the endpoint
`pathName`	`String`	Path of the file where file exists on the endpoint
`md5`	`String`	Md5 hash of file to be analyzed (if available)
`sha1`	`String`	Sha-1 hash of file to be analyzed (if available)
`sha256`	`String`	Sha-256 hash of file to be analyzed
`uploadPath`	`String`	Local upload path for this file on the server (can be a shared network path). Note that file is compressed in a ZIP archive
`uploadedFileSize`	`Int64`	Size of uploaded file. This will be 0 if analysisStatus is 0 (Scheduled)
`analysisStatus`	`Int32`	Status of analysis. Can be one of: 0 = scheduled 1 = submitted (file is sent for analysis)

		2 = processed (file is processed but results are not available yet) 3 = analyzed (file is processed and results are available) 4 = error 5 = cancelled
`analysisResult`	`Int32`	Result of the analysis. Can be one of: 0 = Not yet available 1 = File is clean 2 = File is a potential threat 3 = File is malicious
`analysisTarget`	`String`	Target of the analysis (Connector-dependent)
`analysisError`	`String`	Error that occurred during analysis

Properties modifiable Using PUT/POST Request for pendingAnalysis

Name	Type	Property Description
`analysisStatus`	`Int32`	Status of analysis. Can be one of: 0 = scheduled 1 = submitted (file is sent for analysis) 2 = processed (file is processed but results are not available yet) 3 = analyzed (file is processed and results are available) 4 = error 5 = cancelled
`analysisResult`	`Int32`	Result of the analysis. Can be set only if analysisStatus is set to 3. Possible values are: 0 = Not yet available 1 = File is clean 2 = File is a potential threat 3 = File is malicious
`analysisError`	`String`	Error that occurred during analysis (can be set only if analysisStatus is set to 4)

GET Request for pendingAnalysis

Description: Returns top N pending analysis requests for a given connector in a descending ordered of priority

Required permissions: 'Extend connectors through API'

Call syntax: `bit9platform/v1/pendingAnalysis?connectorId={connectorId}&maxCount={maxCount}`

Name	Source	Type	Description
`connectorId`	FromUri	Int32	Id of connector for which to return results
`maxCount`	FromUri	Int32	(Optional) Max number of results to return. Defaults to 10

GET Request for pendingAnalysis

Description: Returns pending analysis requests for a given id

Required permissions: 'Extend connectors through API'

Call syntax: `bit9platform/v1/pendingAnalysis/{id}?downloadFile={downloadFile}`

Name	Source	Type	Description
`id`	FromUri	Int64	Pending analysis id
`downloadFile`	FromUri	Boolean	Set to true to get binary file back in the response of the message (valid only if uploaded is true). Can return 503 in case when server is overloaded. In that case try again later.

GET Request for pendingAnalysis

Description: Returns object instance of this class

Required permissions: 'Extend connectors through API'

Call syntax: `bit9platform/v1/pendingAnalysis/{id}`

Name	Source	Type	Description
id	FromUri	Int64	id of a requested object

GET Request for pendingAnalysis

Description: Returns objects that match given criteria

Required permissions: 'Extend connectors through API'

Call syntax: `bit9platform/v1/pendingAnalysis?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}`

Name	Source	Type	Description
q	FromUri	List`1	Query condition (Optional - multiple query conditions are supported)
group	FromUri	String	Field name to group by (Optional)
sort	FromUri	String	Field name to sort by (Optional)
offset	FromUri	Int32	Offset in query results (Optional)
limit	FromUri	Int32	Maximum number of results to return. When 0 or not present, all results will be returned. When -1, only count will be returned.

PUT Request for pendingAnalysis

Description: Updates existing pending analysis requests

Required permissions: 'Extend connectors through API'

Call syntax: `bit9platform/v1/pendingAnalysis`

Name	Source	Type	Description
`value`	FromBody	pendingAnalysis	Pending analysis object to update

---

» policy

`v1/policy` object exposes policy information. This is a read-only object and can only be modified from the Bit9 Console.

All Object Properties for policy

Name	Type	Property Description
`id`	`Int32`	Unique id of this policy
`name`	`String`	Name of this policy
`description`	`String`	Description of this policy
`packageName`	`String`	Name of installer package for this policy
`enforcementLevel`	`Int32`	Target enforcement level. Can be one of: 20=High (Block Unapproved)

		30=Medium (Prompt Unapproved) 40=Low (Monitor Unapproved) 60=None (Visibility) 80=None (Disabled)
disconnectedEnforcementLevel	Int32	Target enforcement level for disconnected computers. Can be one of: 20=High (Block Unapproved) 30=Medium (Prompt Unapproved) 40=Low (Monitor Unapproved) 60=None (Visibility) 80=None (Disabled)
helpDeskUrl	String	Helpdesk URL for notifiers in this policy
imageUrl	String	Image logo URL for notifiers in this policy
dateCreated	DateTime	Date/time when policy was created (UTC)
dateModified	DateTime	Date/time when policy was last modified (UTC)
readOnly	Boolean	True if this policy is read-only
hidden	Boolean	True if this policy is hidden in the UI
automatic	Boolean	True if AD mapping is enabled for this policy
loadAgentInSafeMode	Boolean	True if agents in this policy will be loaded when machine is booted in "safe mode"
reputationEnabled	Boolean	True if reputation approvals are enabled in this policy
fileTrackingEnabled	Boolean	True if file tracking enabled in this policy
customLogo	Boolean	True if notifiers in this policy use custom logo
automaticApprovalsOnTransition	Boolean	True if agents in this policy will automatically locally approve files when transitioning into High Enforcement
allowAgentUpgrades	Boolean	True if agents can be upgraded for this policy

clVersionMax	Int32	Max target CL version for agents in this policy

policy is a read-only object and has no modifiable properties.

GET Request for policy

Description: Returns object instance of this class

Required permissions: 'View policies'

Call syntax: `bit9platform/v1/policy/{id}`

Name	Source	Type	Description
id	FromUri	Int64	id of a requested object

GET Request for policy

Description: Returns objects that match given criteria

Required permissions: 'View policies'

Call syntax: `bit9platform/v1/policy?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}`

Name	Source	Type	Description
q	FromUri	List`1	Query condition (Optional - multiple query conditions are supported)
group	FromUri	String	Field name to group by (Optional)
sort	FromUri	String	Field name to sort by (Optional)

offset	FromUri	Int32	Offset in query results (Optional)
limit	FromUri	Int32	Maximum number of results to return. When 0 or not present, all results will be returned. When -1, only count will be returned.

» publisher

v1/publisher object exposes publisher information and allows changing publisher state (Banning or Approving).

All Object Properties for publisher

Name	Type	Property Description
id	Int32	Unique id of this publisher
name	String	Subject name of leaf certificate for this publisher
description	String	User-defined description for this publisher
modifiedBy	String	User that last modified this publisher
dateCreated	DateTime	Date/time when this publisher was first seen (UTC)
dateModified	DateTime	Date/time when this publisher was last modified (UTC)
publisherReputation	Int32	Reputation of this publisher. Can be one of: 0=Not trusted 1=Low 2=Medium 3=High
publisherState	Int32	State for this publisher. Can be one of: 1=Unapproved

		2=Approved 3=Banned
`policyIds`	`String`	List of IDs of policies where this rule applies. Empty if this is a global rule
`reputationApprovalsEnabled`	`Boolean`	True if publisher can be approved by reputation
`sourceType`	`Int32`	Mechanism that changed publisher state. Can be one of: 1 = Manual 3 = Reputation 5 = External (API)
`firstSeenComputerId`	`Int32`	Id of `computer` where this publisher was first seen
`platformFlags`	`Int32`	Set of platform flags where this publisher will be appoved/banned. combination of: 1 = Windows 2 = Mac 4 = Linux
`signedFilesCount`	`Int32`	Number of files this publisher has signed
`signedCertificateCount`	`Int32`	Number of certificates associated with this publisher
`hidden`	`Boolean`	True if publisher is hidden from the UI (because it was not seen on endpoints or modified yet)
`clVersion`	`Int64`	CL version associated with this publisher

Properties modifiable Using PUT/POST Request for publisher

Name	Type	Property Description
`description`	`String`	User-defined description for this publisher
`publisherState`	`Int32`	State for this publisher. Can be one of: 1=Unapproved 2=Approved 3=Banned

policyIds	String	List of IDs of policies where this rule applies. 0 if this is a global rule
reputationApprovalsEnabled	Boolean	True to enable reputation approvals for this publisher

POST Request for publisher

Description: Change publisher state

Required permissions: 'View software rules pages', 'Manage publisher rules'

Call syntax: `bit9platform/v1/publisher`

Name	Source	Type	Description
value	FromBody	publisher	Publisher object with desired parameters.

PUT Request for publisher

Description: Change publisher state

Required permissions: 'View software rules pages', 'Manage publisher rules'

Call syntax: `bit9platform/v1/publisher/{id}`

Name	Source	Type	Description
id	FromUri	Int32	id of publisher to change
value	FromBody	publisher	Publisher object with desired parameters.

DELETE Request for publisher

Description: Delete publisher ban or approval

Required permissions: 'View software rules pages', 'Manage publisher rules'

Call syntax: `bit9platform/v1/publisher/{id}`

Name	Source	Type	Description
id	FromUri	Int32	id of publisher for which to delete ban or approval

GET Request for publisher

Description: Returns object instance of this class

Required permissions: 'View software rules pages'

Call syntax: `bit9platform/v1/publisher/{id}`

Name	Source	Type	Description
id	FromUri	Int64	id of a requested object

GET Request for publisher

Description: Returns objects that match given criteria

Required permissions: 'View software rules pages'

Call syntax: `bit9platform/v1/publisher?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}`

Name	Source	Type	Description
q	FromUri	List`1	Query condition (Optional - multiple query conditions are supported)
group	FromUri	String	Field name to group by (Optional)
sort	FromUri	String	Field name to sort by (Optional)
offset	FromUri	Int32	Offset in query results (Optional)
limit	FromUri	Int32	Maximum number of results to return. When 0 or not present, all results will be returned. When -1, only count will be returned.

» serverConfig

v1/serverConfig object exposes configuration properties for the server. This is a read-only object. Some of more interesting configuration properties are:

- **API_Version**: Version of this API
- **ParityServerVersion**: Version of this server installation
- **WebServerAddress**: URL of this server
- **BinaryPort**: Port used for agent connections
- **CBServerUrl**: URL of CarbonBlack server if installed
- **ParityServerOSDescription**: OS of this system

All Object Properties for serverConfig

Name	Type	Property Description
id	Int32	Unique id of this serverConfig

name	String	Name of property
value	String	Value of property
dateModified	DateTime	Date/time when this property was last modified (UTC)
modifiedBy	String	User that last modified this property

serverConfig is a read-only object and has no modifiable properties.

GET Request for serverConfig

Description: Returns object instance of this class

Required permissions: 'View system configuration'

Call syntax: `bit9platform/v1/serverConfig/{id}`

Name	Source	Type	Description
id	FromUri	Int64	id of a requested object

GET Request for serverConfig

Description: Returns objects that match given criteria

Required permissions: 'View system configuration'

Call syntax: `bit9platform/v1/serverConfig?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}`

Name	Source	Type	Description

q	FromUri	List`1	Query condition (Optional - multiple query conditions are supported)
group	FromUri	String	Field name to group by (Optional)
sort	FromUri	String	Field name to sort by (Optional)
offset	FromUri	Int32	Offset in query results (Optional)
limit	FromUri	Int32	Maximum number of results to return. When 0 or not present, all results will be returned. When -1, only count will be returned.

» serverPerformance

`v1/serverPerformance` object exposes server performance statistics. This is a read-only object.

All Object Properties for serverPerformance

Name	Type	Property Description
id	Int64	Id of entry. Note id is ordinal in the result set and cannot be persisted/cached
dateCreated	DateTime	Date/Time of the performance entry (UTC)
connectedAgents	Int32	Average number of connected agents
agentFileBacklog	Int64	Size of all agent file change queues
agentProcessingRate	Int64	Daily processing rate from the agent queue
serverFileBacklog	Int64	Size of server file backlog
serverProcessingRate	Int64	Daily processing rate of agent file changes

serverFiles	Int64	Total number of inventory files server is tracking
diskDataWrite	Int64	Disk data file write rate in B/second
diskDataRead	Int64	Disk data file read rate in B/second
diskIndexWrite	Int64	Disk index file write rate in B/second
diskIndexRead	Int64	Disk index file read rate in B/second
diskLogWrite	Int64	Disk log file write rate in B/second
diskDataIOPS	Decimal	Disk data file IOPS
diskIndexIOPS	Decimal	Disk index file IOPS
diskLogIOPS	Decimal	Disk log file IOPS
avgDiskLogWriteStallMs	Decimal	Average disk log file write stall in Ms
avgDiskDataWriteStallMs	Decimal	Average disk data file write stall in Ms
avgDiskIndexWriteStallMs	Decimal	Average disk index file write stall in Ms
avgDiskDataReadStallMs	Decimal	Average disk data file read stall in Ms
avgDiskIndexReadStallMs	Decimal	Average disk index file read stall in Ms
sqlMemoryPressure	Decimal	Memory pressure of SQL server in % of maximum recommended value
sqlLatencyMs	Decimal	Average network latency between Bit9 Server and SQL server in Ms
sqlInsertLatencyMs	Decimal	Average network latency between Bit9 Server and SQL server when inserting data into database in Ms

serverPerformance is a read-only object and has no modifiable properties.

GET Request for serverPerformance

Description: Returns serverPerformance object

Required permissions: 'View system configuration'

Call syntax: `bit9platform/v1/serverPerformance/{id}?period={period}`

Name	Source	Type	Description
`id`	FromUri	Int64	id of a requested policy
`period`	FromUri	Int32	Period for statistics in hours. If omitted, it defaults to 24.

GET Request for serverPerformance

Description: Returns serverPerformance objects that match given criteria

Required permissions: 'View system configuration'

Call syntax: `bit9platform/v1/serverPerformance?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}&period={period}`

Name	Source	Type	Description
`q`	FromUri	List`1	Query parts
`group`	FromUri	String	Group by field
`sort`	FromUri	String	Sort by fields
`offset`	FromUri	Int32	Offset in query results
`limit`	FromUri	Int32	Maximum number of results to return. Omit to get only count of results.
`period`	FromUri	Int32	Period for statistics in hours. If omitted, it defaults to 24.

» updater

v1/updater object exposes updater information and allows enabling/disabling of updaters.

All Object Properties for updater

Name	Type	Property Description
id	Int32	Unique updaterId
name	String	Updater name
version	String	Updater version
enabled	Boolean	True if updater is enabled
dateCreated	DateTime	Date/time when this updater was created (UTC)
createdBy	String	User that created this updater
dateModified	DateTime	Date/time when this updater was last modified (UTC)
modifiedBy	String	User that last modified this updater
clVersion	Int64	CL version associated with this updater
platformFlags	Int32	Set of platform flags where this updater is valid. combination of: 1 = Windows 2 = Mac 4 = Linux

Properties modifiable Using PUT/POST Request for updater

Name	Type	Property Description
enabled	Boolean	True if updater is enabled

POST Request for updater

Description: Change updater state

Required permissions: 'View software rules pages', 'Manage updaters'

Call syntax: `bit9platform/v1/updater`

Name	Source	Type	Description
`value`	FromBody	updater	updater object with desired parameters.

PUT Request for updater

Description: Change updater state

Required permissions: 'View software rules pages', 'Manage updaters'

Call syntax: `bit9platform/v1/updater/{id}`

Name	Source	Type	Description
`id`	FromUri	Int32	id of updater to change
`value`	FromBody	updater	updater object with desired parameters.

GET Request for updater

Description: Returns object instance of this class

Required permissions: 'View software rules pages'

Call syntax: `bit9platform/v1/updater/{id}`

Name	Source	Type	Description
`id`	FromUri	Int64	id of a requested object

GET Request for updater

Description: Returns objects that match given criteria

Required permissions: 'View software rules pages'

Call syntax: `bit9platform/v1/updater?q={q1}&q={q2}...&group={group}&sort={sort}&offset={offset}&limit={limit}`

Name	Source	Type	Description
`q`	FromUri	List`1	Query condition (Optional - multiple query conditions are supported)
`group`	FromUri	String	Field name to group by (Optional)
`sort`	FromUri	String	Field name to sort by (Optional)
`offset`	FromUri	Int32	Offset in query results (Optional)
`limit`	FromUri	Int32	Maximum number of results to return. When 0 or not present, all results will be returned. When -1, only count will be returned.