McAfee Network Security Platform 10.1.x Manager API Reference Guide

Overview

McAfee® Network Security Manager (NSM) provides an Application Programming Interface (API) framework for external applications to access core Network Security Platform (NSP) functionalities through the REST protocol.

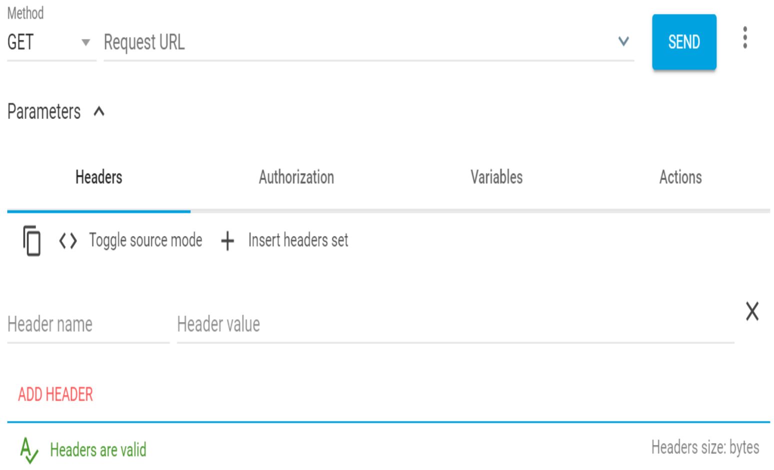
REST stands for Representational State Transfer. It relies on a stateless, client-server and cacheable communication protocol – HTTP. It is an architecture style for designing networked applications. RESTful applications use HTTP requests to post data (create and/or update), get data (query information) and delete data. Thus, REST uses HTTP for all CRUD (Create/Read/Update/Delete) operations. It is a lightweight alternative to mechanisms like RPC (Remote Procedure Calls) and Web Services (SOAP, WSDL, et al.).

SDK API Access

The NSM REST SDK user must authenticate with the Manager by creating a unique "session" resource URL first to make API calls. The session information is then embedded in subsequent API calls to authenticate them.

The steps below walk you through downloading a REST client, creating an API session in the Manager and using the session information to make an API call.

1. To download the Advanced REST client (ARC), which is a free, browser-based REST client, go to https://install.advancedrestclient.com/#/install.
2. Click Download.
3. Once the setup file is downloaded, install it like any setup file installation.
4. Once installed, go to the folder location where the file is downloaded and open ARC (Advanced REST client).

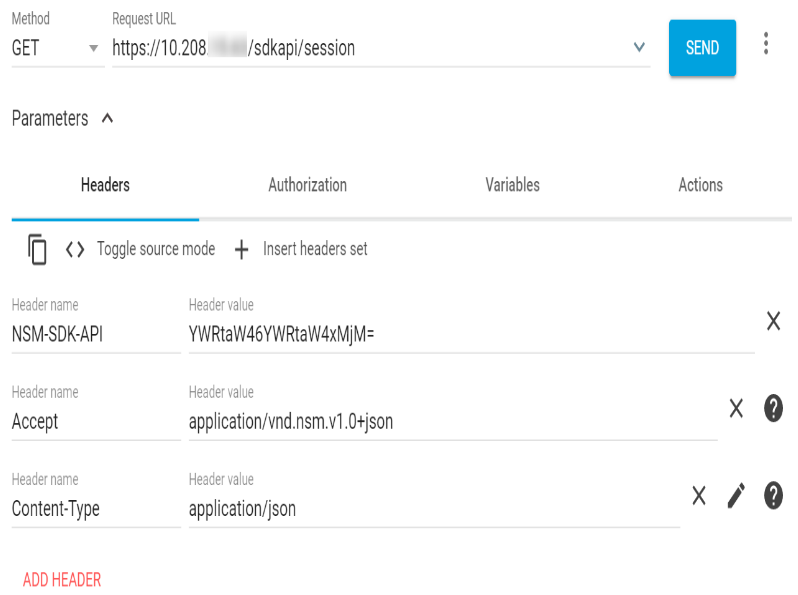


5. Select `GET` from the Method drop-down list.
6. In Request URL, type `https://<nsm_ip>/sdkapi/session`.
7. For Session resource URL, add the following three headers:

   Note: For more headers, select ADD HEADER.

Header Name	Header Value
NSM-SDK-API	<base64 encoded value of Manager credentials, that is `username:userpassword`> **Note:** Base 64 encoded values can be generated at https://www.base64encode.org/. For example, the base 64 encoded value of `admin:admin123` is `YWRtaW46YWRtaW4xMjM=`

Header Name	Header Value
	Note: To make API calls, the user should have the role of a super user in the Manager.
Accept	application/vnd.nsm.v1.0+json
Content-Type	application/json



Method: GET
Request URL: https://10.208.[redacted]/sdkapi/session

Header name: NSM-SDK-API
Header value: YWRtaW46YWRtaW4xMjM=

Header name: Accept
Header value: application/vnd.nsm.v1.0+json

Header name: Content-Type
Header value: application/json

8. Click Send.

Response

```
{ "session": <ABC3AC9AB39EE322C261B733272FC49F> "userId": "1" }
```

9. For other resource urls, In Request URL, type `https://<nsm_ip>/sdkapi/<Resource URL>`.
10. Add the following three headers:

Note: For more headers, select "ADD HEADER."

Header Name	Header Value
NSM-SDK-API	Use the response details obtained in step 8 in https://www.base64encode.org/ to change the header value of the NSM-SDK-API to access other Manager API resources. For example, the base 64 encoded value of `ABC3AC9AB39EE322C261B733272FC49F:1>` is `QUJDM0FDOUFCMzlFRTMyMkMyNjFCNzMzMjcyRkM0OUY6MQ==` **Note:** To make API calls, the user should have the role of a super user in the Manager.
Accept	application/vnd.nsm.v1.0+json **Note:** For a few resource URLs, the parameter value changes. Refer to the table below for different Accept values.
Content-Type	application/json

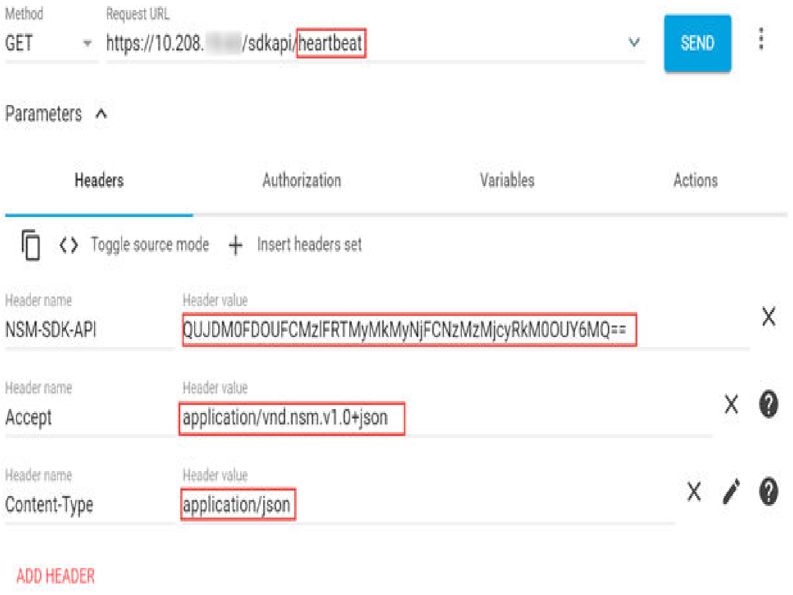
Header Name	Header Value
	Note: For a few resource URLs, the parameter value changes. Refer to the table below for different Content-Type values.

For a few resource URLs, the Accept and Content-Type values also change with the NSM-SDK-API value. Hence, use the table given below for the URLs with different Accept and Content-Type values:

Resource	Resource URL	Method	Content-type value	Accept value
Import the Domain Name Exceptions to the Manager	POST / domainnameexceptions/ import	POST	multipart/form-data; boundary=<x>	
Import custom internal Web Server certificate	PUT /domain/ sslconfiguration/ importinternalwebservercerts	PUT	multipart/form-data; boundary=<x>	
Get the list of importable IPS and Reconnaissance policies	PUT /domain/ <domain_id>/ ipsreconpolicy/import	PUT	multipart/form-data; boundary=<x>	
Import a custom re-sign certificate	PUT /domain/ sslconfiguration/ importresigncert	PUT	multipart/form-data; boundary=<x>	
Nessus Scan Report Import	PUT domain/ <domain_id>/ integration/ vulnerability/ importscanreport	PUT	multipart/form-data; boundary=<x>	
Import a custom trusted CA certificate	PUT /domain/ sslconfiguration/ importtrustedcert	PUT	multipart/form-data; boundary=<x>	
Import the Exceptions	POST /domain/ <domain_id>/ exceptions/import	POST	multipart/form-data; boundary=<x>	
Import the Firewall policies	POST /domain/ <domain_id>/ firewallpolicy/import	POST	multipart/form-data; boundary=<x>	
Import the IPS and Reconnaissance policies	POST /domain/ <domain_id>/ ipsreconpolicy/import	POST	multipart/form-data; boundary=<x>	
Import the Malware policies	POST /domain/ <domain_id>/ malwarepolicy/import	POST	multipart/form-data; boundary=<x>	
Import Custom Fingerprints	PUT /domain/ <domain_id>/	PUT	multipart/form-data; boundary=<x>	

Resource	Resource URL	Method	Content-type value	Accept value
	filereputation/ customfingerprints			
Import Allowed Fingerprints	PUT /domain/ <domain_id>/ filereputation/ allowedfingerprints	PUT	multipart/form-data; boundary=<x>	
Manual Device Software Import to Manager	PUT /devicesoftware/ import/manual	PUT	multipart/form-data; boundary=<x>	
Manual Botnet File Import to Manager	PUT /botnetdetectors/ import/manual	PUT	multipart/form-data; boundary=<x>	
Manual Gateway Anti-Malware File Import to Manager	PUT /gam/import/ manual	PUT	multipart/form-data; boundary=<x>	
Manual Signature Set Import to Manager	PUT /signatureset/ import/manual	PUT	multipart/form-data; boundary=<x>	
Import the Sensor Configuration	PUT /sensor/ <sensor_id>/ importconfiguration	PUT	multipart/form-data; boundary=<x>	
Import SSL Key to the Manager	POST /sensor/ <sensor_id>/action/ sslkey	POST	multipart/form-data; boundary=<x>	
Import License	PUT /vmips/license	PUT	multipart/form-data; boundary=<x>	
Export the public key of the active re-sign certificate	GET /domain/ sslconfiguration/ exportresigncert	GET		application/octet-stream
Export the PCAP file captured	PUT /sensor/ <sensor_id>/ packetcapturepcapfile/ export	PUT		application/octet-stream
Export the Diagnostic Trace file captured	PUT /sensor/ <sensor_id>/ diagnosticstrace/export	PUT		application/octet-stream

For example consider heartbeat resource, in Request URL give `https://<nsm_ip>/sdkapi/heartbeat` and NSM-SDK-API with `QUJDM0FDOUFCMzlFRTMyMkMyNjFCNzMzMjcyRkM0OUY6MQ==`



Method: GET

Request URL: https://10.208.[redacted]/sdkapi/heartbeat

Header name	Header value
NSM-SDK-API	QUJDM0FDOUFCMzlFRTMyMkMyNjFCNzMzMjcyRkM0OUY6MQ==
Accept	application/vnd.nsm.v1.0+json
Content-Type	application/json

11. Click **Send**.

    The response of the resource URL is displayed.

Starting release 9.1, only SSL protocol TLS 1.2 is supported for connection with the Manager. All requests to API use TLS 1.2. On successful authentication, 'Session' resource URL returns the user ID and session ID in the response body. Every resource URL in the SDK is required to pass these credentials for validation and authorization in NSM-SDK-API custom header.

SDK Authentication/Validation

Every request needs to pass a custom header, called NSM-SDK-API. The header will carry a base64 encoded value. If the header is not passed in a request, the request will result into an exception.

Note:

Only a user with "SuperUser" Role is allowed access to SDK APIs. Users with other roles will be allowed to login but will be denied access to SDK APIs.

Version Support

The requested input and output needs to be specified as JSON.

In future releases, multiple versions or different representations of the same Resource will be supported. To accommodate version support, the version of the requested resource should be specified while accessing the resource.

The version requested comes as a part of the "Accept" request header, E.g.,

SDK API Version	Accept Header data
1	application/vnd.nsm.v1.0+json
2	application/vnd.nsm.v2.0+json

"Accept" Request Header is a mandatory parameter. All resources are required to pass the Accept request Header; else the request will be rejected.

Resources

The operation to be performed in a Resource is mentioned as a HTTP verb (`GET/POST/PUT/DELETE`).
The following sections provide details regarding the URIs and actions performed on requesting them.

Session

S.No	Request URI	Actions Allowed	Actions Performed
1	/session	`GET`	Login using credentials specified in NSM-SDK-API request header
2	/session	`DELETE`	Logs off the user

Heartbeat

S.No	Request URI	Actions Allowed	Actions Performed
1	/heartbeat	`GET`	Get the MDR configuration of the Manager
2	/heartbeat	`PUT`	Update MDR configuration of the Manager

Domain

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain	`POST`	Add a new domain
2	/domain/<domain_id>	`PUT`	Update the domain details
3	/domain/<domain_id>	`GET`	Get the specified domain details
4	/domain/<domain_id>	`DELETE`	Delete the specified domain
5	/domain/<domain_id>/ reconpolicies	`GET`	Get the list of recon policies in the domain
6	/domain	`GET`	Get details of all admin domains in the Manager - starting from root AD and all

S.No	Request URI	Actions Allowed	Actions Performed
			child ADs including hierarchy information
7	/domain/<domain_id>	GET	Get details of all child admin domains including hierarchy information in the specified domain

Dashboard Monitors

S.No	Request URI	Actions Allowed	Actions Performed
1	/alerts/TopN/active_botnets	GET	Get top active botnets
2	/alerts/TopN/attack_applications	GET	Get top attack applications
3	/alerts/TopN/attack_subcategories	GET	Get top attack subcategories
4	/alerts/TopN/attacker_countries	GET	Get top attacker countries
5	/alerts/TopN/attackers	GET	Get top attackers
6	/alerts/TopN/attacks	GET	Get top attacks
7	/alerts/TopN/highrisk_hosts	GET	Get top highrisk hosts
8	/alerts/TopN/malware_downloads	GET	Get top malware downloads
9	/alerts/TopN/target_countries	GET	Get top target countries
10	/alerts/TopN/targets	GET	Get top targets
11	/alerts/TopN/unblocked_malware_downloads	GET	Get top unblocked malware downloads
12	/alerts/TopN/endpoint_executables	GET	Get top endpoint executables

Sensor

S.No	Request URI	Actions Allowed	Actions Performed
1	/sensors?domain=<domain_id>	GET	Get the list of Sensors available in

S.No	Request URI	Actions Allowed	Actions Performed
			the specified domain If the domain is not specified, details of all the Sensors in all ADs will be provided
2	/sensor/<sensor_id>	GET	Get details for the specified Sensor
3	/sensor/<sensor_id>/action/update_sensor_config	PUT	Perform configuration update for the specified Sensor
4	/sensor/<sensor_id>/action/update_sensor_config/<request_id>	GET	Get the configuration update status for the specified request id
5	/sensor/<sensor_id>/action/update_sensor_config	GET	Provides the info whether Sensor configuration has been changed and configuration update is pending to the Sensor. The configuration change details are provided as well.

S.No	Request URI	Actions Allowed	Actions Performed
6	/sensor/<sensor_id>/performancestats?metric=<metric>&portId=<port_id>	GET	Provides performance stats for the specified Sensor, metric and port Id
7	/sensor/<sensor_id>/action/reboot	PUT	Reboot the specified Sensor
8	/sensor/<sensor_id>/ipv6	POST	Drop/Pass/Scan IPv6 on the specified Sensor
9	/sensor/<sensor_id>/ipv6	GET	Provides the IPv6 setting (Drop/Pass/Scan) set on the specified Sensor
10	/sensor/<sensor_id>/status	GET	Provides the Sensor status “Active”/”Disconnected”
11	sensor/<sensor_id>/policy/applicationidentification	GET	Get application identification
12	sensor/<sensor_id>/policy/applicationidentification	PUT	Update application identification
13	sensor/<sensor_id>/ntbaintegration	GET	Get NTBA integration configuration
14	sensor/<sensor_id>/ntbaintegration	PUT	Update NTBA integration configuration

S.No	Request URI	Actions Allowed	Actions Performed
15	sensor/<sensor_id>/deploydevicesoftware	GET	Get device software's deployed
16	sensor/<sensor_id>/deploydevicesoftware/<swVersion>	PUT	Upgrade the software on device
17	sensor/<sensor_id>/deploydevicesoftware/<requestId>	GET	Get the upgrade software status

Interface

S.No	Request URI	Actions Allowed	Actions Performed
1	/sensor/<sensor_id>/interface/<interface_id or subinterface_id>	GET	Get interface or sub interface details.
2	/sensor/<sensor_id>/interface/<interface_id or subinterface_id>	PUT	Updates interface or sub interface details.
3	/sensor/<sensor_id>/interface/<interface_id>	POST	Adds a sub interface to the specified interface. The details of sub interface to be created are given in the request body.
4	/sensor/<sensor_id>/interface/<subinterface_id>	DELETE	Deletes the sub interface. Only sub interface can be deleted, if an interface id is mentioned, the

S.No	Request URI	Actions Allowed	Actions Performed
			operation throws an error.
5	/sensor/<sensor_id>/interface/<interface_id or subinterface_id>/vlan	`POST`	Adds a vlan to the specified interface. If a sub interface is given, the VLAN is assigned to the sub interface.
6	/sensor/<sensor_id>/interface/<interface_id or subinterface_id>/vlan/<vlan_ids>	`DELETE`	Revokes vlans from sub interface if subinterface id is mentioned. Deletes vlan from interface if interface id is mentioned. **Note:** multiple comma separated vlans can be provided for this operation.
7	/domain/<domain_id>/sensor/<sensor_id>/availableinterfaces	`GET`	Get the available interface to be allocated.
8	/domain/<domain_id>/sensor/<sensor_id>/allocatedinterfaces	`GET`	Get interfaces allocated to a Sensor inside a domain.
9	/sensor/<sensor_id>/interface/<interface_id>/allocatedcidrlist	`GET`	Get CIDR list allocated to an interface
10	/domain/<domain_id>/sensor/<sensor_id>/allocateinterface	`PUT`	Allocate an interface to a Sensor in child domain.

S.No	Request URI	Actions Allowed	Actions Performed
11	/domain/<domain_id>/sensor/<sensor_id>/interface/<interface_id>/revokeinterface?value=<id>	DELETE	Revoke an interface from a Sensor in child domain.
12	/sensor/<sensor_id>/interface/<interface_id or subinterface_id>/cidr	POST	Adds CIDRs to the specified interface. If a sub interface is given, the CIDRs are assigned to the sub interface.
13	/sensor/<sensor_id>/interface/<interface_id or subinterface_id>/cidr	DELETE	Revokes CIDRs from sub interface if subinterface id is mentioned. Deletes CIDRs from interface if interface id is mentioned.

Port

S.No	Request URI	Actions Allowed	Actions Performed
1	/sensor/<sensor_id>/port/<port_id>/	GET	Get port configuration details for a specific port of a Sensor

Attacks

S.No	Request URI	Actions Allowed	Actions Performed
1	/attacks/	GET	Get all available attack definitions in the Manager
2	/attack/<attack_id>	GET	Get details for a particular attack

IPS Policies

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/ ipspolicies	`GET`	Get all the IPS policies defined in the specific domain
2	/ipspolicy/<policy_id>	`GET`	Get the policy details (including attack set and response actions) for the specific IPS policy
3	/sensor/<sensor_id>/ interface/<interface_id or subinterface_id>/ localipspolicy/	`POST`	Create/Update a light weight policy for a specific interface or sub-interface
4	/sensor/<sensor_id>/ interface/<interface_id or subinterface_id>/ localipspolicy/	`GET`	Get the details of a light weight policy associated with a specific interface or sub-interface
5	/sensor/<sensor_id>/ interface/<interface_id or subinterface_id >/ localipspolicy/	`DELETE`	Delete a light weight policy associated with a specific interface or sub-interface
6	/domain/<domainId>/ ipspolicies/createips	`POST`	Create new IPS policy
7	/ipspolicy/<policyId>	`PUT`	Update IPS policy
8	/ipspolicy/<policyId>	`DELETE`	Delete IPS policy

Attack Filters

S.No	Request URI	Actions Allowed	Actions Performed
1	/attackfilter/	`POST`	Add a new attack filter
2	/attackfilter/<attackfilter_id>	`PUT`	Update attack filter
3	/attackfilter/<attackfilter_id>	`DELETE`	Delete attack filter
4	/attackfilter/<attackfilter_id>	`GET`	Get attack filter details
5	/attackfilters? domain=<domain_id>	`GET`	Get all attack filters defined in the specified domain
6	/domain/< domain_id>/ attackfilter	`POST`	Assign the specified attack filters to a particular domain and attack

S.No	Request URI	Actions Allowed	Actions Performed
7	/domain/<domain_id>/ attackfilter/<attack_id>	`GET`	Get all the attack filters assigned to the domain for a specific attack
8	/domain/<domain_id>/ attackfilter/<attack_id>	`DELETE`	Delete all the attack filters assigned to the domain for a specific attack
9	/sensor/<sensor_id>/ attackfilter	`POST`	Assign the specified attack filters to a particular sensor and attack
10	/sensor/<sensor_id>/ attackfilter/<attack_id>	`GET`	Get all the attack filters assigned to the sensor for a specific attack
11	/sensor/<sensor_id>/ attackfilter/<attack_id>	`DELETE`	Delete all the attack filters assigned to the sensor for a specific attack
12	/sensor/<sensor_id>/ interface/<interface_id or subinterface_id>/attackfilter	`POST`	Assigns the specified attack filters to a particular Interface or sub interface and attack
13	/sensor/<sensor_id>/ interface/<interface_id or subinterface_id>/attackfilter/ <attack_id>	`GET`	Get all the attack filters assigned to an Interface or sub interface for a specific attack
14	/sensor/<sensor_id>/ interface/<interface_id or subinterface_id>/attackfilter/ <attack_id>	`DELETE`	Delete all the attack filters assigned to an Interface or sub interface for a specific attack
15	/attackfilter/<attackfilter_id/ assignments	`GET`	Get all assignments of an attack filter across all attacks and resources

Rule Objects

S.No	Request URI	Actions Allowed	Actions Performed
1	/ruleobject	`POST`	Add a new rule object
2	/ruleobject/<ruleobject_id>	`PUT`	Update a rule object
3	/ruleobject/<ruleobject_id>	`DELETE`	Delete a rule object
4	/ruleobject/<ruleobject_id>	`GET`	Get a particular rule object

S.No	Request URI	Actions Allowed	Actions Performed
5	/ruleobject/<ruleobject_id>/ assignments	`GET`	Get the associations of rule objects in all the modules where it is being used
6	/domain/<domain_id>/ ruleobject? type=<ruleobject_type>	`GET`	Get the list of rule objects defined in a particular domain Query Parameter: **?type=** • application • applicationgroup • applicationoncustomport • country • finitetimeperiod • hostdnsname • hostipv4 • hostipv6 • ipv4addressrange • ipv6addressrange • networkipv4 • networkipv6 • networkgroup • recurringtimeperiod • recurringtimeperiodgroup • service • servicerange • servicegroup
7	/ruleobject/user? filter=<user_name_filter> &maxcount=<max_entries_expected>	`GET`	Get the user rule objects matching to a particular filter string
8	/ruleobject/usergroup	`GET`	Get the user group rule objects

Firewall Policies

S.No	Request URI	Actions Allowed	Actions Performed
1	/firewallpolicy	`POST`	Add a new firewall policy and access rules
2	/firewallpolicy/ <policy_id>	`PUT`	Update the firewall policy details
3	/firewallpolicy/ <policy_id>	`DELETE`	Delete the specified firewall policy
4	/firewallpolicy/ <policy_id>	`GET`	Get the policy details

S.No	Request URI	Actions Allowed	Actions Performed
5	/domain/<domain_id>/ firewallpolicy/	GET	Get the list of firewall policies defined in a particular domain

Scanning Exception

S.No	Request URI	Actions Allowed	Actions Performed
1	/sensor/<sensor_id>/ scanningexception	POST	Create a new scanning exception on a Sensor
2	/sensor/<sensor_id>/ scanningexception	GET	Get the scanning exceptions defined on a Sensor
3	/sensor/<sensor_id>/ scanningexception	DELETE	Delete a scanning exception on a Sensor
4	/sensor/<sensor_id>/ scanningexception/ status	PUT	Enable/Disable scanning exception on a Sensor
5	/sensor/<sensor_id>/ scanningexception/ status	GET	Get the scanning exception Enable/ Disable status on Sensor

IPS Quarantine

S.No	Request URI	Actions Allowed	Actions Performed
1	/sensor/<sensor_id>/ action/quarantinehost	POST	Quarantine a host for a particular duration on the specified Sensor
2	/sensor/<sensor_id>/ action/quarantinehost	PUT	Update the quarantine duration for the specified host
3	/sensor/<sensor_id>/ action/quarantinehost/ <IPAddress>	DELETE	Releases the specified quarantined host
4	/sensor/<sensor_id>/ action/quarantinehost	GET	Get the list of quarantined hosts on the specific Sensor

S.No	Request URI	Actions Allowed	Actions Performed
5	/sensor/<sensor_id>/action/quarantinehost/details	GET	Get the list of quarantined hosts with details on the specific Sensor/domain

Connection Limiting Policies

S.No	Request URI	Actions Allowed	Actions Performed
1	/connectionlimitingpolicy	POST	Add a new connection limiting policy
2	/connectionlimitingpolicy/<policy_id>	PUT	Update a connection limiting policy
3	/connectionlimitingpolicy/<policy_id>	GET	Get a connection limiting policy
4	/connectionlimitingpolicy/<policy_id>	DELETE	Delete a connection limiting policy
5	/connectionlimitingpolicy/countrylist	GET	Get the available country list
6	/domain/<domain_id>/connectionlimitingpolicies	GET	Get all the connection limiting policies defined in the specified domain

Non Standard Ports

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/nonstandardports	POST	Add a non-standard port on the specified domain
2	/sensor/<sensor_id>/nonstandardports	POST	Add a non-standard port on the specified Sensor
3	/domain/<domain_id>/nonstandardports	GET	Get all the non-standard ports configured on the specified domain
4	/sensor/< sensor _id>/nonstandardports	GET	Get all the non-standard ports configured on the specified Sensor

S.No	Request URI	Actions Allowed	Actions Performed
5	/domain/<domain_id>/ nonstandardports? transport=<transport_type>&nonStandardPortNumber=<port_number>	DELETE	Delete a non-standard port configured on the specified domain
6	/sensor/<sensor_id>/ nonstandardports? transport=<transport_type>&nonStandardPortNumber=<port_number>	DELETE	Delete a non-standard port configured on the specified Sensor

SSL Key

S.No	Request URI	Actions Allowed	Actions Performed
1	/sensor/<sensor_id>/action/ sslkey	POST	Import SSL key for the Sensor. Not applicable for 9.2 NS-series Sensors.
2	/sensor/<sensor_id>/action/ sslkey /<ssl_id>	DELETE	Delete SSL key on the Sensor. Not applicable for 9.2 NS-series Sensors.
3	/sensor/<sensor_id>/action/ sslkey	GET	Get SSL keys present on the Sensor. Not applicable for 9.2 NS-series Sensors.
4	/sensor/<sensor_id>/ sslconfiguration	GET	Get the SSL configuration on the Sensor. Not applicable for 9.2 NS-series Sensors.
5	/sensor/<sensor_id>/ sslconfiguration	PUT	Update the SSL configuration on the Sensor. Not applicable for 9.2 NS-series Sensors.
6	/domain/<domainId>/ sslconfiguration	GET	Get the SSL configuration at domain level
7	/domain/<domainId>/ sslconfiguration	PUT	Update the SSL configuration on domain
8	/domain/<domainId>/ sslconfiguration/resigncert	GET	Get the re-sign certificate on the Manager
9	/domain/sslconfiguration/ generateresigncert	GET	Re-generate the default re-sign certificate
10	/domain/<domainId>/ sslconfiguration/ exportresigncert	GET	Export the public key of the active re-sign certificate
11	/domain/sslconfiguration/ importresigncert	PUT	Import a custom re-sign certificate

S.No	Request URI	Actions Allowed	Actions Performed
12	/domain/sslconfiguration/trustedcerts	GET	Get all the trusted CA certificates
13	/domain/sslconfiguration/trustedcert	GET	Get a single trusted CA certificate
14	/domain/sslconfiguration/updatetrustedcertstate	PUT	Enable or disable multiple trusted CA certificates
15	/domain/sslconfiguration/updatedefaulttrustedcerts	GET	Update the default trusted CA certificates
16	/domain/sslconfiguration/importtrustedcert	PUT	Import a custom trusted CA certificate
17	/domain/sslconfiguration/deletetrustedcerts	DELETE	Delete multiple trusted CA certificates
18	/domain/sslconfiguration/internalwebservercerts	GET	Get all the internal web server certificates
19	/domain/sslconfiguration/importinternalwebservercerts	PUT	Import multiple internal web server certificates
20	/domain/sslconfiguration/deleteinternalwebservercerts	DELETE	Delete internal web server certificates
21	/domain/sslconfiguration/inboundproxyrules	GET	Get all the inbound proxy rules created on the Manager
22	/domain/sslconfiguration/inboundproxyruledetail/<ruleId>	GET	Get detail of the given inbound proxy rule id
23	/domain/sslconfiguration/inboundproxyrules	POST	Add inbound proxy rule
24	/domain/sslconfiguration/inboundproxyrules/<ruleId>	PUT	Update inbound proxy rule
25	/domain/sslconfiguration/inboundproxyrules	DELETE	Delete multiple inbound proxy rules
26	/sensor/<sensor_id>/decryptionsettings	GET	Get the SSL configuration on Sensor. Applicable for 9.2 NS-series Sensors.
27	/sensor/<sensor_id>/decryptionsettings	PUT	Update the SSL configuration on Sensor. Applicable for 9.2 NS-series Sensors.

Rate Limiting Profiles

S.No	Request URI	Actions Allowed	Actions Performed
1	/ratelimitingprofile	POST	Add a rate limiting profile
2	/ratelimitingprofile/<profile_id>	PUT	Update the rate limiting profile details
3	/ratelimitingprofile/<profile_id>	DELETE	Delete the specified rate limiting profile
4	/ratelimitingprofile/<profile_id>	GET	Get the rate limiting profile details
5	/domain/<domain_id>/ratelimitingprofiles	GET	Get the list of rate limiting profiles defined in a particular domain

QoS Policy

S.No	Request URI	Actions Allowed	Actions Performed
1	/qospolicy	POST	Add a QoS policy and rules
2	/qospolicy/<policy_id>	PUT	Update the QoS policy details
3	/qospolicy/<policy_id>	DELETE	Delete the specified QoS policy
4	/qospolicy/<policy_id>	GET	Get the QoS policy details
5	/domain/<domain_id>/qospolicy	GET	Get the list of QoS policies defined in a particular domain

Advanced Malware Policy

S.No	Request URI	Actions Allowed	Actions Performed
1	/malwarepolicy	POST	Add an advanced malware policy
2	/malwarepolicy/<policy_id>	PUT	Update the malware policy details
3	/malwarepolicy/<policy_id>	DELETE	Delete the specified malware policy
4	/malwarepolicy/<policy_id>	GET	Get the malware policy details

S.No	Request URI	Actions Allowed	Actions Performed
5	/domain/<domain_id>/ malwarepolicy	GET	Get the list of malware policies defined in a particular domain
6	/malwarepolicy/ defaultscanningoptions	GET	Get the default scanning options configuration
7	/malwarepolicy/ malwareprotocols	GET	Get the supported malware protocols list
8	/advancedmalware/ blockedhashes? search=<search_string>	GET	Get the list of blocked hashes
9	/advancedmalware/ allowedhashes? search=<search_string>	GET	Get the list of allowed hashes
10	/advancedmalware/ blockedhashes /<hash>/ takeaction/<action>	PUT	Move the hashes from blocked to allowed
11	/advancedmalware / allowedhashes/<hash>/ takeaction/<action>	PUT	Move the hashes from allowed to blocked
12	/advancedmalware/ blockedhashes/multipleHash/ takeaction/allow	PUT	Moves multiple hashes from blocked to allowed
13	/advancedmalware/ allowedhashes/multipleHash/ takeaction/block	PUT	Moves multiple hashes from allowed to blocked
14	/advancedmalware/ blockedhashes/takeaction/ removeall	PUT	Removes all the blocked hashes
15	/advancedmalware / allowedhashes/takeaction/ removeall	PUT	Removes all the allowed hashes
16	/advancedmalware? type=<hashtype>	POST	Add a hash file to either a block list or an allow list
17	/advancedmalware? type=<hashtype>	PUT	Update the details of file hash
18	/advancedmalware? type=<hashtype>	DELETE	Delete multiple file hashes

File Reputation

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/filereputation/gti	PUT	Update severity for GTI
2	/domain/<domain_id>/filereputation/allowedfingerprints	PUT	Import the list of allowed fingerprints to the Manager
3	/domain/<domain_id>/filereputation/allowedfingerprints	DELETE	Delete the allowed fingerprints imported in the Manager
4	/domain/<domain_id>/filereputation/customfingerprints	PUT	Import the list of custom fingerprints to the Manager
5	/domain/<domain_id>/filereputation/customfingerprints	DELETE	Delete the custom fingerprints imported in the Manager
6	/domain/<domain_id>/filereputation/filetypes	PUT	Provide the supported file types/formats to be scanned
7	/domain/<domain_id>/filereputation/fingerprintscount	GET	Provide the count of custom and allowed fingerprints in use

Alert Relevance

S.No	Request URI	Actions Allowed	Actions Performed
1	/alertrelevance	PUT	Enable/Disable alert relevance
2	/alertrelevance	GET	Get the current status of alert relevance

Manage Import

S.No	Request URI	Actions Allowed	Actions Performed
1	/botnetdetectors/import/automatic	PUT	Automatically downloads the latest botnet file from Update Server to Manager
2	/botnetdetectors/import/manual	PUT	Import the botnet file manually to Manager

S.No	Request URI	Actions Allowed	Actions Performed
3	/signatureset/import/manual	`PUT`	Import the signature set file manually to Manager
4	/devicesoftware/import/manual	`PUT`	Import the device software file manually to Manager
5	/botnetdetectors/version	`GET`	Get the botnet version in the Manager
6	/gam/import/manual	`PUT`	Import the Gateway Anti-Malware engine file manually to Manager
7	/devicesoftware/import/automatic	`PUT`	Download the device software from the server
8	/devicesoftware/versions	`GET`	Get the device software's available in the server
9	signatureset/available/version	`GET`	Get the signature sets available in the server
10	botnetdetectors/available/version	`GET`	Get the callback detectors available in the server

Malware Archive

S.No	Request URI	Actions Allowed	Actions Performed
1	/malwarearchive/action	`PUT`	This URL adds the filehash to the allow list
2	/malwarearchive/download/<filehash>	`GET`	Download the malware file as Base64 encoded ByteStream
3	/malwarearchive/list	`GET`	Get the list of malware files currently archived on the Manager
4	/malwarearchive?fileHash=	`DELETE`	Delete the malware file query Parameter: ?fileHash= 1. · fileHashValue If the filehash value is not provided, all the archived files will be deleted

Passive Device Profiling

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/passivedeviceprofiling	GET	Get passive device profiling setting at the domain level
2	/domain/<domain_id>/passivedeviceprofiling	PUT	Update passive device profiling setting at the domain level
3	/sensor/<sensor_id>/passivedeviceprofiling	GET	Get passive device profiling setting at the Sensor level
4	/sensor/<sensor_id>/passivedeviceprofiling	PUT	Update passive device profiling setting at the Sensor level

Alert Exception

S.No	Request URI	Actions Allowed	Actions Performed
1	/alertexception	POST	Adds a alert exception
2	/alertexception/{alertExceptionID}	GET	Get the alert exception details
3	/alertexception	GET	Get all the alert exception available
4	/alertexception/{alertExceptionID}	DELETE	Delete the alert exception

Global Auto Acknowledgment

S.No	Request URI	Actions Allowed	Actions Performed
1	/globalautoack	PUT	Configure global auto ack setting
2	/globalautoack	GET	Get global auto ack setting
3	/globalautoack/attack/<search_string>	GET	Get attacks for rules configuration
4	/globalautoack/rules	GET	Get global auto ack rules
5	/globalautoack/rules/<rule_id>	POST	Get global auto ack rule

S.No	Request URI	Actions Allowed	Actions Performed
6	/globalautoack/rules	POST	Create global auto ack rules
7	/globalautoack/rules/<rule_id>	POST	Update global auto ack rules

Name Resolution Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/nameresolution	PUT	Updates name resolution setting at the domain level
2	/domain/<domain_id>/nameresolution	GET	Retrieves name resolution setting at the domain level
3	/sensor/<sensor_id>/nameresolution	PUT	Updates name resolution setting at the Sensor level
4	/sensor/<sensor_id>/nameresolution	GET	Retrieves name resolution setting at the Sensor level

Device Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/device	POST	Creates a device in the Manager
2	/domain/<domainId>/device/<device_id>	GET	Retrieves the device detail
3	/domain/<domainId>/device/<device_id>	PUT	Updates the device
4	/domain/<domainId>/device/<device_id>	DELETE	Deletes the device
5	/domain/<domainId>/device	GET	Retrieves all the device available in the domain

NTBA Monitors

S.No	Request URI	Actions Allowed	Actions Performed
1	/ntbamonitors	GET	Retrieves the available NTBA monitors

S.No	Request URI	Actions Allowed	Actions Performed
2	/ntbamonitors/{ntbaId}/ hoststhreatfactor? TopN=<TopN> &timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>	GET	Retrieves the list of hosts threat factors details
3	/ntbamonitors/{ntbaId}/ topurls? TopN=<TopN> &timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>	GET	Retrieves the list of top URLs details
4	/ntbamonitors/{ntbaId}/ topzoneurls/<zoneid>	GET	Retrieves the list of top zone URLs details
5	/ntbamonitors/{ntbaId}/ tophosturls/<hostId >	GET	Retrieves the list of top host URLs details
6	/ntbamonitors/{ntbaId}/ topurlsbyreputation? TopN=<TopN> &timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>	GET	Retrieves the list of top URLs by reputation details
7	/ntbamonitors/{ntbaId}/ showurlactivity/ {urlid}? TopN=<TopN> &timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>	GET	Retrieves the list of URL activity details
8	/ntbamonitors/{ntbaId}/ topurlsbycategory? TopN=<TopN> &timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>	GET	Retrieves the list of top URLs category details
9	/ntbamonitors/{ntbaId}/ topurlsbycategory/ <category_id>? TopN=<TopN> &timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>	GET	Retrieves the details of top URLs detail by category ID
10	/ntbamonitors/{ntbaId}/ topfiles? TopN=<TopN> &timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>	GET	Retrieves the list of top file details
11	/ntbamonitors/{ntbaId}/ topzonefiles/<zone_id	GET	Retrieves the list of top zone file details
12	/ntbamonitors/{ntbaId}/ tophostfiles/<host_id	GET	Retrieves the detail of top host files by Id

S.No	Request URI	Actions Allowed	Actions Performed
13	/ntbamonitors/{ntbaId}/ fileactivity/{fileid}? TopN=<TopN> &timePeriod=<timePeriod>&startTime= <startTime>&endTime=<endTime>	GET	Retrieves the list of file activity details
14	/ntbamonitors/{ntbaId}/ topexthostsbyreputation? TopN=<TopN> &timePeriod=<timePeriod>&startTime= <startTime>&endTime=<endTime>	GET	Retrieves the list of top external host by reputation details
15	/ntbamonitors/{ntbaId}/ newhosts? TopN=<TopN>	GET	Retrieves the details of new hosts
16	/ntbamonitors/{ntbaId}/ activehosts? TopN=<TopN> &timePeriod=<timePeriod>&startTime= <startTime>&endTime=<endTime>	GET	Retrieves the list of active hosts details
17	/ntbamonitors/{ntbaId}/ tophoststraffic? TopN=<TopN> &startTime=<startTime>&endTime= <endTime>&direction=<direction>	GET	Retrieves the list of top hosts traffic details
18	/ntbamonitors/{ntbaId}/ applicationtraffic? TopN=<TopN> &startTime=<startTime>&endTime= <endTime>&direction=<direction>&frequency=<frequency>	GET	Retrieves the list of application on traffic details
19	/ntbamonitors/{ntbaId}/ applicationtraffic/ profile/{appId}? startTime=<startTime>&endTime= <endTime>	GET	Retrieves the list of application on traffic details for app ID
20	/ntbamonitors/{ntbaId}/ throughputtraffic? TopN=<TopN> &startTime=<startTime>&endTime= <endTime&frequency=<frequency>	GET	Retrieves the list of through put traffic details list
21	/ntbamonitors/{ntbaId}/ bandwidthutilization? TopN=<TopN>	GET	Retrieves the list of bandwidth utilization by retrieves
22	/ntbamonitors/{ntbaId}/ zonetraffic? TopN=<TopN> &direction=<direction>&frequency= <frequency>	GET	Retrieves the list of zone traffic details

S.No	Request URI	Actions Allowed	Actions Performed
23	/ntbamonitors/{ntbaId}/ activeservices? TopN=<TopN> &timePeriod=<timePeriod>&startTime= <startTime>&endTime=<endTime>	GET	Retrieves the list of active users
24	/ntbamonitors/{ntbaId}/ tophostactiveservices/ <host_id>? TopN=<TopN> &timePeriod=<timePeriod>&startTime= <startTime>&endTime=<endTime>	GET	Retrieves the list of top host active users
25	/ntbamonitors/{ntbaId}/ newservices? TopN=<TopN>	GET	Retrieves the list of new services
26	/ntbamonitors/{ntbaId}/ activeapplications? TopN=<TopN> &timePeriod=<timePeriod>&startTime= <startTime>&endTime=<endTime>	GET	Retrieves the list of active applications
27	/ntbamonitors/{ntbaId}/ newapplications? TopN=<TopN>	GET	Retrieves the list of new applications
28	/ntbamonitors/{ntbaId}/ tophostactiveapplications/ <host_id>? TopN=<TopN> &timePeriod=<timePeriod>&startTime= <startTime>&endTime=<endTime>	GET	Retrieves the list of top host active applications
29	/ntbamonitors/{ntbaId}/ tophostports/ <host_id>? TopN=<TopN> &timePeriod=<timePeriod>&startTime= <startTime>&endTime=<endTime>	GET	Retrieves the list of top host ports

Endpoint Executables Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/<nbaid>/ endpointintelligence? search=<search_string>&& confidencetype=<confidencetype>&& classificationtype=<classificationtype>&&duration=<duration>	GET	Retrieves the list of executables running on your internal endpoints

S.No	Request URI	Actions Allowed	Actions Performed
2	/<nbaid>/ endpointintelligence/<hash>/ executableinformation? duration=<duration>	GET	Retrieves the executable information for given hash value
3	/<nbaid>/ endpointintelligence/<hash>/ endpoints? duration=<duration>	GET	Retrieves the endpoints information
4	/<nbaid>/ endpointintelligence/<hash>/ applications? duration=<duration>	GET	Retrieves the applications information
5	/<nbaid>/ endpointintelligence/<hash>/ events? duration=<duration>	GET	Retrieves the events information
6	/<nbaid>/ endpointintelligence/<hash>/ takeaction/<action>	PUT	Updates the hash to make it allow/block/classified

NMS IP Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id> / nmsips	GET	Retrieves the NMS IPs at the domain
2	/domain/<domain_id> /nmsip	POST	Creates the NMS IP at the domain
3	/domain/<domain_id> /nmsip/ <ipId>	DELETE	Deletes the NMS IP at the domain
4	/sensor/<sensor_id> /nmsips	GET	Retrieves the NMS IPs at the Sensor
5	/sensor/<sensor_id> /nmsips/ available	GET	Retrieves the NMS IPs available to allocate to the Sensor
6	/sensor/<sensor_id> /nmsip	POST	Creates the NMS IP at the Sensor
7	/sensor/<sensor_id> /nmsip/ allocate/<ipId>	POST	Allocates the NMS IP to the Sensor
8	/sensor/<sensor_id> /nmsip	DELETE	Deletes the NMS IP at the Sensor

NMS Users Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id> / nmsusers	GET	Retrieves the NMS users at the domain
2	/domain/<domain_id> / nmsuser	POST	Creates the NMS user at the domain
3	/domain/<domain_id> / nmsuser/<nmsuser_id>	PUT	Updates the NMS user at the domain
4	/domain/<domain_id> / nmsuser/<nmsuser_id>	GET	Retrieves the NMS user details at the domain
5	/domain/<domain_id> / nmsuser/<nmsuser_id>	DELETE	Deletes the NMS user at the domain
6	/sensor/<sensor_id> / nmsusers	GET	Retrieves the NMS users at the Sensor
7	/sensor/<sensor_id> / nmsusers/available	GET	Retrieves the available NMS users for allocation to the Sensor
8	/sensor/<sensor_id> /nmsuser	POST	Creates the NMS user at the Sensor
9	/sensor/<sensor_id> / nmsuser/<nmsuser_id>	POST	Allocates the NMS user to the Sensor
10	/sensor/<sensor_id> / nmsuser/<nmsuser_id>	PUT	Updates the NMS user at the Sensor
11	/sensor/<sensor_id> / nmsuser/<nmsuser_id>	GET	Retrieves the NMS user details at the Sensor
12	/sensor/<sensor_id> / nmsuser/<nmsuser_id>	DELETE	Deletes the NMS user at the Sensor

Policy Export Import Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/ ipsreconpolicy/import	PUT	Retrieves the importable IPS reconnaissance policies at the domain from the XML file

S.No	Request URI	Actions Allowed	Actions Performed
2	/domain/<domain_id>/ ipsreconpolicy/import	`POST`	Imports the IPS reconnaissance policies from the XML file to the domain
3	/domain/<domain_id>/ malwarepolicy/import	`POST`	Imports the malware policies from the XML file to the domain
4	/domain/<domain_id>/ firewallpolicy/import	`POST`	Imports the firewall policies from the XML file to the domain
5	/domain/<domain_id>/ exceptions/import	`POST`	Imports the exceptions from the XML file to the domain

TCP Settings Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/sensor/<sensor_id>/ tcpsettings	`PUT`	Updates TCP settings on a Sensor
2	/sensor/<sensor_id>/ tcpsettings	`GET`	Retrieves TCP settings on a Sensor

IP Settings Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/sensor/<sensor_id>/ ipsettings	`PUT`	Updates IP settings on a Sensor
2	/sensor/<sensor_id>/ ippsettings	`GET`	Retrieves IP settings on a Sensor

Firewall Logging Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/sensor/<sensor_id>/ firewalllogging	`PUT`	Updates the firewall logging details for the Sensor
2	/sensor/<sensor_id>/ firewalllogging	`GET`	Retrieves the firewall logging details for the Sensor

IPS Alerting Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/sensor/<sensor_id>/ ipsalerting/alertsuppression	`PUT`	Updates the alert suppression details for the Sensor
2	/sensor/<sensor_id>/ ipsalerting/alertsuppression	`GET`	Retrieves the alert suppression details for the Sensor

Failover Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/ failoverpair	`POST`	Adds a new failover pair
2	/domain/<domain_id>/ failoverpair/<failoverpair_id>	`GET`	Retrieves the failover pair details
3	/domain/<domain_id>/ failoverpair	`GET`	Retrieves the list of failover pair details in the domain
4	/domain/<domain_id>/ failoverpair/<failoverpair_id>	`DELETE`	Deletes the specified failover pair

Syslog Firewall Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/ notification/firewall/syslog	`GET`	Retrieves the syslog configuration for firewall notification
2	domain/<domain_id>/ notification/firewall/syslog	`PUT`	Creates the syslog configuration for firewall notification

Syslog Faults Notification Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/ notification/faults/syslog	GET	Retrieves the syslog configuration for faults notification
2	/domain/<domain_id>/ notification/faults/syslog	PUT	Creates the syslog configuration for faults notification

Tacacs Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	domain/<domain_id>/ remoteaccess/tacacs	GET	Retrieves the Tacacs configuration
2	domain/<domain_id>/ remoteaccess/tacacs	PUT	Creates the Tacacs configuration

Active Botnets Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/ activebotnets? includeChildDomain=<includeChildDomain> &&duration=<duration>	GET	Retrieves the list of active botnets
2	/domain/<domain_id>/ activebotnetzombies/ <bot_id>? includeChildDomain=<includeChildDomain> &&duration=<duration>	GET	Retrieves the list of zombies for an active botnet

Automatic Update Configuration Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	autoupdateconfiguration/ sigset	GET	Retrieves the signature set automatic update configuration on the Manager

S.No	Request URI	Actions Allowed	Actions Performed
2	autoupdateconfiguration/ botnet	GET	Retrieves the botnet automatic update configuration on the Manager
3	/autoupdateconfiguration/ sigsetdownloadconfig	PUT	Updates the automatic signature set download configuration
4	/autoupdateconfiguration/ botnetdownloadconfig	PUT	Updates the automatic botnet download configuration
5	/autoupdateconfiguration/ sigsetdeploymentconfig	PUT	Updates the automatic signature set deployment configuration
6	/autoupdateconfiguration/ botnetdeploymentconfig	PUT	Updates the automatic botnet deployment configuration

Malware Downloads Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/ malwaredownloads? duration=<duration>&resultType=<resultType> &confidenceType=<confidenceType>& includeChildDomain=<includeChildDomain>	GET	Retrieves malware downloads summary
2	/domain/<domain_id>/ malwaredownloads/filehash/ {fileHash}? duration=<duration>&resultType=<resultType> &confidenceType=<confidenceType> &includeChildDomain=<includeChildDomain>	GET	Retrieves malware alerts respect to the file hash

Nessus Scan Report Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/ integration/vulnerability/ importscanreport	PUT	Import NESSUS scan report

ATD Configuration Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/ ipsdevices/atdintegration	GET	Retrieves ATD integration in a particular domain
2	/domain/<domain_id>/ ipsdevices/atdintegration	PUT	Update ATD integration in a particular domain
3	sensor/<sensor_id>/ atdintegration	GET	Retrieves ATD integration in a particular Sensor
4	sensor/<sensor_id>/ atdintegration	PUT	Update ATD integration in a particular Sensor

Sensor Configuration Export Import Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/sensor/<sensor_id>/ exportconfiguration	PUT	Export the Sensor's configuration to an XML file
2	/sensor/<sensor_id>/ importconfiguration	PUT	Imports the Sensor configuration from the XML file and pushes to the Sensor

Denial Of Services Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/sensor/<sensor_id>/ dosprofilesonmanager	GET	Retrieves the DoS Profiles on Manager for the Sensor
2	/sensor/<sensor_id>/ dosprofilelearningmode	PUT	Updates the DoS Learning mode on the Sensor
3	/sensor/<sensor_id>/ dospacketforwarding	GET	Retrieves the Dos Packet forwarding details
4	/sensor/<sensor_id>/ uploaddosprofile	PUT	Uploads the profile to the Manager
5	/sensor/<sensor_id>/ restoredosprofile	PUT	Downloads the profile to the Sensor
6	/sensor/<sensor_id>/ deletedosprofile	DELETE	Deletes the profile from the Manager
7	/sensor/<sensor_id>/ exportdosprofile	PUT	Exports the profile to machine

Domain Name Exceptions Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/ domainnameexceptions	GET	Retrieves the domain name exceptions from the Manager
2	/ domainnameexceptions/ import	POST	Imports the domain name exceptions to the Manager
3	/ domainnameexceptions/ export	GET	Exports the domain name exceptions from the Manager
4	/ domainnameexceptions	PUT	Updates a domain name exception's comment
5	/ domainnameexceptions	DELETE	Deletes some domain name exceptions
6	/ domainnameexceptions/ all	DELETE	Deletes all domain name exceptions
7	/ domainnameexceptions	POST	Adds a domain name to the callback detector allow list
8	/ domainnameexceptions	PUT	Updates the details of the domain name exception

EPO Integration Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/ epointegration	GET	Retrieves the ePO integration configuration for domain
2	/domain/<domain_id>/ epointegration	PUT	Updates the ePO integration configuration for domain

Packet Capture Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/sensor/<sensor_id>/ packetcapture	GET	Retrieves the packet capture settings
2	/sensor/<sensor_id>/ packetcapture	PUT	Updates the packet capture settings

S.No	Request URI	Actions Allowed	Actions Performed
3	/sensor/<sensor_id>/packetcapturestate	PUT	Updates the packet capturing status
4	/sensor/<sensor_id>/packetcaptureruletemplate	GET	Retrieves the list/a particular rule template
5	/sensor/<sensor_id>/packetcaptureruletemplate	POST	Adds a packet capture rule template
6	/sensor/<sensor_id>/packetcapturepcapfiles	GET	Retrieves the list of PCAP files captured
7	/sensor/<sensor_id>/packetcapturepcapfile/export	PUT	Exports the PCAP file
8	/sensor/<sensor_id>/packetcapturepcapfile	DELETE	Deletes the PCAP file
9	/domain/<domain_id>/packetcaptureruletemplate	GET	Retrieves the list/a particular rule template
10	/domain/<domain_id>/packetcaptureruletemplate	POST	Adds a packet capture rule template
11	/domain/<domain_id>/packetcaptureruletemplate/<name>	PUT	Updates a packet capture rule template
12	/domain/<domain_id>/packetcaptureruletemplate/<name>	DELETE	Deletes a packet capture rule template

Policy Group Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/policygroup	GET	Retrieves all policy group
2	/domain/<domain_id>/policygroup/	POST	Creates policy group
3	/domain/<domain_id>/policygroup/<policygroup_id>	GET	Retrieves policy group
4	/domain/<domain_id>/policygroup/<policygroup_id>	PUT	Updates policy group
5	/domain/<domain_id>/policygroup/<policygroup_id>	DELETE	Deletes policy group

Policy Assignments Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/policyassignments/interface	GET	Retrieves all assigned policy for interface
2	/domain/<domain_id>/policyassignments/interface/<vids_id>	GET	Retrieves all assigned policy for particular interface
3	/domain/<domain_id>/policyassignments/device	GET	Retrieves all assigned policy for device
4	/domain/<domain_id>/policyassignments/device/<device_id>	GET	Retrieves all assigned policy for particular device
5	/domain/<domain_id>/policyassignments/interface/<vids_id>	PUT	Updates policies for the interface
6	/domain/<domain_id>/policyassignments/device/<device_id>	PUT	Updates policies for the device

Ignore Rules/NTBA Ignore Rules

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domainId>/attackfilter82?context=<context>	GET	Retrieves all the ignore rules created in a domain
2	/domain/<domainId>/attackfilter82/<ruleId>?context=<context>	GET	Retrieves the details of ignore rule with the given rule ID
3	/domain/<domainId>/attackfilter82?context=<context>	POST	Creates a new ignore rule
4	/domain/<domainId>/attackfilter82/<ruleId>?context=<context>	PUT	Updates an ignore rule
5	/domain/<domainId>/attackfilter82/<ruleId>?context=<context>	DELETE	Deletes an ignore rule

Inspection Options Policy Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	protectionoptionspolicy	GET	Retrieves all inspection options policy
2	protectionoptionspolicy / <policy_id>	GET	Retrieves details of inspection options
3	protectionoptionspolicy	POST	Creates inspection options policy
4	protectionoptionspolicy/ <policy_id>	PUT	Updates inspection options policy
5	protectionoptionspolicy / <policy_id>	DELETE	Deletes inspection options policy

DXL Integration Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/ dxlintegration	GET	Retrieves the DXL integration configuration for the domain
2	/domain/<domain_id>/ dxlintegration	PUT	Updates the DXL integration configuration for the domain
3	/sensor/<sensor_id>/ dxlintegration	GET	Retrieves the DXL integration configuration at the Sensor
4	/sensor/<sensor_id>/ dxlintegration	PUT	Updates the DXL integration configuration at the Sensor

Threat Explorer Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/ threatexplorer/alerts/ TopN/<count>/direction/ <direction>/duration/ <duration>? includeChildDomain= <includeChildDomain>&&action= <action>&&value=<value>	GET	Retrieves the Threat explorer data

S.No	Request URI	Actions Allowed	Actions Performed
2	/domain/<domain_id> /threatexplorer/alerts/TopN/ <count>/direction/ <direction>/ duration/<duration>/attacks? includeChildDomain=<include ChildDomain> &&action=<action>&&value=<value>	GET	Retrieves the List of top attacks
3	/domain/<domain_id>/ threatexplorer/alerts/TopN/ <count>/direction/ <direction>/ duration/<duration>/ attackers? includeChildDomain=<includeChildDomain> &&action=<action>&&value=<value>	GET	Retrieves the List of top attackers
4	/domain/<domain_id>/ threatexplorer/alerts/TopN/ <count>/direction/ <direction>/ duration/<duration>/targets? includeChildDomain=<includeChildDomain> &&action=<action>&&value=<value>	GET	Retrieves the List of top targets
5	/domain/<domain_id>/ threatexplorer/alerts/TopN/ <count>/direction/ <direction>/ duration/<duration>/ attack_applications? includeChildDomain=<includeChildDomain> &&action=<action>&&value=<value>	GET	Retrieves the List of top attack applications
6	/domain/<domain_id>/ threatexplorer/alerts/TopN/ <count>/direction/ <direction>/ duration/<duration>/ malware? includeChildDomain=<includeChildDomain> &&action=<action>&&value=<value>	GET	Retrieves the List of top malwares
7	/domain/<domain_id>/ threatexplorer/alerts/TopN/ <count>/direction/ <direction>/ duration/<duration>/ executables? includeChildDomain=<includeChildDomain> &&action=<action>&&value=<value>	GET	Retrieves the List of top executables

Network Forensics

S.No	Request URI	Actions Allowed	Actions Performed
1	/networkforensics/<ipaddress>?startime=<start_time>&&duration=<duration>&&ntba=<ntb a _id>	GET	Retrieves the host summary for given IP address. URL Parameter 1: **ipaddress** Query Parameter1: **starttime=** Date in the format yyyy-MMM-dd HH:mm Query Parameter 2: **duration** = • NEXT_60_SECONDS • NEXT_5_MINUTES • NEXT_60_MINUTES • NEXT_30_MINUTES Query Parameter 3: **ntba id**
2	/networkforensics/<ipaddress>/suspiciousflows ?startime=<start_time>&&duration=<duration>&&ntba=<ntba_id>	GET	Retrieves the top suspicious flows for the given IP address. URL Parameter 1: **ipaddress** Query Parameter1: **starttime=** Date in the format yyyy-MMM-dd HH:mm Query Parameter 2: **duration** = • NEXT_60_SECONDS • NEXT_5_MINUTES • NEXT_60_MINUTES • NEXT_30_MINUTES Query Parameter 3: **ntba id**

Gateway Anti-Malware Engine Update Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/gamupdatesettings	GET	Retrieves the Gateway Anti-Malware engine updating configuration for the domain
2	/domain/<domain_id>/gamupdatesettings	PUT	Update the Gateway Anti-Malware engine updating configuration for the domain
3	/sensor/<sensor_id>/gamupdatesettings	GET	Retrieves the Gateway Anti-Malware engine updating configuration at the Sensor

S.No	Request URI	Actions Allowed	Actions Performed
4	/sensor/<sensor_id>/ gamupdatesettings	PUT	Update the Gateway Anti-Malware engine updating configuration at the Sensor

Users

S.No	Request URI	Actions Allowed	Actions Performed
1	/user/{userId}	GET	Retrieves the details of a user with the given user id
2	/user	POST	Creates a new user
3	/user/{userId}	DELETE	Deletes an existing user with the given user id
4	/user/{userId}	PUT	Updates the details of user with the given user id

Alert Pruning

S.No	Request URI	Actions Allowed	Actions Performed
1	/Maintenance/prunealerts	PUT	Configures the alert pruning settings

Custom Role

S.No	Request URI	Actions Allowed	Actions Performed
1	/role	GET	Retrieves the details of all the roles
2	/role	POST	Creates a new custom role
3	/role/{roleName}	DELETE	Deletes a custom role with the given name

Direct Syslog Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/directsyslog	`GET`	Retrieves the direct syslog configuration for the domain
2	/domain/<domain_id>/directsyslog	`PUT`	Updates the direct syslog configuration for the domain
3	/sensor/<sensor_id>/directsyslog	`GET`	Retrieves the direct syslog configuration at the Sensor
4	/sensor/<sensor_id>/directsyslog	`PUT`	Updates the direct syslog configuration at the Sensor
5	/domain/<domain_id>/directsyslog/testconnection	`PUT`	Tests the connection for direct syslog configuration for the domain
6	/sensor/<sensor_id>/directsyslog/testconnection	`PUT`	Tests the connection for direct syslog configuration at the Sensor

Radius Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domain_id>/remoteaccess/radius	`GET`	Retrieves the radius configuration for the domain
2	/domain/<domain_id>/remoteaccess/radius	`PUT`	Updates the radius configuration for the domain

Advanced Device Configuration Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domainId>/advanceddeviceconfiguration	`GET`	Get the advanced device configuration at domain level
2	/domain/<domainId>/advanceddeviceconfiguration	`PUT`	Update the advanced device configuration at domain level
3	/sensor/<sensorId>/advanceddeviceconfiguration	`GET`	Get the advanced device configuration at Sensor level
4	/sensor/<sensorId>/advanceddeviceconfiguration	`PUT`	Update the advanced device configuration at Sensor level

Attack Log Resource

Priority	Request URI	Actions Allowed	Actions Performed
1	/alerts? domainId=<domain_id>&includeChildDomain=<true/ false>&alertstate=<state>&timeperiod=<timeperiod> &startime=<start_time>&endtime=<endBtime> &search=<search_string> &page=<page>&filter=<filterBvalue>	GET	Gets the alerts based on the given filter criteria in the URL parameter.
2	/alerts? alertstate=<state> &timeperiod==<timeperiod> &startime==<start_time> &endtime=<end_time>&search=<search_strng> &filter=<filter_value>	DELTE	Deletes the all alerts which fulfil the given filter criteria in the URL parameter.
3	/alerts? alertstate=<state> &timeperiod==<timeperiod> &startime==<start_time>&endtime=<end_time> &search=<search_strng>&fromalert=<alert_uuid> &page=<page>&filter=<filter_value>	UPDATE	This method is used to update alert state to Acknowledged/ Unacknowledged all alerts which fulfil the given filter criteria in the URL parameter
4	/alerts/<alert_uuid>? sensorId=<sensor_id>&manager=<manager_name>	GET	This method is used to get alert
5	/alerts/<alert_uuid>? sensorId=<sensor_id>&manager=<manager_name>	PUT	This method is used to update alert state to Acknowledge/ Unacknowledged and to update assign to.
6	/alerts/<alert_uuid>? sensorId=<sensor_id>&manager=<manager_name>	DELETE	Delete the single alert.
7	/alerts/<alert_id>/ triggeredpkt? sensorId=<sensor_id>	GET	Retrieves the packet logs associated with an alert component in a ZIP file.

Traffic Statistics

S.No	Request URI	Actions Allowed	Actions Performed
1	/sensor/{sensorId}/port/ {portId}/trafficstats/trafficrxtx	GET	Get traffic received/ send statistics for a given Sensor on a given port
2	/sensor/{sensorId}/ trafficstats/flows	GET	Get the flows statistics for a given Sensor

S.No	Request URI	Actions Allowed	Actions Performed
3	/sensor/{sensorId}/port/{portId}/trafficstats/droppedpackets	GET	Get he dropped packets statistics for a given Sensor on a given port
4	/sensor/{sensorId}/trafficstats/malwarestatsgroupbyengine	GET	Get the advance malware engine statistics for a given Sensor grouped by engine type
5	/sensor/{sensorId}/trafficstats/malwarestatsgroupbyfile	GET	Get the advance malware engine statistics for a given Sensor grouped by file type
6	/sensor/{sensorId}/trafficstats/advcallbackdetectionstats	GET	Get the advance callback detection statistics for a given Sensor
7	/sensor/{sensorId}/trafficstats/sensorsslstats	GET	Gets the sensor SSL statistics
8	/sensor/{sensorId}/trafficstats/outboundsslstats	GET	Gets the outbound SSL statistics
9	/sensor/{sensorId}/trafficstats/sslinternalwebcertmatches	GET	Gets the details of the inter web certificates matched
10	/sensor/{sensorId}/trafficstats/resetsslcounters	GET	Resets the SSL counters

CLI Auditing Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domainId>/cliauditing	GET	Get the CLI auditing configuration at the domain level.
2	/domain/<domainId>/cliauditing	PUT	Update the CLI auditing configuration at the domain level.
3	/sensor/<sensorId>/cliauditing	GET	Get the CLI auditing configuration at the Sensor level.
4	/sensor/<sensorId>/cliauditing	PUT	Update the CLI auditing configuration at the Sensor level.

Diagnostics Trace Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/sensor/<sensor_id>/ diagnosticstrace	GET	Get the diagnostic trace files
2	/sensor/<sensor_id>/ diagnosticstrace/upload	PUT	Upload the diagnostic trace file.
3	/sensor/<sensor_id>/ diagnosticstrace/upload	GET	Get the upload status.
4	/sensor/<sensor_id>/ diagnosticstrace /export	PUT	Export the diagnostic trace file
5	/sensor/<sensor_id>/ diagnosticstrace	DELETE	Deletes the diagnostic trace file

Health Check Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/healthcheck	GET	Get the health check
2	/healthcheck	PUT	Run the health check

McAfee Cloud Integration Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/mcafeecloudintegration	GET	Get the McAfee cloud integration settings
2	/mcafeecloudintegration	PUT	Update the McAfee cloud integration settings.
3	/mcafeecloudintegration/ testconnection	PUT	Test the connection for McAfee cloud integration settings
4	/mcafeecloudintegration/ statistics	GET	Get the statistics
5	/mcafeecloudintegration/ resetstatistics	PUT	Reset the statistics

Performance Monitoring Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domainId>/ performancemonitoring	`GET`	Get the Performance Monitoring settings at the domain level
2	/domain/<domainId>/ performancemonitoring	`PUT`	Update the Performance Monitoring settings at the domain level
3	/sensor/<sensorId>/ performancemonitoring	`GET`	Get the Performance Monitoring settings at the Sensor level
4	/sensor/<sensorId>/ performancemonitoring	`PUT`	Update the Performance Monitoring settings at the Sensor level

Attack Set Profile

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domainId>/ attacksetprofile/getallrules	`GET`	Get list of all the attack set profile details at domain level.
2	/domain/<domainId>/ attacksetprofile/ rulesetdetails/<policyId>	`GET`	Get the rule set of given policy at domain level.
3	/domain/<domainId>/ attacksetprofile/createruleset	`POST`	Creates a new attack set at domain level.
4	/domain/<domainId>/ attacksetprofile/ updateruleset/<policyId>	`PUT`	Updates particular attack set at domain level.
5	/domain/<domainId>/ attacksetprofile/deleteruleset/ <policyId>	`DELETE`	Deletes particular attack set at domain level.

Proxy Server

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domainId>/ proxyserver	`GET`	Get the proxy server configuration at domain level

S.No	Request URI	Actions Allowed	Actions Performed
2	/domain/<domainId>/ proxyserver	PUT	Update the proxy server configuration at domain level
3	/device/<device_id>/ proxyserver	GET	Get the proxy server configuration at device level
4	/device/<device_id>/ proxyserver	PUT	Update the proxy server configuration at device level
5	/domain/proxyserver	GET	Get the proxy server configuration at the Manager level
6	/domain/proxyserver	PUT	Update the proxy server configuration at the Manager level

Cloud Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/cloud/getclusterid	POST	Get the cluster ID based on name
2	/cloud/getcontrollerid	POST	Get the controller ID based on name
3	/cloud/checkprobestatus/ <ip_address>	GET	Get the probe status
4	/cloud/<domain_id>/ connector	GET	Get all the controllers in domain
5	/cloud/<domain_id>/ connector	POST	Create the controller in domain
6	/cloud/connector/<id>	GET	Get the controller details
7	/cloud/connector/<id>/ testcontrollerconnection	GET	Test the connection to controller
8	/cloud/connector/<id>/ testcloudconnection	GET	Test the controller cloud connection
9	/cloud/connector/<id>	PUT	Update the controller details
10	/cloud/connector/<id>	DELETE	Delete the controller
11	/cloud/connector/<id>/ upgrade	PUT	Upgrade the controller software
12	/cloud/<domain_id>/cluster	GET	Get all the clusters in the domain

S.No	Request URI	Actions Allowed	Actions Performed
13	/cloud/<domain_id>/cluster	POST	Create the cluster in the domain
14	/cloud/cluster/<id>	GET	Get the cluster details
15	/cloud/cluster/<id>	PUT	Update the cluster details
16	/cloud/cluster/<id>	DELETE	Delete the cluster
17	/cloud/cluster/<id>/vmgroups	GET	Get the protected VM groups in the cluster
18	/cloud/cluster/<id>/vmgroup	POST	Create the protected VM group in the cluster
19	/cloud/cluster/<id>/getvmgroup	PUT	Get the protected VM group
20	/cloud/cluster/<id>/vmgroup	PUT	Update the protected VM group
21	/cloud/cluster/<id>/vmgroup	Delete	Delete the protected VM group
22	/cloud/cluster/<id>/downloadagent	GET	Download the virtual probe agent associated with the cluster
23	/cloud/cluster/<id>/upgradeagents	PUT	Upgrade the agents associated with the cluster
24	/cloud/cluster/<id>/getProtectedVMHosts	GET	Get the list of protected VM hosts
25	/cloud/cluster/downloadprobeagent	GET	Download probe agent for cluster

Quarantine Zone Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domainId>/quarantineZone/<quarantineZoneID>	GET	Get quarantine zone at given domain.
2	/domain/<domainId>/quarantineZone	GET	Get all quarantine zones visible at given domain.
3	/domain/<domainId>/quarantineZone/<quarantineZoneID>	PUT	Update quarantine zone.

S.No	Request URI	Actions Allowed	Actions Performed
4	/domain/<domainId>/ quarantineZone	`POST`	Add quarantine zone at given domain.
5	/domain/<domainId>/ quarantineZone	`DELETE`	Delete quarantine zone.

GTI and Telemetry Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/gticonfiguration/private	`GET`	Get the GTI private cloud configuration
2	/gticonfiguration/private	`PUT`	Update the GTI private cloud details
3	/gticonfiguration/private/ importcert	`PUT`	Import GTI private cloud certificate
4	/gticonfiguration/private/ {ip_address}/testconnection	`GET`	Get the IP status from GTI private cloud
5	/gticonfiguration	`GET`	Get telemetry configuration
6	/gticonfiguration	`PUT`	Update telemetry configuration

License Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	/license/vmips	`GET`	Get VMIPS licenses present on the Manager
2	/license/proxy	`GET`	Get proxy licenses present on the Manager
3	/license/capacity	`GET`	Get capacity licenses present on the Manager
4	/license	`PUT`	Import licenses to Manager
5	/license/assignlicense	`PUT`	Assign a license to the given device
6	/license/ unassignlicense	`PUT`	Unassign a license
7	/license/delete/<licensetype>	`DELETE`	Delete multiple licenses

S.No	Request URI	Actions Allowed	Actions Performed
8	/license/ getSensorsforassociation	GET	Get Sensors list for association with the given license

IPS Inspection Allowlist Resource

S.No	Request URI	Actions Allowed	Actions Performed
1	domainnameexceptions/ ipsinspectionallowlist	GET	Gets the IPS inspection allow list from the Manager
2	domainnameexceptions/ ipsinspectionallowlist/ IPSDNEDetail	GET	Gets the details of a domain name from the IPS inspection allow list
3	domainnameexceptions/ ipsinspectionallowlist	POST	Adds the domain name to the IPS inspection allow list
4	domainnameexceptions/ ipsinspectionallowlist/import	POST	Imports the domain name exceptions to the Manager
5	domainnameexceptions/ ipsinspectionallowlist/export	GET	Exports the domain name exceptions to the Manager
6	domainnameexceptions/ ipsinspectionallowlist	PUT	Updates the details of the domain name exception
7	domainnameexceptions/ ipsinspectionallowlist	DELETE	Deletes some domain names from the IPS inspection allow list
8	domainnameexceptions/ ipsinspectionallowlist/all	DELETE	Deletes all the domain names from the IPS inspection allow list
9	domainnameexceptions/ ipsinspectionallowlist/ bulkUpdate	PUT	Updates the status of some domain name exceptions from the IPS Inspection allow list

SSL Exception Rules

S.No	Request URI	Actions Allowed	Actions Performed
1	/domain/<domainId>/ outboundsslexceptions	GET	Gets all the Outbound Exception rules

S.No	Request URI	Actions Allowed	Actions Performed
2	/domain/<domainId>/outboundsslexceptions/<ruleId>	`GET`	Gets a single Outbound Exception rule
3	/domain/<domainId>/outboundsslexceptions	`POST`	Creates an Outbound Exception rule
4	/domain/<domainId>/outboundsslexceptions/<ruleId>	`PUT`	Updates an Outbound Exception rule
5	/domain/<domainId>/outboundsslexceptions/<ruleId>	`DELETE`	Deletes an Outbound Exception rule

Error Information

All APIs return web error Information in case of failure. The SDK API error code and message will be returned as part of payload of web error.

SDK API Error Details	Description	Data Type
errorId	Error code	Number
errorMessage	Error message	String

Login

This URL allows a third party application to log in to NSM API framework.

Resource URL

GET /session

Request Parameters

NSM REST SDK user needs to authenticate with the Manager by calling the 'Session' resource URL first. The 'Session' resource takes the user name and password in a base64 encoded string through the custom header, NSM-SDK-API.

Field Name	Description	Data Type	Mandatory
`userName`	Login user name. Minimum of 8 characters'	String	Yes
`password`	Login user password	String	Yes

Response Parameters

On successful authentication, the 'Session' resource URL returns the user id and session in the response body.

Every other resource URLs in the SDK is required to pass credentials for validation and authorization in the custom header **NSM-SDK-API**. The credentials are user id and session id return from the 'Session' resource URL. They are also passed in base64 encoded format.

Field Name	Description	Data Type
`session`	Logged in session id	String
`userId`	Logged in user id	Number

Note: The default SDK API session inactivity timeout is 24 hours

Example

Request

`GET` https://%3CNSM_IP%3E/sdkapi/session

Response

```
{ "session": "4B63900C0C913E8944EAC68CABF12ACF", "userId": "1" }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error code	SDK API errorId	errorMessage
1	401		Invalid credentials
2	415		Invalid accept header
3	415		Invalid content type header

Logout

This URL allows logging out from the Manager. It generates either a response or a error message.

Resource URL

DELETE /session

Request Parameters

None

Response Parameters

The return value is 1 if logout is successful, otherwise an error message is returned

Field Name	Description	Data Type
`return`	Return value	Number

Example

Request

`DELETE` https://%3CNSM_IP%3E/sdkapi/session

Response

```
{ "return": 1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error code	SDK API errorId	errorMessage
1	400	4501	Unable to get the Manager details

Get Manager Availability Information

This URL provides Manager availability information to the user with basic details like MDR configuration.

Resource URL

GET /heartbeat

Request Parameters

None

Response Parameters

Field Name	Description	Data Type
`mdrAdministrativeStatus`	MDR administrative status	String
`lastUpdatedTime`	Last updated timestamp	String
`mdrPeerIpAddress`	MDR peer IP address	String
`mdrOperationalStatus`	MDR operational status	String
`downTimeForSwitchOver`	Down time switch over	String

Example

Request

`GET` https://%3CNSM_IP%3E/sdkapi/heartbeat

Response

```
{ "mdrAdministrativeStatus": "Primary", "mdrOperationalStatus": "Active", "mdrPeerIpAddress": "172.16.232.97",
"downTimeForSwitchOver": "5 minutes", "lastUpdatedTime": "2013-06-13 11:11:59" }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error code	SDK API errorId	errorMessage
1	400	4501	Unable to get the Manager details

Create a new Domain

This URL creates a new domain.

Resource URL

POST /domain

Request Parameters

Payload Parameters:

Field Name	Description	Data Type
`SubscriberDescriptor`	Object that contains the details of the field to be sent	Object

Details of fields in SubscriberDescriptor:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain Id	Number	No
`parentDomainId`	Parent domain Id	Number	No
`domainName`	Domain name	String	Yes
`contactPerson`	Contact person	String	Yes
`emailAddress`	Email address	String	Yes
`Title`	Title	String	No
`contactPhoneNumber`	Contact phone number	String	No
`companyPhoneNumber`	Company phone number	String	No
`Organization`	Organization	String	No
`Address`	Address	Object	No
`City`	City	String	No
`State`	State	String	No
`Country`	Country	String	No
`allowChildAdminDomain`	Allow child admin domain	Boolean	No
`allowDevices`	Allow devices	Boolean	No
`defaultIPSPolicy`	Default IPS policy	String	Yes
`defaultReconPolicy`	Default recon policy	String	Yes

Details of fields in Address:

Field Name	Description	Data Type
`address1`	Address1	String
`address2`	Address2	String

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique ID of the created domain	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/domain

Payload

```
{ "parentDomainId": 0, "domainName": "Test Child Domain 1", "contactPerson": "McAfee", "emailAddress":
"b@mcafee.com", "title": "Intel", "contactPhoneNumber": "9999999999", "companyPhoneNumber": "080-12345678",
"organization": "McAfee", "address": { "address1": "Bangalore", "address2": "India" }, "city": "Bangalore",
"state": "Karnataka", "country": "India", "allowChildAdminDomain": true, "allowDevices": true,
"defaultIPSPolicy": "Default Inline IPS", "defaultReconPolicy": "Default Reconnaissance Policy" }
```

Response

```
{ "createdResourceId": 101 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4415	Invalid parent domain id
2	400	4418	No child domain can be added to domain
3	400	4401	Domain name is required
4	400	4402	Domain name exceeding maximum size(55)
5	400	4416	Duplicate admin domain name detected
6	400	4403	Invalid domain name
7	400	4422	IPS policy is required
8	400	4417	Invalid IPS policy
9	400	4423	Recon policy is required
10	400	1112	Invalid recon policy
11	400	4402	Company name exceeding maximum size(55)
12	400	4409	Invalid company name

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
13	400	4402	Address1 exceeding maximum size(55)
14	400	4402	Address2 exceeding maximum size(55)
15	400	4402	Company phone number exceeding maximum size(20)
16	400	4404	Invalid company phone number
17	400	4405	Contact person required
18	400	4402	Contact person exceeding maximum size(55)
19	400	4406	Invalid contact person
20	400	4407	Email address required
21	400	4408	Invalid email address
22	400	4402	Country name exceeding maximum size(30)
23	400	4410	Invalid country
24	400	4402	Contact phone number exceeding maximum size(20)
25	400	4411	Invalid contact phone number
26	400	4402	State name exceeding maximum size(20)
27	400	4412	Invalid state
28	400	4402	Title exceeding maximum size(55)
28	400	4413	Invalid title
29	400	4402	City exceeding maximum size(55)
30	400	4414	Invalid city

Update a Domain

This URL updates a domain.

Resource URL

PUT /domain/<domain_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domainId	Domain Id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type
SubscriberDescriptor	Object that contains the details of the field to be sent	Object

Details of fields in SubscriberDescriptor:

Field Name	Description	Data Type	Mandatory
domainId	Domain Id	Number	No
parentDomainId	Parent domain Id	Number	No
domainName	Domain name	String	Yes
contactPerson	Contact person	String	Yes
emailAddress	Email address	String	Yes
Title	Title	String	No
contactPhoneNumber	Contact phone number	String	No
companyPhoneNumber	Company phone number	String	No
Organization	Organization	String	No
Address	Address	Object	No
City	City	String	No
State	State	String	No
Country	Country	String	No
allowChildAdminDomain	Allow child admin domain	Boolean	No
allowDevices	Allow devices	Boolean	No
defaultIPSPolicy	Default IPS policy	String	Yes
defaultReconPolicy	Default recon policy	String	Yes

Details of fields in Address:

Field Name	Description	Data Type
address1	Address1	String

Field Name	Description	Data Type
address2	Address2	String

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/domain/101

Payload

```
{ "parentDomainId": 0, "domainName": "Test Child Domain 2", "contactPerson": "McAfee", "emailAddress":
"b@mcafee.com", "title": "Intel", "contactPhoneNumber": "9999999999", "companyPhoneNumber": "080-12345678",
"organization": "McAfee", "address": { "address1": "Bangalore", "address2": "India" }, "city": "Bangalore",
"state": "Karnataka", "country": "India", "allowChildAdminDomain": true, "allowDevices": true,
"defaultIPSPolicy": "Default Inline IPS", "defaultReconPolicy": "Default Reconnaissance Policy" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4415	Invalid parent domain id
2	400	4418	No child domain can be added to domain
3	400	4401	Domain name is required
4	400	4402	Domain name exceeding maximum size(55)
5	400	4416	Duplicate admin domain name detected
6	400	4403	Invalid domain name
7	400	4422	IPS policy is required
8	400	4417	Invalid IPS Policy
9	400	4423	Recon policy is required
10	400	1112	Invalid recon policy
11	400	4402	Company name exceeding maximum size(55)
12	400	4409	Invalid company name

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
13	400	4402	Address1 exceeding maximum size(55)
14	400	4402	Address2 exceeding maximum size(55)
15	400	4402	Company phone number exceeding maximum size(20)
16	400	4404	Invalid company phone number
17	400	4405	Contact person required
18	400	4402	Contact person exceeding maximum size(55)
19	400	4406	Invalid contact person
20	400	4407	Email address required
21	400	4408	Invalid email address
22	400	4402	Country name exceeding maximum size(30)
23	400	4410	Invalid country
24	400	4402	Contact phone number exceeding maximum size(20)
25	400	4411	Invalid contact phone number
26	400	4402	State name exceeding maximum size(20)
27	400	4412	Invalid state
28	400	4402	Title exceeding maximum size(55)
28	400	4413	Invalid title
29	400	4402	City exceeding maximum size(55)
30	400	4414	Invalid city
31	400	4419	Parent domain id cannot be changed
32	400	4420	Allow child admin domain field cannot be changed
33	400	4421	Allow devices field cannot be changed
34	404	1105	Invalid domain

Get a Domain

This URL gets the specified domain.

Resource URL

GET /domain/<domain_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain Id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`SubscriberDescriptor`	Object that contains the details of the fields	Object

Details of fields in SubscriberDescriptor:

Field Name	Description	Data Type
`domainId`	Domain Id	Number
`parentDomainId`	Parent domain Id	Number
`domainName`	Domain name	String
`contactPerson`	Contact person	String
`emailAddress`	Email address	String
`Title`	Title	String
`contactPhoneNumber`	Contact phone number	String
`companyPhoneNumber`	Company phone number	String
`Organization`	Organization	String
`Address`	Address	Object
`City`	City	String
`State`	State	String
`Country`	Country	String
`allowChildAdminDomain`	Allow child admin domain	Boolean
`allowDevices`	Allow devices	Boolean

Field Name	Description	Data Type
`defaultIPSPolicy`	Default IPS policy	String
`defaultReconPolicy`	Default recon policy	String

Details of fields in Address:

Field Name	Description	Data Type
`address1`	Address1	String
`address2`	Address2	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/domain/101

Response

```
{ "parentDomainId": 0, "domainName": "Test Child Domain 2", "contactPerson": "McAfee", "emailAddress":
"b@mcafee.com", "title": "Intel", "contactPhoneNumber": "9999999999", "companyPhoneNumber": "080-12345678",
"organization": "McAfee", "address": { "address1": "Bangalore", "address2": "India" }, "city": "Bangalore",
"state": "Karnataka", "country": "India", "allowChildAdminDomain": true, "allowDevices": true,
"defaultIPSPolicy": "Default Inline IPS", "defaultReconPolicy": "Default Reconnaissance Policy" }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Delete a Domain

This URL deletes a domain.

Resource URL

DELETE /domain/<domain_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain Id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

DELETE https://%3CNSM_IP%3E/sdkapi/domain/105

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Get Default Recon Policies

This URL gets default recon policies at domain level.

Resource URL

GET /domain/<domain_id>/defaultreconpolicies

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain Id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
ReconPolicyDescList	Array of object that contains the details of the fields	Array

Details of Object in ReconPolicyDesc:

Field Name	Description	Data Type
policyName	Policy name	String
policyId	Policy Id	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/domain/101/defaultreconpolicies

Response

```
{ " reconPolicyList ": [ { "policyName": " Default Reconnaissance Policy ", "policyId": "0" }, { "policyName": "
NSAT 7.1 Reconnaissance Policy ", "policyId": "301" } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Get All Admin Domains

This URL gets details of all admin domains in the Manager starting from root AD and all child ADs including hierarchy information.

Resource URL

GET /domain

Request Parameters

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`DomainDescriptor`	Domain details	Object

Details of DomainDescriptor:

Field Name	Description	Data Type
`id`	Domain Id	Number
`name`	Domain name	String
`childdomains`	List of domain descriptor object	Array

Example

Request

`GET` https://%3Cnsm_ip%3E/sdkapi/domain

Response

```
{ "DomainDescriptor": { "childdomains": [ { "childdomains": null, "id": 102, "name": "Test Child Domain 2" },
{ "childdomains": [ { "childdomains": [ { "childdomains": null, "id": 104, "name": "Test Child Domain
1.1.1" } ], "id": 103, "name": "Test Child Domain 1.1" } ], "id": 101, "name": "Test Child Domain 1" } ], "id":
0, "name": "My Company" } }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error code	SDK API errorId	errorMessage
1	400	4501	Unable to get the Manager details

Get All Child Domains in a Admin Domain

This API gets details of all child admin domains in the Manager including hierarchy information in the specified domain.

Resource URL

GET /domain/<domain_id>

Request Parameters

Field Name	Description	Data Type
`domain_id`	Domain ID	Number

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`DomainDescriptor`	Domain details	Object

Details of DomainDescriptor:

Field Name	Description	Data Type
`id`	Domain Id	Number
`name`	Domain name	String
`childdomains`	List of domain descriptor object	Array

Example

Request

`GET` https://%3CNSM_IP%3E/sdkapi/domain/101

Response

```
{ "DomainDescriptor": { "id": 101, "name": "Test Child Domain 1", "childdomains": [ { "id": 103, "name": "Test
Child Domain 1.1", "childdomains": [ { "id": 104, "name": "Test Child Domain 1.1.1", "childdomains":
null } ] } ] } }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Get all Sensors in a Domain

This API gets the list of Sensors available in the specified domain. If the domain is not specified, details of all the Sensors in all ADs will be provided.

Resource URL

GET /sensors?domain=<domain_id>

Request Parameters

Field Name	Description	Data Type	Mandatory
Domain_id	Domain Id	Number	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
SensorDescriptor	Brief Sensor detail	Array

Details of object in SensorDescriptor:

Field Name	Description	Data Type
sensorId	Sensor primary key	Number
name	Name of the Sensor	String
model	Sensor model	String
Description	Sensor description	String
DomainId	Id of domain to which this Sensor belongs to	Number
isFailOver	Is the Sensor fail over	Boolean
isLoadBalancer	Is the Sensor load balancer	Boolean
SigsetVersion	Signature set version number applied to the Sensor	String
SoftwareVersion	Sensor software version	String
LastSignatureUpdateTs	Last configuration download timestamp	String
IPSPolicyID	IPS policy id applied to the Sensor	Number
ReconPolicyID	Recon policy id applied to the Sensor	Number
LastModTs	Last modified timestamp	String
sensorIPAddress	Sensor IP address	String

Field Name	Description	Data Type
`nsmVersion`	Manager version	String
`MemberSensors`	Member Sensors in case of fail over and load balancer	Array

Details of object in member Sensors:

Field Name	Description	Data Type
`sensorId`	Sensor primary key	Number
`name`	Name of the Sensor	String
`sensorIPAddress`	Sensor IP address	String
`SigsetVersion`	Signature set version number applied to the Sensor	String

Example

Request

`GET` https://%3CNSM_IP%3E/sdkapi/sensors

Response

```
{ "SensorDescriptor": [ { "DomainID": 0, "name": "M-1450", "model": "M-1450", "ReconPolicyID": 0, "IPSPolicyID":
19, "SigsetVersion": "7.5.14.25", "SoftwareVersion": "7.1.2.29", "LastSignatureUpdateTs": "2012-07-21 00:19:00",
"sensorId": 1001, "LastModTs": "2012-07-24 00:19:00", "Description": "MCAFEE-NETWORK-SECURITY-PLATFORM"
"sensorIPAddress": "172.16.232.56", "nsmVersion": "8.0.5.1.20" , "isFailOver": false }, { "DomainID": 101,
"name": "M-2950", "model": "M-2950", "ReconPolicyID": 0, "IPSPolicyID": 301, "SigsetVersion": "7.5.14.25",
"SoftwareVersion": "7.1.2.29", "LastSignatureUpdateTs": "2012-07-23 00:10:00", "sensorId": 1002, "LastModTs":
"2012-07-24 00:19:00", "Description": "MCAFEE-NETWORK-SECURITY-PLATFORM" "sensorIPAddress": "172.16.232.72",
"nsmVersion": "8.0.5.1.20" , "isFailOver": false }, { "sensorId": 1006, "name": "FO_3050", "model": "M-3050",
"Description": "MCAFEE-NETWORK-SECURITY-PLATFORM", "DomainID": 101, "isFailOver": true, "SigsetVersion":
"8.6.39.6", "SoftwareVersion": "8.1.3.16", "LastSignatureUpdateTs": "2014-09-05 20:43:54", "IPSPolicyID": 19,
"ReconPolicyID": 0, "sensorIPAddress": "10.213.174.50", "nsmVersion": "8.1.7.5.10", "MemberSensors":
[ { "sensorId": 1006, "name": "API_M3050_1", "sensorIPAddress": "10.213.174.50", "SigsetVersion": "8.6.39.6" },
{ "sensorId": 1007, "name": "API_M3050_2", "sensorIPAddress": "10.213.174.51", "SigsetVersion":
"8.6.39.6" } ] } ] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Get Sensor Details

This URL gets the details for the specified Sensor.

Resource URL

GET /sensor/<sensor_id>

Request Parameters

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`SensorInfo`	Sensor details	Object

The detail of the Sensor Info is given below

Field Name	Description	Data Type
`SensorDescriptor`	Sensor details	Object
`Interfaces`	Details of all Interfaces	Object
`Ports`	Details of all ports	Object

Details of SensorDescriptor:

Field Name	Description	Data Type
`sensorId`	Sensor primary key	Number
`name`	Name of the Sensor	String
`model`	Sensor model	String
`Description`	Sensor description	String
`DomainId`	Id of domain to which this Sensor belongs	Number
`isFailOver`	Whether the Sensor is a failover Sensor	Boolean
`isLoadBalancer`	Whether the Sensor is a load balancer Sensor	Boolean
`SigsetVersion`	Signature set version number applied to the Sensor	String
`DATVersion`	Botnet version present on Sensor	String
`SoftwareVersion`	Sensor software version	String
`LastSignatureUpdateTs`	Last configuration download timestamp	Number
`IPSPolicyID`	IPS policy id applied to the Sensor	Number
`ReconPolicyID`	Recon policy id applied to the Sensor	Number
`LastModTs`	Last modified timestamp	String
`sensorIPAddress`	Sensor 's IP address	String
`nsmVersion`	Manager version	String
`MemberSensors`	Member sensors in case of FO or LB	Array

Details of objects in MemberSensors:

Field Name	Description	Data Type
sensorId	Sensor primary key	Number
name	Name of the Sensor	String
sensorIPAddress	Sensor' s IP address	String
SigsetVersion	Signature set version number applied to the sensor	String
DATVersion	Botnet version present on sensor	String

Details of interfaces:

Field Name	Description	Data Type
InterfaceInfo	List of interfaces	Array

Details of object in InterfaceInfo:

Field Name	Description	Data Type
vidsId	Unique Id to identify interface/ subinterface	Number
name	Name of the interface	String
Description	Interface description	String
InterfaceType	Traffic type	Object
IPSPolicyId	IPS policy applied on interface	Number
DomainId	ID of the domain to which the interface is added	Number
SubInterfaces	Sub interface details	Object
LastModTs	Last modified timestamp	String

Details of InterfaceType:

Field Name	Description	Data Type
Dedicated	Default traffic type. No segmentation of traffic	Object
Vlan	Segment of interface into multiple networks by VLAN tags	Object
Cidr	Enables segment of interface into multiple networks by CIDR addressing	Object
BridgeVlan	Segment of interface into multiple networks by bridge VLAN tags	Object

Details of BridgeVlan:

Field Name	Description	Data Type
`bridgeVlanRangeList`	List of bridge VLAN range	Array

Details of CIDR:

Field Name	Description	Data Type
`CidrId`	List of CIDR IDs	Array

Details of Vlan:

Field Name	Description	Data Type
`id`	List of sub interfaces	Array

Details of object in SubInterfaceInfo:

Field Name	Description	Data Type
`name`	Name of the interface	String
`vidsId`	Unique Id to identify subinterface	Number
`InterfaceType`	Traffic type. VLAN or CIDR	String
`IPSPolicyId`	IPS policy applied on interface	Number
`LastModTs`	Last modified timestamp	String

Details of ports:

Field Name	Description	Data Type
`PortInfo`	Port information	Object

Details of PortInfo:

Field Name	Description	Data Type
`portId`	Unique Id to identify port	Number
`portSettings`	Describes port configurations	Object
`operatingMode`	Port operating mode	Object
`ResponseMode`	Port response mode	Object

Details of portSettings:

Field Name	Description	Data Type
`portName`	Name of the port	String

Field Name	Description	Data Type
`portType`	Describes port type	String
`configuration`	Port configuration (Speed and Duplex)	Object
`administrativeStatus`	Port administrative status. Can be "Enabled" or "Disabled"	String
`operationalStatus`	Port operational status. Can be "Up" or "Down"	String

Details of configuration:

Field Name	Description	Data Type
`Speed`	Port speed	String
`Duplex`	Full/Half duplex port	String

Details of operatingMode:

Field Name	Description	Data Type
`Mode`	Port mode	String
`peerPort`	Describes port peer	String
`connectedTo`	Peer port connected to, can be "Inside Network" / "Outside Network" / "n/a" (incase of span port)	String

Details of ResponseMode:

Field Name	Description	Data Type
`sendResponseFrom`	Send response from port	String

Example

Request

`GET` https://%3CNSM_IP%3E/sdkapi/sensor/1001

Response

```
{ "SensorInfo": { "SensorDescriptor": { "sensorId": 1001, "name": "NS7100", "model": "IPS-NS7100",
"Description": "MCAFEE-NETWORK-SECURITY-PLATFORM", "DomainID": 0, "isFailOver": false, "isLoadBalancer": false,
"SigsetVersion": "9.8.11.1", "DATVersion": "1854.0", "SoftwareVersion": "9.1.5.20", "LastSignatureUpdateTs":
"2017-12-11 23:03:41", "IPSPolicyID": 19, "ReconPolicyID": 0, "LastModTs": null, "sensorIPAddress": null,
"nsmVersion": null, "MemberSensors": [] }, "Interfaces": { "InterfaceInfo": [{ "vidsId": 119, "name": "G0/1-
G0/2", "Description": "", "Interfacetype": { "Dedicated": { }, "Vlan": null, "Cidr": null, "BridgeVlan": null },
"IPSPolicyId": 19, "DomainId": 0, "SubInterfaces": null, "LastModTs": "2017-12-08 09:43:57" }, { "vidsId": 189,
"name": "G3/1-G3/2", "Description": "", "Interfacetype": { "Dedicated": null, "Vlan": { "id": [] }, "Cidr":
null, "BridgeVlan": null }, "IPSPolicyId": 308, "DomainId": 101, "SubInterfaces": { "SubInterfaceInfo":
[{ "vidsId": 200, "name": "Sub-49", "Description": null, "Interfacetype": { "Dedicated": null, "Vlan": { "id":
["49"] }, "Cidr": null, "BridgeVlan": null }, "IPSPolicyId": 306, "DomainId": 101, "SubInterfaces": null,
"LastModTs": "2017-12-09 16:13:25" }] }, "LastModTs": "2017-12-09 03:43:18" }, { "vidsId": 118, "name": "G3/1-
G3/2", "Description": "Interface", "Interfacetype": { "Dedicated": null, "Vlan": { "id": [] }, "Cidr": null,
"BridgeVlan": null }, "IPSPolicyId": 308, "DomainId": 0, "SubInterfaces": { "SubInterfaceInfo": [{ "vidsId":
210, "name": "Sub-60", "Description": null, "Interfacetype": { "Dedicated": null, "Vlan": { "id": ["60"] },
"Cidr": null, "BridgeVlan": null }, "IPSPolicyId": 19, "DomainId": 0, "SubInterfaces": null, "LastModTs":
"2017-12-09 03:43:26" }, { "vidsId": 209, "name": "Sub-241", "Description": null, "Interfacetype":
{ "Dedicated": null, "Vlan": { "id": ["241"] }, "Cidr": null, "BridgeVlan": null }, "IPSPolicyId": 308,
"DomainId": 0, "SubInterfaces": null, "LastModTs": "2017-12-09 19:24:11" }] }, "LastModTs": "2017-12-11
19:19:13" }, { "vidsId": 117, "name": "G3/3-G3/4", "Description": "", "Interfacetype": { "Dedicated": { },
"Vlan": null, "Cidr": null, "BridgeVlan": null }, "IPSPolicyId": 19, "DomainId": 0, "SubInterfaces": null,
"LastModTs": "2017-12-08 09:43:57" }, { "vidsId": 116, "name": "G3/5-G3/6", "Description": "", "Interfacetype":
```

```
{ "Dedicated": { }, "Vlan": null, "Cidr": null, "BridgeVlan": null }, "IPSPolicyId": 19, "DomainId": 0,
"SubInterfaces": null, "LastModTs": "2017-12-08 09:43:57" }, { "vidsId": 115, "name": "G3/7-G3/8",
"Description": "", "Interfacetype": { "Dedicated": null, "Vlan": null, "Cidr": null, "BridgeVlan":
{ "bridgeVlanRangeList": ["4094-4095", "5-6", "3-4", "1-2"] } }, "IPSPolicyId": 19, "DomainId": 0,
"SubInterfaces": null, "LastModTs": "2017-12-12 16:56:11" }] }, "Ports": { "PortInfo": [{ "portId": 131,
"portSettings": { "portName": "G0/1", "portType": "SFP 1G Fiber", "configuration": { "speed": "TENGBPS",
"autoNegotiate": false, "duplex": "FULL", "mediaType": "FIBER", "useOnlyMcafeeCertifiedSFP": false },
"administrativeStatus": "DISABLE", "operationalStatus": "Down" }, "operatingMode": { "mode":
"INLINE_FAIL_CLOSE", "peerPort": "G0/2", "connectedTo": "INSIDE_NETWORK", "failOpenKit": "Unknown" },
"ResponseMode": { "sendResponseFrom": "THIS_PORT", "responsePortNo": 0 }, "ipSettings": null }, { "portId": 132,
"portSettings": { "portName": "G0/2", "portType": "---", "configuration": null, "administrativeStatus": null,
"operationalStatus": "---" }, "operatingMode": null, "ResponseMode": null, "ipSettings": null }, { "portId":
133, "portSettings": { "portName": "G3/1", "portType": "Copper Gigabit Ethernet (Gbps)", "configuration":
{ "speed": "ONEGBPS", "autoNegotiate": true, "duplex": "FULL", "mediaType": "COPPER",
"useOnlyMcafeeCertifiedSFP": true }, "administrativeStatus": "ENABLE", "operationalStatus": "Up" },
"operatingMode": { "mode": "INLINE_FAIL_CLOSE", "peerPort": "G3/2", "connectedTo": "OUTSIDE_NETWORK",
"failOpenKit": "Unknown" }, "ResponseMode": { "sendResponseFrom": "THIS_PORT", "responsePortNo": 0 },
"ipSettings": null }, { "portId": 134, "portSettings": { "portName": "G3/2", "portType": "Copper Gigabit
Ethernet (Gbps)", "configuration": { "speed": "ONEGBPS", "autoNegotiate": true, "duplex": "FULL", "mediaType":
"COPPER", "useOnlyMcafeeCertifiedSFP": true }, "administrativeStatus": "ENABLE", "operationalStatus": "Up" },
"operatingMode": { "mode": "INLINE_FAIL_CLOSE", "peerPort": "G3/1", "connectedTo": "INSIDE_NETWORK",
"failOpenKit": "Unknown" }, "ResponseMode": { "sendResponseFrom": "THIS_PORT", "responsePortNo": 0 },
"ipSettings": null }, { "portId": 135, "portSettings": { "portName": "G3/3", "portType": "Copper Gigabit
Ethernet (Gbps)", "configuration": { "speed": "ONEGBPS", "autoNegotiate": true, "duplex": "FULL", "mediaType":
"COPPER", "useOnlyMcafeeCertifiedSFP": true }, "administrativeStatus": "DISABLE", "operationalStatus": "Down" },
"operatingMode": { "mode": "INLINE_FAIL_OPEN_PASSIVE", "peerPort": "G3/4", "connectedTo": "INSIDE_NETWORK",
"failOpenKit": "Bypassing" }, "ResponseMode": { "sendResponseFrom": "THIS_PORT", "responsePortNo": 0 },
"ipSettings": null }, { "portId": 136, "portSettings": { "portName": "G3/4", "portType": "Copper Gigabit
Ethernet (Gbps)", "configuration": { "speed": "ONEGBPS", "autoNegotiate": true, "duplex": "FULL", "mediaType":
"COPPER", "useOnlyMcafeeCertifiedSFP": true }, "administrativeStatus": "DISABLE", "operationalStatus": "Down" },
"operatingMode": { "mode": "INLINE_FAIL_OPEN_PASSIVE", "peerPort": "G3/3", "connectedTo": "OUTSIDE_NETWORK",
"failOpenKit": "Bypassing" }, "ResponseMode": { "sendResponseFrom": "THIS_PORT", "responsePortNo": 0 },
"ipSettings": null }, { "portId": 137, "portSettings": { "portName": "G3/5", "portType": "Copper Gigabit
Ethernet (Gbps)", "configuration": { "speed": "ONEGBPS", "autoNegotiate": true, "duplex": "FULL", "mediaType":
"COPPER", "useOnlyMcafeeCertifiedSFP": true }, "administrativeStatus": "DISABLE", "operationalStatus": "Down" },
"operatingMode": { "mode": "INLINE_FAIL_OPEN_PASSIVE", "peerPort": "G3/6", "connectedTo": "INSIDE_NETWORK",
"failOpenKit": "Bypassing" }, "ResponseMode": { "sendResponseFrom": "THIS_PORT", "responsePortNo": 0 },
"ipSettings": null }, { "portId": 138, "portSettings": { "portName": "G3/6", "portType": "Copper Gigabit
Ethernet (Gbps)", "configuration": { "speed": "ONEGBPS", "autoNegotiate": true, "duplex": "FULL", "mediaType":
"COPPER", "useOnlyMcafeeCertifiedSFP": true }, "administrativeStatus": "DISABLE", "operationalStatus": "Down" },
"operatingMode": { "mode": "INLINE_FAIL_OPEN_PASSIVE", "peerPort": "G3/5", "connectedTo": "OUTSIDE_NETWORK",
"failOpenKit": "Bypassing" }, "ResponseMode": { "sendResponseFrom": "THIS_PORT", "responsePortNo": 0 },
"ipSettings": null }, { "portId": 139, "portSettings": { "portName": "G3/7", "portType": "Copper Gigabit
Ethernet (Gbps)", "configuration": { "speed": "ONEGBPS", "autoNegotiate": true, "duplex": "FULL", "mediaType":
"COPPER", "useOnlyMcafeeCertifiedSFP": true }, "administrativeStatus": "DISABLE", "operationalStatus": "Down" },
"operatingMode": { "mode": "INLINE_FAIL_OPEN_PASSIVE", "peerPort": "G3/8", "connectedTo": "INSIDE_NETWORK",
"failOpenKit": "Bypassing" }, "ResponseMode": { "sendResponseFrom": "THIS_PORT", "responsePortNo": 0 },
"ipSettings": null }, { "portId": 140, "portSettings": { "portName": "G3/8", "portType": "Copper Gigabit
Ethernet (Gbps)", "configuration": { "speed": "ONEGBPS", "autoNegotiate": true, "duplex": "FULL", "mediaType":
"COPPER", "useOnlyMcafeeCertifiedSFP": true }, "administrativeStatus": "DISABLE", "operationalStatus": "Down" },
"operatingMode": { "mode": "INLINE_FAIL_OPEN_PASSIVE", "peerPort": "G3/7", "connectedTo": "OUTSIDE_NETWORK",
"failOpenKit": "Bypassing" }, "ResponseMode": { "sendResponseFrom": "THIS_PORT", "responsePortNo": 0 },
"ipSettings": null }] } } }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor

Update Sensor Configuration

This URL performs configuration update for the specified Sensor.

Resource URL

PUT /sensor/<sensor_id>/action/update_sensor_config

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Integer	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`deviceName`	Name of the device	String	No
`isSigsetConfigPushRequired`	Is signature set/configuration required	Boolean	Yes
`isSSLPushRequired`	Policy visible to child domain	Boolean	Yes
`isBotnetPushRequired`	Firewall policy description	Boolean	Yes
`lastUpdateTime`	Last updated timestamp of the config push	String	No
`pendingChanges`	Configuration changes details	Object	No

Details of pendingChanges:

Field Name	Description	Data Type	Mandatory
`isPolicyConfigurationChanged`	Is policy configuration changed or not	Boolean	No
`isConfigurationChanged`	Is configuration changed or not	Boolean	No
`isSignatureSetConfigurationChanged`	Is signature set configuration changed or not	Boolean	No
`isSSLConfigurationChanged`	Is SSL configuration changed or not	Boolean	No
`isGloablPolicyConfigurationChanged`	Is global policy configuration changed or not	Boolean	No
`isGAMUpdateRequired`	Gateway Anti-Malware update on Sensor is required or not	Boolean	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`RequestId`	Sensor config update request id	String

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/sensor/1001/action/update_sensor_config

```
{ "deviceName" : "M-2950", "lastUpdateTime" : "2013-09-03 20:16:54.000 IST", "pendingChanges" :
{ "isPolicyConfigurationChanged" : true, "isConfigurationChanged" : false, "isMalwareConfigurationChanged" :
```

```
false, "isSignatureSetConfigurationChanged" : false, "isSSLConfigurationChanged" : false,
"isBotnetConfigurationChanged" : true, "isGloablPolicyConfigurationChanged" : false },
"isSigsetConfigPushRequired" : true, "isSSLPushRequired" : false, "isBotnetPushRequired" : true
"isGAMUpdateRequired": true }
```

Response

```
{ "RequestId": "1337547887180" }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1101	Error updating Sensor
3	500	1124	The Sensor is inactive
4	400	1140	Sensor is currently running in layer 2 bypass mode
5	400	1141	Concurrent process are running on the update server
6	400	1142	Please wait a minute and then try again, check the system log for details
7	400	1143	Bot file is null/not compatible with the Sensor
8	400	1144	Sensor is not a standalone device.Signature set download cannot be done on a failover device
9	400	1145	Botnet import is supported only for NTBA or IPS/NAC Sensor
10	400	1146	Invalid SSL keys, check the system log for details
11	400	1147	Total exception objects count exceeded the limit of
12	400	1148	Sensor software version is not compatible with the Manager
13	400	1149	SSL key decryption not enabled on Sensor
14	400	1150	No configuration changes to push
15	400	1151	No SSL decryption key existed
16	400	1152	Botnet is not enabled/ supported for this Sensor

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
17	400	1153	SSL key decryption is not supported for this Sensor
18	400	1201	This device requires a valid system license.
19	400	1202	This device requires a valid proxy decryption license.
20	400	1203	Incompatible license assignments detected. (The proxy decryption and system licenses must have the same capacity).
21	400	1204	The devices in this HA pair are running at different capacities and/or have invalid or mismatched system licenses.
22	400	1205	The devices in this HA pair are having mismatched proxy decryption licenses.
23	400	1206	One or more stack member Sensors not discovered.

Get Configuration Update Status

This URL gets the configuration update status for the specified request_id.

Resource URL

GET /sensor/<sensor_id>/action/update_sensor_config/<request_id>

Request Parameters

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes
`RequestId`	Sensor config update request ID	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`sigsetConfigPercentageComplete`	Percentage of the push completed	Number
`sigsetConfigStatusMessage`	Status message of the push	String
`botnetPercentageComplete`	Percentage of the push completed	Number

Field Name	Description	Data Type
`botnetStatusMessage`	Status message of the push	String
`SSLPercentageComplete`	Percentage of the push completed	Number
`SSLStatusMessage`	Status message of the push	String
`GamUpdatePercentageComplete`	Percentage of the push completed	Number
`GamUpdateStatusMessage`	Status message of the push	String

Example

Request

`GET` https://%3CNSM_IP%3E/sdkapi/sensor/1001/action/update_sensor_config/1337547887180

Response

```
{ "sigsetConfigPercentageComplete": 1, "sigsetConfigStatusMessage": "IN PROGRESS:Generating Signature Segments
for Sensor: M-2950. Sig Version: 8.6.0.19", "botnetPercentageComplete": 0, "botnetStatusMessage": "IN
PROGRESS:Queued: Generation of BOT DAT Signature file Segment for Sensor: M-2950", "SSLPercentageComplete": 100,
"SSLStatusMessage": "DOWNLOAD COMPLETE" "GamUpdatePercentageComplete":100, "GamUpdateStatusMessage ": "DOWNLOAD
COMPLETE" }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor

Is Sensor Config Modified

This URL provides the information whether sensor config has been modified and configuration update is pending to the Sensor. The configuration change details are provided as well.

Resource URL

GET /sensor/<sensor_id>/config/status

Request Parameters

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`deviceName`	Name of the device	String
`isSigsetConfigPushRequired`	Is sigset configuration required	Boolean
`isSSLPushRequired`	Policy visible to child domain	Boolean
`isBotnetPushRequired`	Firewall policy description	Boolean

Field Name	Description	Data Type
`lastUpdateTime`	Last updated timestamp of the config push	String
`pendingChanges`	Configuration changes details	Object
`isGAMUpdateRequired`	Gateway Anti-Malware update on Sensor is required or not	Boolean

Details of pendingChanges:

Field Name	Description	Data Type
`isPolicyConfigurationChanged`	Is policy configuration changed or not	Boolean
`isConfigurationChanged`	Is configuration changed or not	Boolean
`isSignatureSetConfigurationChanged`	Is sigset configuration changed or not	Boolean
`isSSLConfigurationChanged`	Is SSL configuration changed or not	Boolean
`isGloablPolicyConfigurationChanged`	Is global policy configuration changed or not	Boolean

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/sensor/1001/%20action/update_sensor_config

Response

```
{ "deviceName" : "M-2950", "lastUpdateTime" : "2013-09-03 20:16:54.000 IST", "pendingChanges" :
{ "isPolicyConfigurationChanged" : true, "isConfigurationChanged" : false, "isMalwareConfigurationChanged" :
false, "isSignatureSetConfigurationChanged" : false, "isSSLConfigurationChanged" : false,
"isBotnetConfigurationChanged" : true, "isGloablPolicyConfigurationChanged" : false },
"isSigsetConfigPushRequired" : true, "isSSLPushRequired" : false, "isBotnetPushRequired" : true
"isGAMUpdateRequired": true }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor

Get Sensor Performance Stats

This URL provides performance stats for the given metric for the specified sensor, and portId.

Resource URL

GET /sensor/<sensor_id>/performancestats?metric=<metric>&portId=<port_id>&sampling=<sampling>

Request Parameters

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor ID	Number	Yes

Field Name	Description	Data Type	Mandatory
`metric`	Performance stats metric. Can be "CPU_UTILIZATION" / "MEMORY_UTILIZATION" / "SENSOR_THROUGHPUT" (default) / "PORT_THROUGHPUT"	String	Yes
`port_id`	Port ID needs to be specified only if the metric being queried is PORT_THROUGHPUT	Number	No
`sampling`	Sampling for the stats. Can be “MINUTES” (default), “HOURS”,”DAYS”, “WEEKS”, “MONTHS”	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`statistics`	Statistics	Array

Details of object in statistics:

Field Name	Description	Data Type
`time`	Time	String
`value`	Value	Double
`flows`	Flow usage. Will be populated if the metric is "MEMORY_UTILIZATION "	Object

Details of object in flows:

Field Name	Description	Data Type
`flowUsage`	Flow usage value	Double
`decryptedFlow`	Decrypted flow value	Double
`packetBuffer`	Packet buffer value	Double
`systemMemory`	System memory value	Double

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/performancestats?metric=memory_utilization

Response

```
{ "statistic": [ { "time": "Tue Oct 25 22:24:00 PDT 2016", "value": 0, "flows": { "flowUsage": 0,
"decryptedFlow": 0, "packetBuffer": 0, "systemMemory": 33 } }, { "time": "Tue Oct 25 22:27:00 PDT 2016",
"value": 0, "flows": { "flowUsage": 0, "decryptedFlow": 0, "packetBuffer": 0, "systemMemory": 33 } }, ...............
{ "time": "Tue Oct 25 23:21:00 PDT 2016", "value": 0, "flows": { "flowUsage": 0, "decryptedFlow": 0,
"packetBuffer": 0, "systemMemory": 33 } } ] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	404	1123	Invalid performance metric
3	404	1122	Invalid port

Reboot Sensor

This URL reboots the specified Sensor.

Resource URL

PUT /sensor/<sensor_id>/action/reboot

Request Parameters

Field Name	Description	Data Type	Mandatory
sensor_id	Sensor ID	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Describes whether reboot has been successfully initiated	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1001/action/reboot

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive

Set IPv6

This URL does IPv6 Setting (Drop/Pass/Scan IPv6) on the specified Sensor.

Resource URL

POST /sensor/<sensor_id>/ipv6

Request Parameters

URL Request Parameter

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes

Payload Request Parameters

Field Name	Description	Data Type	Mandatory
`ipv6Mode`	IPv6 Mode to be set. Can be "DROP_IPV_6_TRAFFICINLINE_ONLY", "PASS_IPV_6_TRAFFIC", "SCAN_IPV_6_TRAFFIC"	string	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status returned	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/sensor/1001/ipv6

Payload

```
{ "ipv6Mode": "SCAN_IPV_6_TRAFFIC" }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive

Get IPv6 Setting

This URL gets IPv6 Setting (Drop/Pass/Scan IPv6) on the specified Sensor.

Resource URL

GET /sensor/<sensor_id>/ipv6

Request Parameters

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`ipv6Mode`	IPv6 Mode to be set. Can be "DROP_IPV_6_TRAFFICINLINE_ONLY", "PASS_IPV_6_TRAFFIC", "SCAN_IPV_6_TRAFFIC"	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/sensor/1001/ipv6

Response

```
{ "ipv6Mode": "SCAN_IPV_6_TRAFFIC" }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive

Get Sensor Status

This URL gets the Sensor status (Active/Disconnected).

Resource URL

GET /sensor/<sensor_id>/status

Request Parameters

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Sensor status, can be "ACTIVE"/"DISCONNECTED"	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/sensor/1001/status

Response

```
{ "status": "ACTIVE" }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor

Get Application Identification

This URL gets the application identification configuration defined for the Sensor.

Resource URL

GET sensor/<sensor_id>/policy/applicationidentification

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`enableApplicationIdentification`	Enable application identification flag	Boolean
`selectedPorts`	Selected ports	Strings list

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1003/policy/applicationidentification

Response

```
{ "enableApplicationIdentification": true, "selectedPorts": [ "1A", "1B", "2A" ] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1106	Invalid Sensor Id

Update Application Identification

This URL update to application identification configuration for the Sensor.

Resource URL

PUT sensor/<sensor_id>/policy/applicationidentification

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes

Payload Parameter

Field Name	Description	Data Type
`enableApplicationIdentification`	Enable application identification flag	Boolean
`selectedPorts`	Selected Ports	strings list

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Operation Status	Int

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1003/policy/applicationidentification

```
{ "enableApplicationIdentification": true, "selectedPorts": [ "1A", "1B", "2A" ] }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1106	Invalid Sensor Id

Get NTBA Integration Configuration

This URL gets the NTBA integration configuration.

Resource URL

GET sensor/<sensor_id>/ntbaintegration

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
sensor_id	Sensor Id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
exportingData	Exporting data	Object

Details of flow exporting data:

Field Name	Description	Data Type
ntbaIntegration	NTBA Integration	String
targetNTBA	NTBA name	String
flowCollectionIPAddr	Destination IP	String
flowCollectionUDPPort	Destination UDP port	Number
portUsedToExportTraffic	Flow source	Object
monitoringPorts	Monitoring ports	Object list

Details of portUsedToExportTraffic:

Field Name	Description	Data Type
designatedPort	Designated port for NTBA	String
portIPAddr	IP address for port	String
networkMask	network mask	String
defaultGateway	default gateway	String
VLANId	VLAN Id	Number

Details of monitoring ports:

Field Name	Description	Data Type
port	Port name	String

Field Name	Description	Data Type
portNTBADirection	NTBA direction for port	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/0/ntbaintegration

Response

```
{ "exportingData": { "ntbaIntegration":"ENABLED_EXPORTING_ONLY", "destinationNTBA":"ntba-nsmapi",
"destinationIPAddr":"1.1.1.8", "destinationUDPPort":9996 "portUsedToExportTraffic": { "designatedPort":"8A",
"portIPAddr":"1.1.1.11", "networkMask":"255.255.255.0", "defaultGateway":"1.1.1.8", "VLANId":0 },
"monitoringPorts": [ { "port":"8A", "portNTBADirection":"INTERNAL" } ] } } }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1106	Invalid Sensor Id

Update NTBA Integration Configuration

This URL updates the NTBA integration configuration.

Resource URL

PUT sensor/<sensor_id>/ntbaintegration

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
sensor_id	Sensor Id	Number	Yes

Payload Parameter

Field Name	Description	Data Type
exportingData	Exporting data	Object

Details of exporting data:

Field Name	Description	Data Type
ntbaIntegration	NTBA integration	String
targetNTBA	NTBA name	String
flowCollectionIPAddr	Destination IP	String
flowCollectionUDPPort	Destination UDP port	Number
portUsedToExportTraffic	Flow source	Object

Field Name	Description	Data Type
`monitoringPorts`	Monitoring ports	Object list

Details of portUsedToExportTraffic:

Field Name	Description	Data Type
`designatedPort`	Designated port for NTBA	String
`portIPAddr`	IP address for port	String
`networkMask`	network mask	String
`defaultGateway`	default gateway	String
`VLANId`	VLAN Id	Number

Details of monitoring ports:

Field Name	Description	Data Type
`port`	Port Name	string
`portNTBADirection`	NTBA Direction for PORT	string

Possible values for port NTBA direction

1. INTERNAL
2. EXTERNAL

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Operation Status	Int

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/0/ntbaintegration

Response

```
{ "exportingData": { "ntbaIntegration":"ENABLED_EXPORTING_ONLY", "destinationNTBA":"ntba-nsmapi",
"destinationIPAddr":"1.1.1.8", "destinationUDPPort":9996 "portUsedToExportTraffic": { "designatedPort":"8A",
"portIPAddr":"1.1.1.11", "networkMask":"255.255.255.0", "defaultGateway":"1.1.1.8", "VLANId":0 },
"monitoringPorts": [ { "port":"8A", "portNTBADirection":"INTERNAL" } ] } }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1106	Invalid Sensor Id

Get Device Software's Deployed and Available

This URL retrieves the device software's deployed and available.

Resource URL

GET sensor/<sensor_id>/deploydevicesoftware

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor ID	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`runningSoftwareVersion`	Software version deployed on the Sensor	String
`softwaresReadyForInstallation`	List of software versions ready for installation	Array

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/deploydevicesoftware

Response

```
{ " runningSoftwareVersion ": ‘9.1.5.9’, " softwaresReadyForInstallation ": [ "9.1.5.9","8.1.3.12" ] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1106	Invalid Sensor ID

Upgrade the Software on Device

This URL upgrades the software on device.

Resource URL

PUT sensor/<sensor_id>/deploydevicesoftware/<swVersion>

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor ID	Number	Yes

Field Name	Description	Data Type	Mandatory
`swVersion`	Software version to upgrade	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`RequestId`	The ID of the upgrade process	String

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1001/deploydevicesoftware/9.1.5.9

Response

```
{ "RequestId": "1337547887180" }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1106	Invalid Sensor ID
2	400	3010	Software version provided does not exist for the Sensor : (<sensor>:<version>)

Get the Upgrade Software Status

This URL gets the upgrade software status.

Resource URL

GET sensor/<sensor_id>/ deploydevicesoftware/<requestId>

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor ID	Number	Yes
`requestId`	Request ID returned while issuing the Sensor upgrade	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`updatePercentageComplete`	Percentage of the upgrade completed	Number

Field Name	Description	Data Type
updateStatusMessage	Update message	String

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1001/deploydevicesoftware/1337547887180

Response

```
{ " updatePercentageComplete ": 100, “updateStatusMessage” : “DOWNLOAD COMPLETE” }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1106	Invalid Sensor ID

Get Interface/Sub Interface Details

This URL gets interface or sub interface details.

Resource URL

GET /sensor/<sensor_id>/interface/<interface_id or subinterface_id>

Request Parameters

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes
`interface_id or subinterface_id`	Unique id of interface/sub interface	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Details of Interfaces:

Field Name	Description	Data Type
`InterfaceInfo`	List of interfaces	Array

Details of object in InterfaceInfo:

Field Name	Description	Data Type
`vidsId`	Unique Id to identify interface/sub interface	Number
`name`	Name of the interface	String
`Description`	Interface description	String
`InterfaceType`	Traffic type	Object
`IPSPolicyId`	IPS policy applied on interface	Number
`DomainId`	ID of the domain to which the interface is added	Number
`SubInterfaces`	Sub interface details	Object
`LastModTs`	Last modified timestamp	String

Details of InterfaceType:

Field Name	Description	Data Type
`Dedicated`	Default traffic type. No segmentation of traffic	Object

Field Name	Description	Data Type
`Vlan`	Segment of interface into multiple networks by VLAN tags	Object
`Cidr`	Enables segment of interface into multiple networks by CIDR addressing	Object
`BridgeVlan`	Segment of interface into multiple networks by bridge VLAN tags	Object

Details of CIDR:

Field Name	Description	Data Type
`CidrId`	List of CIDR IDs	Array

Details of Vlan:

Field Name	Description	Data Type
`id`	List of VLAN IDs	Array

Details of Bridge Vlan:

Field Name	Description	Data Type
`bridgeVlanRangeList`	List of bridge VLAN range	Array

Details of SubInterfaces:

Field Name	Description	Data Type
`SubInterfaceInfo`	List of sub interfaces	Array

Details of object in SubInterfaceInfo:

Field Name	Description	Data Type
`name`	Name of the interface	String
`vidsId`	Unique Id to identify subinterface	Number
`InterfaceType`	Traffic type. VLAN, CIDR, or BridgeVlan	String
`IPSPolicyId`	IPS policy applied on interface	Number
`LastModTs`	Last modified timestamp	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/sensor/1001/interface/105

Response

```
{ "InterfaceInfo": { "vidsId": 115, "name": "G3/7-G3/8", "Description": "", "Interfacetype": { "Dedicated":
null, "Vlan": null, "Cidr": null, "BridgeVlan": { "bridgeVlanRangeList": ["4094-4095", "5-6", "3-4", "1-2"] } },
"IPSPolicyId": 19, "DomainId": 0, "SubInterfaces": { "SubInterfaceInfo": [] }, "LastModTs": "2017-12-12
16:56:11" } }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	404	1107	Invalid interface or sub-interface id

Update Interface/Sub Interface Details

This URL updates interface or sub interface details.

Resource URL

PUT /sensor/<sensor_id>/interface/<interface_id or subinterface_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes
`interface_id or subinterface_id`	Unique id of interface/sub interface	Number	Yes

Payload Parameters:

Details of Interfaces :

Field Name	Description	Data Type
`InterfaceInfo`	List of interfaces	Array

Details of object in InterfaceInfo:

Field Name	Description	Data Type
`vidsId`	Unique Id to identify interface/sub interface	Number
`name`	Name of the interface	String
`Description`	Interface description	String
`InterfaceType`	Traffic type	Object
`IPSPolicyId`	IPS policy applied on interface	Number
`DomainId`	ID of the Domain to which the interface is added	Number
`SubInterfaces`	Sub interface details	Object

Field Name	Description	Data Type
LastModTs	Last modified timestamp	String

Details of InterfaceType:

Field Name	Description	Data Type
Dedicated	Default traffic type. No segmentation of traffic	Object
Vlan	Segment of interface into multiple networks by VLAN tags	Object
Cidr	Enables segment of interface into multiple networks by CIDR addressing	Object
BridgeVlan	Segment of interface into multiple networks by bridge VLAN tags	Object

Details of CIDR:

Field Name	Description	Data Type
CidrId	List of CIDR IDs	Array

Details of Vlan:

Field Name	Description	Data Type
id	List of VLAN IDs	Array

Details of Bridge Vlan:

Field Name	Description	Data Type
bridgeVlanRangeList	List of bridge VLAN range	Array

Details of SubInterfaces:

Field Name	Description	Data Type
SubInterfaceInfo	List of sub interfaces	Array

Details of object in SubInterfaceInfo:

Field Name	Description	Data Type
name	Name of the interface	String
vidsId	Unique Id to identify subinterface	Number
InterfaceType	Traffic type. VLAN, CIDR, or BridgeVlan	String
IPSPolicyId	IPS policy applied on interface	Number

Field Name	Description	Data Type
`LastModTs`	Last modified timestamp	String

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status returned by deletion	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/sensor/1001/interface/105

Payload

```
{ "InterfaceInfo": { "Description": "try1", "SubInterfaces": null, "IPSPolicyId": 17, "DomainId": 0,
"Interfacetype": { "Dedicated": null, "Vlan": { "id": [ "17", "18", "19", ] }, "Cidr": null }, "vidsId": 0,
"LastModTs": "2012-07-24 00:19:00", "name": "abc" } }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	404	1107	Invalid interface or sub-interface id
3	400	1154	Cannot update an interface in child admin domain
4	400	1157	Invalid interface name
5	400	1155	Name exceeding maximum length: 45
6	400	1156	Description exceeding maximum length: 45
7	400	1158	Non numeric vlan id(s) provided
8	400	1159	Duplicate vlan id(s) provided
9	400	1161	Out of range vlan id(s) provided:[vlan id list], Vlan id should be between 1 and 4094
10	400	1701	Invalid CIDR notation
11	400	1137	Duplicate CIDR entry

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
12	400	1111	Cannot create dedicated type sub interface
13	400	1160	Sub interface type cannot be changed
14	400	1131	Empty Vlan id list provided
15	400	1162	Vlan id(s) not available for allocation:
16	400	1177	Vlan range should be in from-to form
17	400	1176	Non numeric value provided
18	400	1175	From should be less than To in the range
19	400	1178	Duplicate bridge VLAN range found

Add Sub Interface

This URL adds a sub interface to the specified Interface. The details of sub interface to be created are given in the request body.

Resource URL

POST /sensor/<sensor_id>/interface/<interface_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes
`interface_id`	Unique interface id or interface/sub Interface	Number	Yes

Payload Parameters:

Details of Interfaces:

Field Name	Description	Data Type	Mandatory
`InterfaceInfo`	List of Interfaces	array	Yes

Details of object in InterfaceInfo:

Field Name	Description	Data Type	Mandatory
name	Name of the interface	String	Yes
Description	Interface description	String	Yes
InterfaceType	Traffic type	Object	Yes
IPSPolicyId	IPS policy applied on interface	Number	Yes
DomainId	ID of the Domain to which the interface is added	Number	Yes

Details of InterfaceType (Can be either of the below mentioned):

Field Name	Description	Data Type	Mandatory
Vlan	Segment of interface into multiple networks by VLAN tags	Object	Yes
Cidr	Enables segment of interface into multiple networks by CIDR addressing	Object	Yes
BridgeVlan	List of bridge vlan range Applicable for VM-IPS only	Object	Yes

Details of Vlan:

Field Name	Description	Data Type	Mandatory
Id	List of VLAN IDs	array	Yes

Details of CIDR:

Field Name	Description	Data Type
CidrId	List of CIDR IDs	array

Details of Bridge Vlan:

Field Name	Description	Data Type
bridgeVlanRangeList	List of bridge VLAN range	array

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
createdResourceId	Unique ID of the created sub interface	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/sensor/1001/interface/105

Payload

```
{ "InterfaceInfo": { "Description": "try1", "IPSPolicyId": 17, "DomainId": 0, "Interfacetype": { "Vlan": { "id":
[ "17", "18", "19" ] } }, "name": "xyz" } }
```

Response

```
{ "createdResourceId":127 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	404	1107	Invalid interface or sub-interface id
3	400	1108	Invalid policy Id
4	400	1111	Cannot create dedicated type sub interface
5	400	1160	Sub interface type cannot be changed
6	400	1157	Invalid interface name
7	400	1155	Name exceeding maximum length: 45
8	400	1131	Empty Vlan id list provided
9	400	1158	Non numeric vlan id(s) provided
10	400	1159	Duplicate vlan id(s) provided
11	400	1161	Out of range vlan id(s) provided:[vlan id list], Vlan id should be between 1 and 4094
12	400	1163	Following vlan id(s) is/are already added/assigned: [vlan id list]
13	400	1165	No Vlan id is available for assignment in parent interface
14	400	1166	Following vlan id(s) not present in parent interface for assignment on sub interface
15	400	1701	Invalid CIDR notation

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
16	400	1137	Duplicate CIDR entry
17	400	1133	Invalid CIDR provided
18	400	1177	Vlan range should be in from-to form
19	400	1176	Non numeric value provided
20	400	1175	"From" should be less than "To" in the range
21	400	1178	Duplicate bridge VLAN range found

Delete a Sub Interface

This URL deletes a sub interface. Only Sub Interface can be deleted, if an interface_id is mentioned, the operation throws an error.

Resource URL

DELETE /sensor/<sensor_id>/interface/<subinterface_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes
`subinterface_id`	Unique sub Interface ID	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status returned by deletion	Number

Example

Request

DELETE https://%3CNSM_IP%3E/sdkapi/sensor/1001/interface/124

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
2	404	1107	Invalid interface or sub-interface id

Add/Assign VLAN

This URL adds a vlan to the VLAN type specified interface. If a sub interface is given, the VLAN is assigned to the sub interface.

Resource URL

POST /sensor/<sensor_id>/interface/<interface_id or subinterface_id>/vlan

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes
`interface_id or subinterface_id`	Unique interface/subInterface ID	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`VlanIds`	VLAN IDs	Object	Yes

Details of object in VlanIds:

Field Name	Description	Data Type	Mandatory
`id`	List of VLAN IDs	Array	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status returned by deletion	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/sensor/1001/interface/105/vlan

Payload

```
{ "VlanIds": { "id": [ "17", "18", "19" ] } }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	404	1107	Invalid interface or sub-Interface id
3	400	1158	Non numeric vlan id(s) provided
4	400	1159	Duplicate vlan id(s) provided
5	400	1161	Out of range vlan id(s) provided:[vlan id list], Vlan id should be between 1 and 4094
6	400	1173	Cannot add vlan on dedicated/cidr type interface
7	400	1163	Following vlan id(s) is/are already added/assigned:
8	400	1165	No Vlan id is available for assignment in parent interface
9	400	1166	Following vlan id(s) not present in parent interface for assignment on sub interface:

Delete/Revoke VLAN

This URL:

1. Revokes vlans from sub interface if subinterface-id is mentioned
2. Deletes vlan from interface if interface id is mentioned

Multiple comma separated vlans can be provided for this operation.

Resource URL

DELETE /sensor/<sensor_id>/interface/<interface_id or subinterface_id>/vlan/<vlan_ids>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes
`interface_id or subinterface_id`	Unique interface/subInterface ID	Number	Yes
`vlan_ids`	Comma separated VLAN IDs	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status returned by deletion	Number

Example

Request

DELETE https://%3CNSM_IP%3E/sdkapi/sensor/1001/interface/127/vlan/17,18,19

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	404	1107	Invalid interface or sub-Interface id
3	400	1158	Non numeric vlan id(s) provided
4	400	1159	Duplicate vlan id(s) provided
5	400	1161	Out of range vlan id(s) provided:[vlan id list], Vlan id should be between 1 and 4094
6	400	1167	No Vlan Id available to delete/ revoke
7	400	1168	Invalid vlan id(s) provided to delete/revoke
8	400	1169	Cannot revoke all vlan ids from subinterface

Get Available Interfaces to Allocate

This URL returns the available interfaces to be allocated.

Resource URL

GET /domain/<domain_id>/sensor/<sensor_id>/availableinterfaces

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes
sensor_id	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
SensorInfo	Array of type interface information	Array

Details of fields in InterfaceInf:

Field Name	Description	Data Type
interfaceId	Interface Id	Int
name	Interface name	String
interfaceType	Interface type	Object
subInterfaces	Array of type Interface Info	Array

Details of interfaceType:

Field Name	Description	Data Type
Dedicated	Default traffic type. No segmentation of traffic	Object
Vlan	Segment of interface into multiple networks by VLAN tags	Object
Cidr	Enables segment of interface into multiple networks by CIDR addressing	Object
BridgeVlan	List of bridge vlan id(applicable for VM-IPS only)	Object

Details of CIDR:

Field Name	Description	Data Type
cidrList	List of CIDR IDs	Array

Details of BridgeVlan:

Field Name	Description	Data Type
bridgeVlanRangeList	List of bridge VLAN range	Array

Details of Vlan:

Field Name	Description	Data Type
`id`	List of VLAN IDs	Array

Example

Request

https://%3CNSM_IP%3E/sdkapi/domain/103/sensor/1002/availableinterfaces

Response

```
{ "interfaceInfoList": [ { "interafaceId": 123, "name": "3B", "interfacetype": { "Dedicated": { } } },
{ "interafaceId": 116, "name": "1A-1B", "interfacetype": { "Dedicated": { } } }, { "interafaceId": 115, "name":
"2A-2B", "interfacetype": { "Vlan": { "id": [ "8", "9" ] } } }, { "interafaceId": 114, "name": "3A",
"interfacetype": { "Dedicated": { } } }, { "interafaceId": 113, "name": "4A-4B", "interfacetype": { "Dedicated":
{ } } }, { "interafaceId": 112, "name": "5A-5B", "interfacetype": { "Dedicated": { } } }, { "interafaceId": 111,
"name": "6A-6B", "interfacetype": { "Dedicated": { } } }, { "interafaceId": 110, "name": "7A-7B",
"interfacetype": { "Cidr": { "cidrList": [ "192.168.0.0/23" ] } } } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	404	1106	Invalid Sensor

Get List of Interfaces Allocated to a Sensor Inside a Domain

This URL gets interfaces allocated to a Sensor inside a domain.

Resource URL

GET /domain/<domain_id>/sensor/<sensor_id>/allocatedinterfaces

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain ID	Number	Yes
`sensor_id`	Sensor ID	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`AllocatedInterfaceList`	Array of type allocated interface list	Array

Details of fields in allocated interface list:

Field Name	Description	Data Type
`interfaceId`	Interface id	Number

Field Name	Description	Data Type
interfaceName	Interface name	String
interfaceType	Interface Type	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/domain/103/sensor/1001/allocatedinterfaces

Response

```
{ "allocatedInterfaceList": [ { "interfaceName": "2A-2B", "interfaceId": 173, "interfaceType": "Vlan" },
{ "interfaceName": "4A-4B", "interfaceId": 113, "interfaceType": "Dedicated" } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	404	1106	Invalid Sensor

Get List of CIDR Allocated to an Interface

This URL gets CIDR list allocated to an interface.

Resource URL

GET /sensor/<sensor_id>/interface/<interface_id>/allocatedcidrlist

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensor_id	Sensor ID	Number	Yes
interface_id	Interface ID	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
AllocatedCidrListElem	List of CIDR	Array

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/sensor/1002/interface/110/allocatedcidrlist

Response

```
{ "cidrList": [ "192.168.0.0/28" ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	404	1106	Invalid Sensor
3	404	1107	Invalid interface or sub-interface id

Allocate an Interface to a Sensor in Child Domain

This URL allocates an interface to a Sensor in child domain.

Resource URL

PUT /domain/<domain_id>/sensor/<sensor_id>/allocateinterface

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain ID	Number	Yes
`sensor_id`	Sensor ID	Number	Yes

Payload Parameters:

Field Name	Description	Data Type
`AllocatingInterfaceElem`	Object that contains the details of the field to be sent	Object

Details of fields in AllocatingInterfaceElem :

Field Name	Description	Data Type	Mandatory
`interfaceId`	Interface ID	Number	Yes
`vlanIdList`	Vlan ID list, should be provided when allocating an interface of vlan type	Array of number	No
`cidrList`	CIDR list, should be provided when allocating an interface of CIDR type	Array of string	No
`bridgeVlanList`	List of bridge vlan id(applicable for VM-IPS device only)	Array of string	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/domain/103/sensor/1002/allocateinterfaces

Payload

```
{ "interfaceId": 115, "vlanIdList": [8] }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	404	1106	Invalid Sensor
3	404	1107	Invalid interface or sub-interface id
4	400	1131	Empty Vlan id list provided
5	400	1158	Non numeric vlan id(s) provided
6	400	1159	Duplicate vlan id(s) provided
7	400	1161	Out of range vlan id(s) provided:[vlan id list], Vlan id should be between 1 and 4094
8	400	1164	Invalid Vlan id provided
9	400	1164	Provided Vlan id(s) already allocated
10	400	1130	Empty CIDR list provided
11	400	1701	Invalid CIDR notation
12	400	1137	Duplicate CIDR entry

Delete/Revoke an Interface from a Sensor in Child Domain

This URL revokes an interface from a Sensor in child domain.

Resource URL

DELETE /domain/<domain_id>/sensor/<sensor_id>/interface/<interface_id>/revokeinterface?value=<id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain ID	Number	Yes
`sensor_id`	Sensor ID	Number	Yes
`interface_id`	Interface ID	Number	Yes
`id`	Vlan ID, Bridge Vlan ID, or CIDR value, should be provided when revoking an interface of Vlan/CIDR type	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

DELETE https://%3CNSM_IP%3E/sdkapi/domain/103/sensor/1002/interface/124/revokeinterface?value=8

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	404	1106	Invalid Sensor
3	404	1107	Invalid Interface or Sub-interface id
4	400	1134	Provided interface not allocated to the specified domain
5	400	1132	Invalid Vlan id provided
6	400	1133	Invalid CIDR provided

Adds/Assign CIDR

This URL adds CIDRs to a specified Interface.

Resource URL

POST /sensor/<sensor_id>/interface/<interface_id>/cidr

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor ID	Number	Yes
`interface_id`	Interface ID	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`cidrList`	List of CIDRS	Array	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	1 is returned if the operation was successfull.	Number

Example

Request

POST https://<NSM_IP>/sdkapi/sensor/1001/interface/105/cidr

```
Payload { "cidrList": [ "8.8.8.1/32", "8.8.8.12/32", "8.8.8.13/32" ] }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	404	1107	Invalid Interface or Sub-interface id
3	400	1174	Cannot add CIDR on dedicated/vlan type interface
4	400	1701	Invalid CIDR notation
5	400	1137	Duplicate CIDR entry
6	400	1133	Invalid CIDR provided
7	500	1001	Internal error

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
8	400	1170	No CIDR available for allocation

Delete CIDR

This URL deletes CIDRs.

Resource URL

DELETE /sensor/<sensor_id>/interface/<interface_id>/cidr

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes
`interface_id`	Unique interface/subInterface id	Number	Yes

Payload Parameters:

Details of CIDR's:

Field Name	Description	Data Type	Mandatory
`cidrList`	List of CIDRS	Array	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status returned by deletion.	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/sensor/1001/interface/124/cidr

```
Payload { "cidrList": [ "8.8.8.1/32", "8.8.8.12/32", "8.8.8.13/32" ] }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	404	1107	Invalid interface or sub-interface ID

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
3	400	1701	Invalid CIDR notation
4	400	1137	Duplicate CIDR entry
5	400	1133	Invalid CIDR provided
6	500	1001	Internal error
7	400	1170	No CIDR available for allocation
8	400	1172	Invalid CIDR(s) provided to delete/revoke.

Get Port Configuration Details

This URL gets port configuration details for a specific port of a Sensor.

Resource URL

GET /sensor/<sensor_id>/port/<port_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes
`port_id`	Port Id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`PortInfo`	Port information	Object

Details of PortInfo:

Field Name	Description	Data Type
`portId`	Unique Id to identify port	Number
`portSettings`	Describes port configurations	Object
`operatingMode`	Port operating mode	Object
`ResponseMode`	Port response mode	Object

Details of portSettings:

Field Name	Description	Data Type
`portName`	Name of the port	String
`portType`	Describes port type	String
`configuration`	Port configuration (Speed and Duplex)	Object
`administrativeStatus`	Port administrative status. Can be "Enabled" or "Disabled"	String
`operationalStatus`	Port operational status, Can be "Up" or "Down"	String

Details of configuration:

Field Name	Description	Data Type
`Speed`	Port speed	String
`Duplex`	Full/Half duplex port	String

Details of operatingMode:

Field Name	Description	Data Type
`Mode`	Port mode	String
`peerPort`	Describes port peer	String
`connectedTo`	Peer port connected to, can be "Inside Network" / "Outside Network" / "n/a" (in case of span port)	String

Details of ResponseMode:

Field Name	Description	Data Type
`sendResponseFrom`	Send response from port	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/sensor/1001/port/101

Response

```
{ "portInfo": { "ResponseMode": { "sendResponseFrom": "This Port" }, "portId": 112, "operatingMode":
{ "connectedTo": "Inside Network", "mode": "In-line Fail-close (Port Pair)", "peerPort": "2B" }, "portSettings":
{ "portName": "2A", "portType": "SFP Gigabit Ethernet (Gbps) Fiber", "configuration": { "duplex": "Full",
"speed": "1 Gbps Auto-Negotiate" }, "administrativeStatus": "Disabled", "operationalStatus": "Down" } } }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	404	1122	Invalid port

Get all Attacks

This URL gets all available attack definitions in the Manager.

Resource URL

GET /attacks/

Request Parameters

URL Parameters: None

Field Name	Description	Data Type	Mandatory
attack_id	Unique attack id	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
AttackDescriptorDetailsList	List of attacks with basic information of each attack	Array

Details of object in AttackDescriptorDetailsList:

Field Name	Description	Data Type
attackId	Attack NSP id	String
name	Attack name	String
DosDirection	Attack direction, can be "INBOUND" / "OUTBOUND" / "BOTH"	String
Severity	Attack severity, number between 0 and 9	Number
description	Attack details	Object

Details of description:

Field Name	Description	Data Type
definition	Attack definition	String
btp	BTP	String
rfSB	RFSB	String
protectionCategory	Protection category	String
target	Attack target	String

Field Name	Description	Data Type
httpResponseAttack	HTTP response attack	String
priority	Priority	String
protocols	Protocols	String
attackCategory	Attack category	String
attackSubCategory	Attack sub category	String
snortEngine	Snort engine	String
versionAdded	Signature set version in which the attack was added	String
versionUpdated	Recent signature set version in which the attack was updated	String
reference	References	Object
signatures	Signatures	Array
componentAttacks	Component attacks	Array
comments	Comments	Object

Details of reference:

Field Name	Description	Data Type
nspId	NSP id	String
cveId	CVE id list	String
microsoftId	Microsoft id list	String
bugtraqId	Bug Ttaq id list	String
certId	Cert id list	String
arachNidsId	ArchNid id list	String
additionInfo	Any additional info	String

Details of object under signatures:

Field Name	Description	Data Type
name	Signature name	String
conditions	List of conditions	List of string

Details of object under componentAttacks:

Field Name	Description	Data Type
nspId	NSP id	String

Field Name	Description	Data Type
attackName	Attack name	String

Details of comments:

Field Name	Description	Data Type
comments	Comments	String
availabeToChildDomains	Available to child domains or not	Boolean
parentDomainComments	Parent domain comments	String

Example

Request

GET https://<NSM_IP>/sdkapi/attacks

Response

```
{ "AttackDescriptorDetailsList": [ ... { "DosDirection": null, "Severity": 5, "attackId": "0x00000100", "name":
"IP: IP Fragment too Large", "description": { "definition": "The Fragment offset plus the length exceeds 65,535.
This generic condition indicates either errors in some network hardware/software, or maliciously constructed
fragmented packets.\n\nnull\n\nnull\n\nnull\n\nSoftware Packages <br>any Internet connected machine<ul></ul>",
"btp": "Low", "rfSB": "No", "protectionCategory": "[Network Protection/IP]", "target": "Server",
"httpResponseAttack": "No", "priority": "High", "protocols": "ipv4", "attackCategory": "Exploit",
"attackSubCategory": "Protocol Violation", "snortEngine": "---", "versionAdded": "10.8.10.6", "versionUpdated":
"10.8.10.6", "reference": { "nspId": "0x00000100", "cveId": "", "microsoftId": "", "bugtraqId": "", "certId":
"", "arachNidsId": "", "additionInfo": null }, "signatures": [ { "name": "Signature#1", "conditions":
[ "condition 1", " System Event Name=\"ip-fragment-too-large\" " ] } ], "componentAttacks": [], "comments":
{ "comments": "", "availabeToChildDomains": true, "parentDomainComments": null } } } ... ] }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Get Attack Details

This URL gets details for a particular attack.

Resource URL

GET /attack/<attack_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
attack_id	Unique attack id	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
AttackDescriptor	Basic attack information	Object

Details of AttackDescriptor:

Field Name	Description	Data Type
attackId	Attack id	String
name	Attack name	String
DosDirection	Attack direction, can be "INBOUND" / "OUTBOUND" / "BOTH"	String
Severity	Attack severity, number between 0 and 9	Number
description	Attack details	Object

Details of description:

Field Name	Description	Data Type
definition	Attack definition	String
btp	BTP	String
rfSB	RFSB	String
protectionCategory	Protection category	String
target	Attack target	String
httpResponseAttack	HTTP response attack	String
priority	Priority	String
protocols	Protocols	String
attackCategory	Attack category	String
attackSubCategory	Attack sub category	String
snortEngine	Snort engine	String
versionAdded	Signature set version in which the attack was added	String
versionUpdated	Recent signature set version in which the attack was updated	String
reference	References	Object
signatures	Signatures	Array
componentAttacks	Component attacks	Array

Field Name	Description	Data Type
`comments`	Comments	Object

Details of reference:

Field Name	Description	Data Type
`nspId`	NSP id	String
`cveId`	CVE did list	String
`microsoftId`	Microsoft id list	String
`bugtraqId`	Bug traq id list	String
`certId`	Cert id list	String
`arachNidsId`	ArchNid id list	String
`additionInfo`	Any additional info	String

Details of object under signatures:

Field Name	Description	Data Type
`name`	Signature name	String
`conditions`	List of conditions	List of string

Details of object under componentAttacks:

Field Name	Description	Data Type
`nspId`	NSP id	String
`attackName`	Attack name	String

Details of comments:

Field Name	Description	Data Type
`comments`	Comments	String
`availabeToChildDomains`	Available to child domains or not	Boolean
`parentDomainComments`	Parent domain comments	String

Example

Request

GET https://<NSM_IP>/attack/0x00000100

Response

```
{ "AttackDescriptor": { "DosDirection": null, "Severity": 5, "attackId": "0x00000100", "name": "IP: IP Fragment
too Large", "description": { "definition": "The Fragment offset plus the length exceeds 65,535. This generic
condition indicates either errors in some network hardware/software, or maliciously constructed fragmented
packets.\n\nnull\n\nnull\n\nnull\n\nSoftware Packages <br>any Internet connected machine<ul></ul>", "btp":
"Low", "rfSB": "No", "protectionCategory": "[Network Protection/IP]", "target": "Server", "httpResponseAttack":
"No", "priority": "High", "protocols": "ipv4", "attackCategory": "Exploit", "attackSubCategory": "Protocol
Violation", "snortEngine": "---", "versionAdded": "10.8.10.6", "versionUpdated": "10.8.10.6", "reference":
{ "nspId": "0x00000100", "cveId": "", "microsoftId": "", "bugtraqId": "", "certId": "", "arachNidsId": "",
```

"additionInfo": null }, "signatures": [{ "name": "Signature#1", "conditions": ["condition 1", " System Event Name=\"ip-fragment-too-large\" "] }], "componentAttacks": [], "comments": { "comments": "", "availabeToChildDomains": true, "parentDomainComments": null } } } }

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	404	1402	Invalid attack id

Get IPS Policies in a Domain

This URL gets all the IPS policies defined in the specific domain.

Resource URL

GET /domain/<domain_id>/ipspolicies

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`PolicyDescriptorDetailsList`	List of IPS policies with brief policy details	Array

Details of object in PolicyDescriptorDetailsList:

Field Name	Description	Data Type
`IsEditable`	Is policy editable	Boolean
`DomainId`	Id of domain to which this policy belongs to	Number
`VisibleToChild`	Policy visible to child domain	Boolean
`policyId`	Policy id	Number
`name`	Policy name	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/domain/0/ipspolicies

Response

```
{ "PolicyDescriptorDetailsList": [ { "name": "Default IPS Attack Settings", "DomainId": "0", "policyId": "-1",
"IsEditable": "true", "VisibleToChild": "true" }, { "name": "Default IDS", "DomainId": "0", "policyId": "0",
"IsEditable": "true", "VisibleToChild": "true" }, { "name": "All-Inclusive Without Audit", "DomainId": "0",
"policyId": "16", "IsEditable": "true", "VisibleToChild": "true" }, { "name": "All-Inclusive With Audit",
"DomainId": "0", "policyId": "17", "IsEditable": "true", "VisibleToChild": "true" }, { "name": "Null",
"DomainId": "0", "policyId": "18", "IsEditable": "true", "VisibleToChild": "true" }, { "name": "Default Inline
IPS", "DomainId": "0", "policyId": "19", "IsEditable": "true", "VisibleToChild": "true" } ] }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Get IPS Policy Details

This URL gets the policy details (including attack set and response actions) for the specific IPS policy.

Resource URL

GET /ipspolicy/<policy_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
policy_id	IPS policy id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
PolicyDescriptor	Baseline IPS policy details	Object

Details of PolicyDescriptor:

Field Name	Description	Data Type
PolicyName	Baseline IPS policy name	String
Description	Policy description	String
IsVisibleToChildren	Is policy visible to child domain	Boolean
InboundRuleSet	Inbound policy rule set	String
OutboundRuleSet	Outbound policy rule set	String
AttackCategory	Attack category	Object
OutboundAttackCategory	Outbound attack category	Object
DosPolicy	DOS policy	Object
DosResponseSensitivityLevel	Dos response sensitivity level	Number
IsEditable	Is policy editable	Boolean
Timestamp	Time stamp at which the policy was added	String
VersionNum	Policy version number	Number

Field Name	Description	Data Type
`IsLightWeightPolicy`	Is light weight policy configured	Boolean

Details of object in AttackCategory:

Field Name	Description	Data Type
`ExpolitAttackList`	List of exploit attacks	Array

Details of object in ExpolitAttackList:

Field Name	Description	Data Type
`attackName`	Attack name	String
`nspId`	NSP id of the attack	String
`severity`	Attack severity, number between 0 & 9	Number
`isSeverityCustomized`	Is attack severity customized	Boolean
`isEnabled`	Is attack enabled	Boolean
`isAlertCustomized`	Is alert customized	Boolean
`isRecommendedForSmartBlocking`	Is attack recommended for smart blocking	Boolean
`AttackResponse`	Attack response	Object
`notification`	Notifications configured	Object
`protocolList`	List of protocols	Array
`applicationsImpactedList`	List of applications impacted	Array
`attackVector`	List of attack vectors	Array
`benignTriggerProbability`	Attack benign trigger probability	String
`target`	Attack target, can be "Server" or "Client"	String
`blockingType`	Blocking type, can be "Attack Packet"	String
`subCategory`	Attack sub category	String
`direction`	Attack direction, can be "INBOUND" / "OUTBOUND" / "BOTH"	String
`isAttackCustomized`	Is attack customized	Boolean

Details of object in AttackResponse:

Field Name	Description	Data Type
`TCPReset`	TCP reset option, can be “DISABLED” / “SOURCE” / “DESTINATION” / “BOTH”	String

Field Name	Description	Data Type
isTCPResetCustomized	Is TCP reset customized	Boolean
isICMPSend	Send ICMP host unreachable to Source	Boolean
isICMPSendCustomized	Send ICMP host unreachable to Source customized	Boolean
mcafeeNACNotification	NAC notification configured, can be "DISABLED" / "ALL_HOSTS" / "MCAFEE_NAC_UNMANAGED_HOSTS"	String
isMcafeeNACNotificationEnabled	Is NAC notification enabled	Boolean
isQuarantineCustomized	Is quarantine customized	Boolean
isRemediateEnabled	is remediate enabled	Boolean
blockingOption	Blocking option configured, can be "DISABLE" / "ENABLE" / "ENABLE_SMART_BLOCKING"	String
isBlockingOptionCustomized	Is blocking option customized	Boolean
isCapturedPrior	Should application data be captured prior to attack	Boolean
isCapturedPriorCustomized	Should application data be captured prior to attack customized	Boolean
action	Action to be taken on attack, can be "DO_NOTHING" / "SEND_ALERT_AND_LOG_PACKETS" / "SEND_ALERT_ONLY"	String
isLogCustomized	Is logging customized	Boolean
flow	Customixe flow, can be "SINGLE_FLOW" / "FORENSIC_ANALYSIS"	String
isFlowCustomized	Customize flow type	Boolean
isNbytesCustomized	is logging N bytes in each packet customized	Boolean
numberOfBytesInEachPacket	Number of bytes to be logged in each packet	Object
loggingDuration	Packet logging duration	Object
TimeStamp	Time stamp	String

Details of object in numberOfBytesInEachPacket (Can be either of the below mentioned):

Field Name	Description	Data Type
LogEntirePacket	Log entire packet	Object

Field Name	Description	Data Type
`CaptureNBytes`	Capture N bytes	Object

Details of object in CaptureNBytes:

Field Name	Description	Data Type
`NumberOfBytes`	Number of bytes to log	Number

Details of object in loggingDuration (Can be either of the below mentioned):

Field Name	Description	Data Type
`AttackPacketOnly`	Log attack packet only	Object
`CaptureNPackets`	Capture N packets	Object
`CaptureTimeDuration`	Capture for a time duration	Object
`RestOfFlow`	Capture rest of flow	Object

Details of object in CaptureNPackets:

Field Name	Description	Data Type
`npackets`	Log n packets	Number

Details of object in CaptureTimeDuration:

Field Name	Description	Data Type
`time`	Capture time	String
`timeUnit`	Time unit, can be "SECONDS" / "MINUTES" / "HOURS" / "DAYS"	String

Details of object in notification:

Field Name	Description	Data Type
`isEmail`	Is notification configured through email	Boolean
`isPager`	Is notification configured through pager	Boolean
`isScript`	Is notification configured through script	Boolean
`isAutoAck`	Is notification configured through auto ack	Boolean
`isSnmp`	Is notification configured through snmp	Boolean
`isSyslog`	Is notification configured through syslog	Boolean
`isEmailCustomized`	Is notification through email customized	Boolean
`isPagerCustomized`	Is notification through pager customized	Boolean

Field Name	Description	Data Type
`isScriptCustomized`	Is notification through script customized	Boolean
`isAutoAckCustomized`	Is notification through auto ack customized	Boolean
`isSnmpCustomized`	Is notification through snmp customized	Boolean
`isSyslogCustomized`	Is notification through syslog customized	Boolean

Details of object in DosPolicy:

Field Name	Description	Data Type
`LearningAttack`	List of learning attacks	Array
`ThresholdAttack`	List of threshold attacks	Array
`TimeStamp`	Time stamp	String

Details of object in LearningAttack:

Field Name	Description	Data Type
`attackName`	Attack name	String
`nspId`	NSP ID of the attack	String
`isSeverityCustomized`	Is attack severity customized	Boolean
`severity`	Attack severity, number between 0 & 9	Number
`isBlockingSettingCustomized`	Is blocking customized	Boolean
`isDropPacket`	Drop DoS attack packets of this attack type when detected	Boolean
`isAlertCustomized`	Is alert customized	Boolean
`isSendAlertToManager`	Is alert notification to be sent to Manager configured	String
`timeStamp`	Time stamp	String
`direction`	Attack direction, can be "INBOUND" / "OUTBOUND" / "BOTH"	String
`notification`	Notification to be sent via	Object
`isAttackCustomized`	Is DoS learning attack customized	Boolean

Details of object in ThresholdAttack:

Field Name	Description	Data Type
`attackName`	Attack name	String
`nspId`	NSP id of the attack	String

Field Name	Description	Data Type
`isSeverityCustomized`	Is attack severity customized	Boolean
`severity`	Attack severity, number between 0 & 9	Number
`isThresholdValueCustomized`	Is threshold value customized	Boolean
`isThresholdDurationCustomized`	Is threshold duration customized	Boolean
`ThresholdValue`	Threshold values	Number
`ThresholdDuration`	Threshold Interval (Seconds)	Number
`isAlertCustomized`	Is alert customized	Boolean
`isSendAlertToManager`	Is alert notification to be sent to Manager configured	String
`TimeStamp`	Time stamp	String
`Notification`	Notification to be sent	Object
`direction`	Attack direction, can be "INBOUND" / "OUTBOUND" / "BOTH"	String
`isAttackCustomized`	Is DoS threshold attack customized	Boolean

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ipspolicy/0

Response

```
{ "PolicyDescriptor": { "PolicyName": "IpsPolicy", "Description": "To test the IPS policy",
"IsVisibleToChildren": true, "InboundRuleSet": "TestIPS", "OutboundRuleSet": "Null", "AttackCategory":
{ "ExpolitAttackList": [ { "attackName": "FTP: VMware Flaw in NAT Function", "nspId": "0x4050b400", "severity":
7, "isSeverityCustomized": false, "isEnabled": true, "isAlertCustomized": false,
"isRecommendedForSmartBlocking": false, "AttackResponse": { "TCPReset": "DISABLED", "isTcpResetCustomized":
false, "isICMPSend": false, "isICMPSendCustomized": false, "mcAfeeNACNotification": "DISABLED",
"isMcAfeeNACNotificationEnabled": false, "isQuarantineCustomized": false, "isRemediateEnabled": false,
"blockingOption": "DISABLE", "isBlockingOptionCustomized": false, "isCapturedPrior": true,
"isCapturedPriorCustomized": false, "action": "SEND_ALERT_ONLY", "isLogCustomized": false, "isFlowCustomized":
false, "isNbytesCustomized": false, "numberOfBytesInEachPacket": { "LogEntirePacket": { } } }, "notification":
{ "isEmail": false, "isPager": false, "isScript": false, "isAutoAck": false, "isSnmp": false, "isSyslog": false,
"isEmailCustomized": false, "isPagerCustomized": false, "isScriptCustomized": false, "isAutoAckCustomized":
false, "isSnmpCustomized": false, "isSyslogCustomized": false }, "protocolList": [ "ftp" ],
"benignTriggerProbability": "1 (Low)", "blockingType": "attack-packet", "subCategory": "code-execution",
"direction": "INBOUND", "isAttackCustomized": false } ] }, "OutboundAttackCategory": { }, "DosPolicy":
{ "LearningAttack": [ { "attackName": "TCP Control Segment Anomaly", "nspId": "0x40008700",
"isSeverityCustomized": false, "severity": 7, "isBlockingSettingCustomized": false, "isDropPacket": false,
"IsAlertCustomized": false, "isSendAlertToManager": true, "direction": "BOTH", "notification": { "isEmail":
false, "isPager": false, "isScript": false, "isAutoAck": false, "isSnmp": false, "isSyslog": false,
"isEmailCustomized": false, "isPagerCustomized": false, "isScriptCustomized": false, "isAutoAckCustomized":
false, "isSnmpCustomized": false, "isSyslogCustomized": false }, "isAttackCustomized": false } ],
"ThresholdAttack": [ { "attackName": "Too Many Inbound TCP SYNs", "nspId": "0x40008c00", "isSeverityCustomized":
false, "severity": 6, "isThresholdValueCustomized": false, "isThresholdDurationCustomized": false,
"ThresholdValue": 2000, "ThresholdDuration": 5, "isAlertCustomized": false, "isSendAlertToManager": false,
"Notification": { "isEmail": false, "isPager": false, "isScript": false, "isAutoAck": false, "isSnmp": false,
"isSyslog": false, "isEmailCustomized": false, "isPagerCustomized": false, "isScriptCustomized": false,
"isAutoAckCustomized": false, "isSnmpCustomized": false, "isSyslogCustomized": false }, "direction": "INBOUND",
"isAttackCustomized": false } ], "TimeStamp": "2012-06-20 18:44:55.000" }, "DosResponseSensitivityLevel": 0,
"IsEditable": false, "Timestamp": "2012-06-20 18:44:55.000", "VersionNum": 1, "IsLightWeightPolicy": false } }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1108	Invalid policy Id

Create/Update Light Weight Policy

This URL creates/updates a light weight policy for a specific interface or sub interface.

Resource URL

POST /sensor/<sensor_id>/interface/<interface_id or subinterface_id>/localipspolicy

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes
`interface_id or subinterface_id`	Unique interface/sub interface id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`PolicyDescriptor`	Baseline IPS policy details	Object	Yes

Details of PolicyDescriptor:

Field Name	Description	Data Type	Mandatory
`PolicyName`	Baseline IPS policy name	String	Yes
`Description`	Policy description	String	Yes
`IsVisibleToChildren`	Is policy visible to child domain	Boolean	Yes
`InboundRuleSet`	Inbound policy rule set	String	Yes
`OutboundRuleSet`	Outbound policy rule set	String	Yes
`AttackCategory`	Attack category	Object	Yes
`OutboundAttackCategory`	Outbound attack category	Object	Yes
`DosPolicy`	DOS policy	Object	Yes
`ReconPolicy`	Recon policy	Object	Yes

Field Name	Description	Data Type	Mandatory
`DosResponseSensitivityLevel`	DoS response sensitivity level	Number	Yes
`IsEditable`	Is policy editable	Boolean	Yes
`Timestamp`	Time stamp at which the policy was added	String	Yes
`VersionNum`	Policy version number	Number	Yes
`IsLightWeightPolicy`	Is light weight policy configured	Boolean	Yes

Details of object in AttackCategory:

Field Name	Description	Data Type	Mandatory
`ExpolitAttackList`	List of exploit attacks	Array	Yes

Details of object in ExpolitAttackList:

Field Name	Description	Data Type	Mandatory
`attackName`	Attack name	String	Yes
`nspId`	NSP ID of the attack	String	Yes
`severity`	Attack severity, number between 0 & 9	Number	Yes
`isSeverityCustomized`	Is attack severity customized	Boolean	Yes
`isEnabled`	Is attack enabled	Boolean	Yes
`isAlertCustomized`	Is alert customized	Boolean	Yes
`isRecommendedForSmartBlocking`	Is attack recommended for smart blocking	Boolean	Yes
`AttackResponse`	Attack response	Object	Yes
`notification`	Notifications configured	Object	Yes
`protocolList`	List of protocols	Array	Yes
`applicationsImpactedList`	List of applications impacted	Array	Yes
`attackVector`	List of attack vectors	Array	Yes
`benignTriggerProbability`	Attack benign trigger probability	String	Yes
`target`	Attack target, can be "Server" or "Client"	String	Yes

Field Name	Description	Data Type	Mandatory
blockingType	Blocking type, can be "Attack Packet"	String	Yes
subCategory	Attack sub category	String	Yes
direction	Attack direction, can be "INBOUND" / "OUTBOUND" / "BOTH"	String	Yes
isAttackCustomized	Is attack customized	Boolean	Yes

Details of object in AttackResponse:

Field Name	Description	Data Type	Mandatory
TCPReset	TCP reset option, can be “DISABLED” / “SOURCE” / “DESTINATION” / “BOTH”	String	Yes
isTCPResetCustomized	Is TCP reset customized	Boolean	Yes
isICMPSend	Send ICMP host unreachable to Source	Boolean	Yes
isICMPSendCustomized	Send ICMP host unreachable to Source customized	Boolean	Yes
mcafeeNACNotification	NAC notification configured, can be “DISABLED” / “ALL_HOSTS” / “MCAFEE_NAC_UNMANAGED_HOSTS”	String	Yes
isMcafeeNACNotificationEnabled	Is NAC notification enabled	Boolean	Yes
isQuarantineCustomized	Is quarantine customized	Boolean	Yes
isRemediateEnabled	is remediate enabled	Boolean	Yes
blockingOption	Blocking option configured, can be “DISABLE” / “ENABLE” / “ENABLE_SMART_BLOCKING”	String	Yes
isBlockingOptionCustomized	Is blocking option customized	Boolean	Yes
isCapturedPrior	Should application data be captured prior to attack	Boolean	Yes

Field Name	Description	Data Type	Mandatory
isCapturedPriorCustomized	Should application data be captured prior to attack customized	Boolean	Yes
action	Action to be taken on attack, can be "DO_NOTHING" / "SEND_ALERT_AND_LOG_PACKETS" / "SEND_ALERT_ONLY"	String	Yes
isLogCustomized	Is logging customized	Boolean	Yes
flow	Customixe flow, can be "SINGLE_FLOW" / "FORENSIC_ANALYSIS"	String	Yes
isFlowCustomized	Customize flow type	Boolean	Yes
isNbytesCustomized	is logging N bytes in each packet customized	Boolean	Yes
numberOfBytesInEachPacket	Number of bytes to be logged in each packet	Object	Yes
loggingDuration	Packet logging duration	Object	Yes
TimeStamp	Time stamp	String	Yes

Details of object in numberOfBytesInEachPacket (Can be either of the below mentioned):

Field Name	Description	Data Type	Mandatory
LogEntirePacket	Log entire packet	Object	Yes
CaptureNBytes	Capture N bytes	Object	Yes

Details of object in CaptureNBytes:

Field Name	Description	Data Type	Mandatory
NumberOfBytes	Number of bytes to log	Number	Yes

Details of object in loggingDuration (Can be either of the below mentioned):

Field Name	Description	Data Type	Mandatory
AttackPacketOnly	Log attack packet only	Object	Yes
CaptureNPackets	Capture N packets	Object	Yes
CaptureTimeDuration	Capture for a time duration	Object	Yes
RestOfFlow	Capture rest of flow	Object	Yes

Details of object in CaptureNPackets:

Field Name	Description	Data Type	Mandatory
npackets	Log n packets	Number	Yes

Details of object in CaptureTimeDuration:

Field Name	Description	Data Type	Mandatory
time	Capture time	String	Yes
timeUnit	Time unit, can be "SECONDS" / "MINUTES" / "HOURS" / "DAYS"	String	Yes

Details of object in notification:

Field Name	Description	Data Type	Mandatory
isEmail	Is notification configured through email	Boolean	Yes
isPager	Is notification configured through pager	Boolean	Yes
isScript	Is notification configured through script	Boolean	Yes
isAutoAck	Is notification configured through auto ack	Boolean	Yes
isSnmp	Is notification configured through Snmp	Boolean	Yes
isSyslog	Is notification configured through Syslog	Boolean	Yes
isEmailCustomized	Is notification through Email customized	Boolean	Yes
isPagerCustomized	Is notification through Pager customized	Boolean	Yes
isScriptCustomized	Is notification through Script customized	Boolean	Yes
isAutoAckCustomized	Is notification through Auto Ack customized	Boolean	Yes
isSnmpCustomized	Is notification through Snmp customized	Boolean	Yes
isSyslogCustomized	Is notification through Syslog customized	Boolean	Yes

Details of object in DosPolicy:

Field Name	Description	Data Type	Mandatory
`LearningAttack`	List of learning attacks	Array	Yes
`ThresholdAttack`	List of threshold attacks	Array	Yes
`TimeStamp`	Time stamp	String	Yes

Details of object in LearningAttack:

Field Name	Description	Data Type	Mandatory
`attackName`	Attack name	String	Yes
`nspId`	NSP id of the attack	String	Yes
`isSeverityCustomized`	Is attack severity customized	Boolean	Yes
`severity`	Attack severity, number between 0 & 9	Number	Yes
`isBlockingSettingCustomized`	Is blocking customized	Boolean	Yes
`isDropPacket`	Drop DoS attack packets of this attack type when detected	Boolean	Yes
`isAlertCustomized`	Is alert customized	Boolean	Yes
`isSendAlertToManager`	Is alert notification to be sent to Manager configured	String	Yes
`timeStamp`	Time stamp	String	Yes
`direction`	Attack direction, can be "INBOUND" / "OUTBOUND" / "BOTH"	String	Yes
`notification`	Notification to be sent	Object	Yes
`isAttackCustomized`	Is DoS learning attack customized	Boolean	Yes

Details of object in ThresholdAttack:

Field Name	Description	Data Type	Mandatory
`attackName`	Attack name	String	Yes
`nspId`	NSP id of the attack	String	Yes
`isSeverityCustomized`	Is attack severity customized	Boolean	Yes

Field Name	Description	Data Type	Mandatory
severity	Attack severity, number between 0 & 9	Number	Yes
isThresholdValueCustomized	Is threshold value customized	Boolean	Yes
isThresholdDurationCustomized	is threshold duration customized	Boolean	Yes
ThresholdValue	Threshold values	Number	Yes
ThresholdDuration	Threshold interval (Seconds)	Number	Yes
isAlertCustomized	Is alert customized	Boolean	Yes
isSendAlertToManager	Is alert notification to be sent to Manager configured	String	Yes
TimeStamp	Time stamp	String	Yes
Notification	Notification to be sent via	Object	Yes
direction	Attack direction, can be "INBOUND" / "OUTBOUND" / "BOTH"	String	Yes
isAttackCustomized	Is DoS threshold attack customized	Boolean	Yes

Details of object in ReconPolicy:

Field Name	Description	Data Type	Mandatory
ReconAttackList	List of recon attacks	Array	Yes
TimeStamp	Time stamp	String	Yes
attackName	Attack name	String	yes
nspId	NSP id of the attack	String	Yes
isSeverityCustomized	Is attack severity customized	Boolean	Yes
severity	Severity, number between 0 & 9	Number	Yes
isThresholdValueCustomized	Is threshold value customized	Boolean	Yes
Is Threshold valuecustomized	is threshold duration customized	Boolean	Yes
ThresholdValue	Threshold values	Number	Yes

Field Name	Description	Data Type	Mandatory
`ThresholdDuration`	Threshold interval (seconds)	Number	Yes
`mcAfeeNACNotification`	Configured NAC notification that can be "DISABLED" / "ALL_HOSTS" / "MCAFEE_NAC_UNMANAGED_HOSTS"	String	Yes
`isMcAfeeNACNotificationEnable`	Is NAC notification enabled	Boolean	Yes
`isQuarantineCustomized`	Is quarantine customized	Boolean	Yes
`isRemediateEnabled`	is remediate enabled	Boolean	Yes
`isAlertSuppressionTimerCustom`	Is alert suppression customized	Boolean	Yes
`alertSuppressionTimer`	Alert suppression timer	Number	Yes
`IsAlertCustomized`	Is alert customized	Boolean	Yes
`isSendAlertToManager`	Is alert notification to be sent to Manager configured	String	Yes
`timestamp`	Time stamp	String	Yes
`direction`	Attack direction that can be "INBOUND" / "OUTBOUND" / "BOTH"	String	Yes
`notification`	Notification to be sent via	Object	Yes
`isAttackCustomized`	Is recon attack customized	Boolean	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique id of the light weight policy	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/sensor/1001/interface/105/localipspolicy

Payload:

```
{ "PolicyDescriptor": { "IsVisibleToChildren": true, "InboundRuleSet": "testRuleSet", "OutboundRuleSet": "Null",
"AttackCategory": { "ExpolitAttackList": [ { "attackName": "IDENT: TinyIdentD Identification Protocol Request
Handling Remote Stack Overflow", "nspId": "0x42700e00", "severity": 6, "isSeverityCustomized": true,
"isEnabled": true, "isAlertCustomized": false, "isRecommendedForSmartBlocking": false, "AttackResponse":
{ "TCPReset": "DISABLED", "isTcpResetCustomized": false, "isICMPSend": false, "isICMPSendCustomized": false,
"mcAfeeNACNotification": "DISABLED", "isMcAfeeNACNotificationEnabled": false, "isQuarantineCustomized": false,
"isRemediateEnabled": false, "blockingOption": "DISABLE", "isBlockingOptionCustomized": false,
"isCapturedPrior": true, "isCapturedPriorCustomized": false, "action": "SEND_ALERT_ONLY", "isLogCustomized":
false, "isFlowCustomized": false, "isNbytesCustomized": false, "numberOfBytesInEachPacket": { "LogEntirePacket":
{ } } }, "notification": { "isEmail": false, "isPager": false, "isScript": false, "isAutoAck": false, "isSnmp":
false, "isSyslog": false, "isEmailCustomized": false, "isPagerCustomized": false, "isScriptCustomized": false,
"isAutoAckCustomized": false, "isSnmpCustomized": false, "isSyslogCustomized": false }, "protocolList":
[ "ident" ], "benignTriggerProbability": "3 (Medium)", "blockingType": "attack-packet", "subCategory": "buffer-
overflow", "direction": "INBOUND", "isAttackCustomized": true } ] }, "OutboundAttackCategory": { }, "DosPolicy":
{ "LearningAttack": [ { "attackName": "Outbound ICMP Echo Request or Reply Volume Too High", "nspId":
"0x40018000", "isSeverityCustomized": false, "severity": 7, "isBlockingSettingCustomized": false,
"isDropPacket": false, "IsAlertCustomized": false, "isSendAlertToManager": true, "direction": "OUTBOUND",
"notification": { "isEmail": false, "isPager": false, "isScript": false, "isAutoAck": false, "isSnmp": false,
"isSyslog": false, "isEmailCustomized": false, "isPagerCustomized": false, "isScriptCustomized": false,
"isAutoAckCustomized": false, "isSnmpCustomized": false, "isSyslogCustomized": false }, "isAttackCustomized":
false } ], "ThresholdAttack": [ { "attackName": "Too Many Outbound IP Fragments", "nspId": "0x40018800",
"isSeverityCustomized": false, "severity": 6, "isThresholdValueCustomized": false,
"isThresholdDurationCustomized": false, "ThresholdValue": 1000, "ThresholdDuration": 5, "isAlertCustomized":
false, "isSendAlertToManager": false, "Notification": { "isEmail": false, "isPager": false, "isScript": false,
"isAutoAck": false, "isSnmp": false, "isSyslog": false, "isEmailCustomized": false, "isPagerCustomized": false,
"isScriptCustomized": false, "isAutoAckCustomized": false, "isSnmpCustomized": false, "isSyslogCustomized":
false }, "direction": "OUTBOUND", "isAttackCustomized": false } ], "TimeStamp": "2012-08-31 15:20:54.000" },
'ReconPolicy': { 'TimeStamp': None, 'ReconAttackList': [{ 'IsAlertCustomized': False, 'isSeverityCustomized':
False, 'direction': None, 'severity': 5, 'isThresholdDurationCustomized': False, 'isSendAlertToManager': False,
'isQuarantineCustomized': False, 'attackName': 'BOTHeuristic: PotentialBotActivity-
MultipleResetsfromSMTPreceiver', 'ThresholdDuration': 0, 'alertSuppressionTimer': 0,
'isAlertSuppressionTimerCustomized': False, 'isAttackCustomized': False, 'isMcAfeeNACNotificationEnabled':
False, 'isThresholdValueCustomized': False, 'nspId': '0x43f00900', 'mcAfeeNACNotification': 'DISABLED',
'isRemediateEnabled': False, 'timeStamp': None, 'ThresholdValue': 0, 'notification': { 'isSnmp': False,
'isAutoAckCustomized': False, 'isPagerCustomized': False, 'isSyslogCustomized': False, 'isEmail': False,
'isSyslog': False, 'isScriptCustomized': False, 'isSnmpCustomized': False, 'isScript': False, 'isPager': False,
'isEmailCustomized': False, 'isAutoAck': False } }] }, "DosResponseSensitivityLevel": 0, "IsEditable": false,
"Timestamp": "2012-08-31 15:20:55.000", "VersionNum": 1, "IsLightWeightPolicy": true } }
```

Response

```
{ "createdResourceId":105 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	404	1107	Invalid interface or sub-interface id
3	400	1301	The number of attacks does not match the number in the baseline policy
4	400	1302	Number of bytes has to be between 1 to 255
5	400	1303	Please provide the number of bytes to be logged
6	400	1304	Please provide duration of logging for flow
7	400	1305	Number of bytes has to be between 2 to 255
8	400	1306	Time has to be between 1 to 63
9	400	1307	Please provide a time
10	400	1308	Please provide a time interval
11	400	1309	Please provide the flow

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
12	400	1310	Invalid severity - please provide a value between 0 and 10
13	400	1311	Invalid threshold value - please enter a value between 1 and 2147483647
14	400	1312	Invalid threshold duration - please enter a value between 1 and 2147483647

Get Light Weight Policy details

This URL gets the details of a light weight policy associated with a specific interface or sub interface.

Resource URL

GET /sensor/<sensor_id>/interface/<interface_id or subinterface_id>/localipspolicy

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes
`interface_id or subinterface_id`	Unique interface or subInterface id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`PolicyDescriptor`	Baseline IPS policy details	Object

Details of PolicyDescriptor:

Field Name	Description	Data Type
`PolicyName`	Baseline IPS policy name	String
`Description`	Policy description	String
`IsVisibleToChildren`	Is policy visible to child domain	Boolean
`InboundRuleSet`	Inbound policy rule set	String
`OutboundRuleSet`	Outbound policy rule set	String
`AttackCategory`	Attack category	Object

Field Name	Description	Data Type
OutboundAttackCategory	Outbound attack category	Object
DosPolicy	DOS policy	Object
ReconPolicy	Recon policy	Object
DosResponseSensitivityLevel	Dos response sensitivity level	Number
IsEditable	Is policy editable	Boolean
Timestamp	Time stamp at which the policy was added	String
VersionNum	Policy version number	Number
IsLightWeightPolicy	Is light weight policy configured	Boolean

Details of object in AttackCategory:

Field Name	Description	Data Type
ExpolitAttackList	List of exploit attacks	Array

Details of object in ExpolitAttackList:

Field Name	Description	Data Type
attackName	Attack name	String
nspId	NSP id of the attack	String
severity	Attack severity, number between 0 & 9	Number
isSeverityCustomized	Is attack severity customized	Boolean
isEnabled	Is attack enabled	Boolean
isAlertCustomized	Is alert customized	Boolean
isRecommendedForSmartBlocking	Is attack recommended for smart blocking	Boolean
AttackResponse	Attack response	Object
notification	Notifications configured	Object
protocolList	List of protocols	Array
applicationsImpactedList	List of applications impacted	Array
attackVector	List of attack vectors	Array
benignTriggerProbability	Attack benign trigger probability	String
target	Attack target, can be "Server" or "Client"	String
blockingType	Blocking type, can be "Attack Packet"	String

Field Name	Description	Data Type
`subCategory`	Attack sub category	String
`direction`	Attack direction, can be "INBOUND" / "OUTBOUND" / "BOTH"	String
`isAttackCustomized`	Is attack customized	Boolean

Details of object in AttackResponse:

Field Name	Description	Data Type
`TCPReset`	TCP reset option, can be “DISABLED” / “SOURCE” / “DESTINATION” / “BOTH”	String
`isTCPResetCustomized`	Is TCP reset customized	Boolean
`isICMPSend`	Send ICMP host unreachable to source	Boolean
`isICMPSendCustomized`	Send ICMP host unreachable to source customized	Boolean
`mcafeeNACNotification`	NAC notification configured, can be “DISABLED” / “ALL_HOSTS” / “MCAFEE_NAC_UNMANAGED_HOSTS”	String
`isMcafeeNACNotificationEnabled`	Is NAC notification enabled	Boolean
`isQuarantineCustomized`	Is quarantine customized	Boolean
`isRemediateEnabled`	is remediate enabled	Boolean
`blockingOption`	Blocking option configured, can be “DISABLE” / “ENABLE” / “ENABLE_SMART_BLOCKING”	String
`isBlockingOptionCustomized`	Is blocking option customized	Boolean
`isCapturedPrior`	Should application data be captured prior to attack	Boolean
`isCapturedPriorCustomized`	Should application data be captured prior to attack customized	Boolean
`action`	Action to be taken on attack, can be “DO_NOTHING” / “SEND_ALERT_AND_LOG_PACKETS” / “SEND_ALERT_ONLY”	String
`isLogCustomized`	Is logging customized	Boolean
`flow`	Customixe flow, can be “SINGLE_FLOW” / “FORENSIC_ANALYSIS”	String
`isFlowCustomized`	Customize flow type	Boolean
`isNbytesCustomized`	is logging N bytes in each packet customized	Boolean

Field Name	Description	Data Type
`numberOfBytesInEachPacket`	Number of bytes to be logged in each packet	Object
`loggingDuration`	Packet logging duration	Object
`TimeStamp`	Timestamp	String

Details of object in numberOfBytesInEachPacket (Can be either of the below mentioned):

Field Name	Description	Data Type
`LogEntirePacket`	Log entire packet	Object
`CaptureNBytes`	Capture N bytes	Object

Details of object in CaptureNBytes:

Field Name	Description	Data Type
`NumberOfBytes`	Number of bytes to log	Number

Details of object in loggingDuration (Can be either of the below mentioned):

Field Name	Description	Data Type
`AttackPacketOnly`	Log attack packet only	Object
`CaptureNPackets`	Capture N packets	Object
`CaptureTimeDuration`	Capture for a time duration	Object
`RestOfFlow`	Capture rest of flow	Object

Details of object in CaptureNPackets:

Field Name	Description	Data Type
`npackets`	Log n packets	number

Details of object in CaptureTimeDuration:

Field Name	Description	Data Type
`time`	Capture time	String
`timeUnit`	Time unit, can be "SECONDS" / "MINUTES" / "HOURS" / "DAYS"	String

Details of object in notification:

Field Name	Description	Data Type
`isEmail`	Is Notification configured through email	Boolean

Field Name	Description	Data Type
isPager	Is Notification configured through pager	Boolean
isScript	Is Notification configured through script	Boolean
isAutoAck	Is Notification configured through auto ack	Boolean
isSnmp	Is Notification configured through snmp	Boolean
isSyslog	Is Notification configured through syslog	Boolean
isEmailCustomized	Is Notification through email customized	Boolean
isPagerCustomized	Is Notification through pager customized	Boolean
isScriptCustomized	Is Notification through script customized	Boolean
isAutoAckCustomized	Is Notification through auto ack customized	Boolean
isSnmpCustomized	Is Notification through snmp customized	Boolean
isSyslogCustomized	Is Notification through syslog customized	Boolean

Details of object in DosPolicy:

Field Name	Description	Data Type
LearningAttack	List of learning attacks	Array
ThresholdAttack	List of threshold attacks	Array
TimeStamp	Time stamp	String

Details of object in LearningAttack:

Field Name	Description	Data Type
attackName	Attack name	String
nspId	NSP id of the attack	String
isSeverityCustomized	Is attack severity customized	Boolean
severity	Attack severity, number between 0 & 9	Number
isBlockingSettingCustomized	Is blocking customized	Boolean
isDropPacket	Drop DoS attack packets of this attack type when detected	Boolean
isAlertCustomized	Is alert customized	Boolean
isSendAlertToManager	Is alert notification to be sent to the Manager configured	String
timeStamp	Time stamp	String

Field Name	Description	Data Type
`direction`	Attack direction, can be "INBOUND" / "OUTBOUND" / "BOTH"	String
`notification`	Notification to be sent via	Object
`isAttackCustomized`	Is DoS learning attack customized	Boolean

Details of object in ThresholdAttack:

Field Name	Description	Data Type
`attackName`	Attack name	String
`nspId`	NSP id of the attack	String
`isSeverityCustomized`	Is attack severity customized	Boolean
`severity`	Attack severity, number between 0 & 9	Number
`isThresholdValueCustomized`	Is threshold value customized	Boolean
`isThresholdDurationCustomized`	is threshold duration customized	Boolean
`ThresholdValue`	Threshold values	Number
`ThresholdDuration`	Threshold Interval (Seconds)	Number
`isAlertCustomized`	Is alert customized	Boolean
`isSendAlertToManager`	Is alert notification to be sent to Manager configured	String
`TimeStamp`	Time stamp	String
`Notification`	Notification to be sent	Object
`direction`	Attack direction, can be "INBOUND" / "OUTBOUND" / "BOTH"	String
`isAttackCustomized`	Is DoS threshold attack customized	Boolean

Details of object in ReconPolicy:

Field Name	Description	Data Type	Mandatory
`ReconAttackList`	List of recon attacks	Array	Yes
`TimeStamp`	Time stamp	String	Yes
`attackName`	Attack name	String	yes
`nspId`	NSP id of the attack	String	Yes

Field Name	Description	Data Type	Mandatory
`isSeverityCustomized`	Is attack severity customized	Boolean	Yes
`severity`	Severity, number between 0 & 9	Number	Yes
`isThresholdValueCustomized`	Is threshold value customized	Boolean	Yes
`Is Threshold valuecustomized`	is threshold duration customized	Boolean	Yes
`ThresholdValue`	Threshold values	Number	Yes
`ThresholdDuration`	Threshold Interval (seconds)	Number	Yes
`mcAfeeNACNotification`	Configured NAC notification that can be "DISABLED" / "ALL_HOSTS" / "MCAFEE_NAC_UNMANAGED_HOSTS"	String	Yes
`isMcAfeeNACNotificationEnable`	Is NAC notification enabled	Boolean	Yes
`isQuarantineCustomized`	Is quarantine customized	Boolean	Yes
`isRemediateEnabled`	is remediate enabled	Boolean	Yes
`isAlertSuppressionTimerCustom`	Is alert suppression customized	Boolean	Yes
`alertSuppressionTimer`	Alert suppression timer	Number	Yes
`IsAlertCustomized`	Is alert customized	Boolean	Yes
`isSendAlertToManager`	Is alert notification to be sent to Manager configured	String	Yes
`timestamp`	Time stamp	String	Yes
`direction`	Attack direction that can be "INBOUND" / "OUTBOUND" / "BOTH"	String	Yes
`notification`	Notification to be sent via	Object	Yes
`isAttackCustomized`	Is recon attack customized	Boolean	Yes

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/sensor/1001/interface/105/localipspolicy

Response

```
{ "PolicyDescriptor": { "PolicyName": "Local Policy - /My Company/M-2950/1A-1B clone", "Description": "To test
the policies", "IsVisibleToChildren": true, "InboundRuleSet": "testRuleSet", "OutboundRuleSet": "Null",
"AttackCategory": { "ExpolitAttackList": [ { "attackName": "IDENT: TinyIdentD Identification Protocol Request
Handling Remote Stack Overflow", "nspId": "0x42700e00", "severity": 6, "isSeverityCustomized": true,
"isEnabled": true, "isAlertCustomized": false, "isRecommendedForSmartBlocking": false, "AttackResponse":
{ "TCPReset": "DISABLED", "isTcpResetCustomized": false, "isICMPSend": false, "isICMPSendCustomized": false,
"mcAfeeNACNotification": "DISABLED", "isMcAfeeNACNotificationEnabled": false, "isQuarantineCustomized": false,
"isRemediateEnabled": false, "blockingOption": "DISABLE", "isBlockingOptionCustomized": false,
"isCapturedPrior": true, "isCapturedPriorCustomized": false, "action": "SEND_ALERT_ONLY", "isLogCustomized":
false, "isFlowCustomized": false, "isNbytesCustomized": false, "numberOfBytesInEachPacket": { "LogEntirePacket":
{ } } }, "notification": { "isEmail": false, "isPager": false, "isScript": false, "isAutoAck": false, "isSnmp":
false, "isSyslog": false, "isEmailCustomized": false, "isPagerCustomized": false, "isScriptCustomized": false,
"isAutoAckCustomized": false, "isSnmpCustomized": false, "isSyslogCustomized": false }, "protocolList":
[ "ident" ], "benignTriggerProbability": "3 (Medium)", "blockingType": "attack-packet", "subCategory": "buffer-
overflow", "direction": "INBOUND", "isAttackCustomized": true } ] }, "OutboundAttackCategory": { }, "DosPolicy":
{ "LearningAttack": [ { "attackName": "Outbound ICMP Echo Request or Reply Volume Too High", "nspId":
"0x40018000", "isSeverityCustomized": false, "severity": 7, "isBlockingSettingCustomized": false,
"isDropPacket": false, "IsAlertCustomized": false, "isSendAlertToManager": true, "direction": "OUTBOUND",
"notification": { "isEmail": false, "isPager": false, "isScript": false, "isAutoAck": false, "isSnmp": false,
"isSyslog": false, "isEmailCustomized": false, "isPagerCustomized": false, "isScriptCustomized": false,
"isAutoAckCustomized": false, "isSnmpCustomized": false, "isSyslogCustomized": false }, "isAttackCustomized":
false } ], "ThresholdAttack": [ { "attackName": "Too Many Outbound IP Fragments", "nspId": "0x40018800",
"isSeverityCustomized": false, "severity": 6, "isThresholdValueCustomized": false,
"isThresholdDurationCustomized": false, "ThresholdValue": 1000, "ThresholdDuration": 5, "isAlertCustomized":
false, "isSendAlertToManager": false, "Notification": { "isEmail": false, "isPager": false, "isScript": false,
"isAutoAck": false, "isSnmp": false, "isSyslog": false, "isEmailCustomized": false, "isPagerCustomized": false,
"isScriptCustomized": false, "isAutoAckCustomized": false, "isSnmpCustomized": false, "isSyslogCustomized":
false }, "direction": "OUTBOUND", "isAttackCustomized": false } ], "TimeStamp": "2012-08-31 15:20:54.000" },
'ReconPolicy': { 'TimeStamp': None, 'ReconAttackList': [{ 'IsAlertCustomized': False, 'isSeverityCustomized':
False, 'direction': None, 'severity': 5, 'isThresholdDurationCustomized': False, 'isSendAlertToManager': False,
'isQuarantineCustomized': False, 'attackName': 'BOTHeuristic: PotentialBotActivity-
MultipleResetsfromSMTPreceiver', 'ThresholdDuration': 0, 'alertSuppressionTimer': 0,
'isAlertSuppressionTimerCustomized': False, 'isAttackCustomized': False, 'isMcAfeeNACNotificationEnabled':
False, 'isThresholdValueCustomized': False, 'nspId': '0x43f00900', 'mcAfeeNACNotification': 'DISABLED',
'isRemediateEnabled': False, 'timeStamp': None, 'ThresholdValue': 0, 'notification': { 'isSnmp': False,
'isAutoAckCustomized': False, 'isPagerCustomized': False, 'isSyslogCustomized': False, 'isEmail': False,
'isSyslog': False, 'isScriptCustomized': False, 'isSnmpCustomized': False, 'isScript': False, 'isPager': False,
'isEmailCustomized': False, 'isAutoAck': False } }] }, "DosResponseSensitivityLevel": 0, "IsEditable": false,
"Timestamp": "2012-08-31 15:20:55.000", "VersionNum": 1, "IsLightWeightPolicy": true } }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	404	1107	Invalid interface or sub-interface id
3	400	1301	The number of attacks does not match the number in the baseline policy
4	400	1302	Number of bytes has to be between 1 to 255
5	400	1303	Please provide the number of bytes to be logged
6	400	1304	Please provide duration of logging for flow
7	400	1305	Number of bytes has to be between 2 to 255
8	400	1306	Time has to be between 1 to 63
9	400	1307	Please provide a time

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
10	400	1308	Please provide a time interval
11	400	1309	Please provide the flow
12	400	1310	Invalid severity - please provide a value between 0 and 10
13	400	1311	Invalid threshold value - please enter a value between 1 and 2147483647
14	400	1312	Invalid threshold duration - please enter a value between 1 and 2147483647
15	400	1311	Alert suppression timer should be between 1 and 65535

Delete Light Weight Policy

This URL deletes a L\light weight policy associated with a specific interface or sub interface.

Resource URL

DELETE /sensor/<sensor_id>/interface/<interface_id or subinterface_id>/localipspolicy

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes
`interface_id or subinterface_id`	Unique interface or sub interface id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status returned by deletion	Number

Example

Request

DELETE https://%3CNSM_IP%3E/sdkapi/sensor/1001/interface/105/localipspolicy

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	404	1107	Invalid interface or sub-interface id
3	400	1301	The number of attacks does not match the number in the baseline policy
4	400	1302	Number of bytes has to be between 1 to 255
5	400	1303	Please provide the number of bytes to be logged
6	400	1304	Please provide duration of logging for flow
7	400	1305	Number of bytes has to be between 2 to 255
8	400	1306	Time has to be between 1 to 63
9	400	1307	Please provide a time
10	400	1308	Please provide a time interval
11	400	1309	Please provide the flow
12	400	1310	Invalid severity - please provide a value between 0 and 10
13	400	1311	Invalid threshold value - please enter a value between 1 and 2147483647
14	400	1312	Invalid threshold duration - please enter a value between 1 and 2147483647

Create New IPS Policy

This URL creates new IPS policy.

Resource URL

POST /sdkapi/domain/<domainId>/ipspolicies/createips

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain ID	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`PolicyName`	Policy name	String	Yes
`Description`	Policy description	String	Yes
`IsVisibleToChildren`	Is policy visible to child domain	Boolean	Yes
`InboundRuleSet`	Rule set with inbound direction	Boolean	Yes
`OutboundRuleSet`	Rule set with outbound direction	Boolean	Yes
`DosResponseSensitivityLevel`	DOS response sensitivity level value can be: • 0 • 1	Number	Yes
`isEditable`	Is policy editable after creation	Boolean	No
`direction`	Consider inbound/outbound direction values can be: • 0 • 1	Number	Yes

Response Parameters

Following fields are returned if the operation was successful, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique id of the created policy	Number

Example

Request

POST https://<NSM_IP>/sdkapi/domain/<domainId>/ipspolicies/createips

Payload:

```
{ "PolicyName":"IPS policytest1", "Description":"test", "IsVisibleToChildren":true, "InboundRuleSet":"Default
Prevention", "OutboundRuleSet":"DMZ", "DosResponseSensitivityLevel":1, "direction":1 }
```

Response

```
{ createdResourceId :1 }
```

Error Information

Following error codes are returned by this URL:

S.No	SDK API errorId	SDK API errorMessage
1	1001	Unable to add a policy. A policy with same name could be existing in current or in a different admin domain.
2	1001	Unable to add a policy. Invalid sensitivity Level: 3.
3	9001	Enter valid direction code: 0:Ignore Direction, 1:Consider Direction.
4	9001	Rule set name not found.

Update IPS Policy

Resource URL

This URL updates IPS policy.

PUT /ipspolicy/<policyid>

URL Parameters:

Field Name	Description	Data Type	Mandatory
`policyId`	Policy id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`PolicyName`	Policy name	String	Yes (Custom policy) No (Default policy)
`Description`	Policy description	String	No
`IsVisibleToChildren`	Is policy visible to child domain	Boolean	No
`InboundRuleSet`	Rule set with inbound direction	String	Yes (Custom policy) No (Default policy)
`OutboundRuleSet`	Rule set with outbound direction	String	Yes (Custom policy) No (Default policy)
`ReconPolicy`	Reconnaissance policy attack list	Object	No
`AttackCategory`	Attack category	Object	No
`OutboundAttackCategory`	Outbound attack category	Object	Yes **Note:** The value can be empty if no update is required.

Field Name	Description	Data Type	Mandatory
			However, the key should be present in the payload.
DosPolicy	DOS policy	Object	No
DosResponseSensitivityLevel	DOS response sensitivity level value can be: • 0 • 1	Number	No
isEditable	Is policy editable after creation	Boolean	No
direction	Consider inbound/outbound direction values can be: • 0 • 1	Number	No

Details of object in AttackCategory:

Field Name	Description	Data Type	Mandatory
ExpolitAttackList	List of exploit attacks	Array	No

Details of object in ExpolitAttackList:

Field Name	Description	Data Type	Mandatory
nspId	Network Security Platform id of the attack	String	No
severity	Attack severity between 0 and 9	Number	No
isSeverityCustomized	Is attack severity customized	Boolean	No
isEnabled	Is attack enabled	Boolean	No
isAlertCustomized	Is alert customized	Boolean	No **Note:** isAlertCustomized should be set to **true** for changing the isEnabled field.
isRecommendedForSmartBlocking	Is attack recommended for smart blocking	Boolean	No
AttackResponse	Attack response	Object	No
notification	Notifications configured	Object	Yes **Note:** The value can be empty if no update is required. However, the key should be present in the payload.

Field Name	Description	Data Type	Mandatory
`protocolList`	List of protocols	Array	No
`benignTriggerProbability`	Attack benign trigger probability	String	No
`target`	Attack target, can be server or client	String	No
`blockingType`	Blocking type, can be attack packet	String	No
`subCategory`	Attack sub category	String	No
`direction`	Attack direction can be inbound, outbound, or both	String	No

Details of object in AttackResponse:

Field Name	Description	Data Type	Mandatory
`TCPReset`	TCP reset option, can be • Disabled source • Disabled destination • Both	String	No
`isTCPResetCustomized`	Is TCP reset customized	Boolean	No
`isICMPSend`	Send ICMP host unreachable to source	Boolean	No
`isICMPSendCustomized`	Send ICMP host unreachable to source customized	Boolean	No
`mcafeeNACNotification`	NAC notification configured, can be • Disabled • All hosts • McAfee NAC unmanaged hosts	String	No
`isMcafeeNACNotificationEnabled`	Is NAC notification enabled	Boolean	No
`isQuarantineCustomized`	Is quarantine customized	Boolean	No
`isRemediateEnabled`	Is remediate enabled	Boolean	No
`blockingOption`	Blocking option configured, can be • Disable • Enable • Enable smart blocking	String	No
`isBlockingOptionCustomized`	Is blocking option customized	Boolean	No

Field Name	Description	Data Type	Mandatory
isCapturedPrior	Should application data be captured before an attack	Boolean	No
isCapturedPriorCustomized	Should application data be captured before attack customized	Boolean	No
isAlert	If action is customized set it as true	Boolean	No
action	Action to be taken on attack, can be • Do nothing • Send alert and log packets • Send alert only	String	No
isLogCustomized	Is logging customized	Boolean	No
flow	Customize flow, can be • Single flow • Forensic analysis	String	No
isFlowCustomized	Customize flow type	Boolean	No
isNbytesCustomized	Is logging N number of bytes in each packet customized	Boolean	No
numberOfBytesInEachPacket	Number of bytes to be logged in each packet	Object	No
loggingDuration	Packet logging duration	Object	No

Details of object in numberOfBytesInEachPacket (Can be either of the below mentioned):

Field Name	Description	Data Type	Mandatory
LogEntirePacket	log entire packet	Object	No
CaptureNBytes	Capture N number of bytes	Object	No

Details of object in CaptureNBytes:

Field Name	Description	Data Type	Mandatory
NumberOfBytes	Number of bytes to log	Number	No

Details of object in loggingDuration (Can be either of the below mentioned):

Field Name	Description	Data Type	Mandatory
AttackPacketOnly	Log attack packet only	Object	No
CaptureNPackets	Capture N packets	Object	No
CaptureTimeDuration	Capture for a time duration	Object	No

Field Name	Description	Data Type	Mandatory
`RestOfFlow`	Capture rest of flow	Object	No

Details of object in CaptureNPackets:

Field Name	Description	Data Type	Mandatory
`npackets`	Log n packets	Number	No

Details of object in CaptureTimeDuration:

Field Name	Description	Data Type	Mandatory
`time`	Capture time	String	No
`timeUnit`	Time unit, can be • Seconds • Minutes • Hours • Days	String	No

Details of object in notification:

Field Name	Description	Data Type	Mandatory
`isEmail`	Is notification configured through email	Boolean	No
`isPager`	Is notification configured through pager	Boolean	No
`isScript`	Is notification configured through script	Boolean	No
`isAutoAck`	Is notification configured through auto acknowledge	Boolean	No
`isSnmp`	Is notification configured through snmp	Boolean	No
`isSyslog`	Is notification configured through syslog	Boolean	No
`isEmailCustomized`	Is notification through email customized	Boolean	No
`isPagerCustomized`	Is notification through pager customized	Boolean	No
`isScriptCustomized`	Is notification through script customized	Boolean	No
`isAutoAckCustomized`	Is notification through auto acknowledge customized	Boolean	No

Field Name	Description	Data Type	Mandatory
`isSnmpCustomized`	Is notification through snmp customized	Boolean	No
`isSyslogCustomized`	Is notification through syslog customized	Boolean	No

Details of object in DosPolicy:

Field Name	Description	Data Type	Mandatory
`LearningAttack`	List of learning attacks	Array	No
`ThresholdAttack`	List of threshold attacks	Array	No
`TimeStamp`	Time stamp	String	No

Details of object in LearningAttack:

Field Name	Description	Data Type	Mandatory
`attackName`	Attack name	String	No
`nspId`	Network Security Platform if of the attack	String	No
`isSeverityCustomized`	Is the attack severity customized	Boolean	No
`severity`	Attack severity between 0 and 9	Number	No
`isBlockingSettingCustomized`	Is blocking customized	Boolean	No
`isDropPacket`	Drop DOS attack packets of this attack type when detected	Boolean	No
`isAlertCustomized`	Is alert customized	Boolean	No
`isSendAlertToManager`	Is alert notification to be sent to the Manager configured	Boolean	No
`direction`	Attack direction can be: • Inbound • Outbound • Inbound and outbound	String	No
`notification`	Specifies the Manager's action for the attack.	Object	Yes **Note:** The value can be empty if no update is required. However, the key should be present in the payload.

Details of object in ThresholdAttack:

Field Name	Description	Data Type	Mandatory
`attackName`	Attack name	String	No
`nspId`	Network Security Platform if of the attack	String	No
`isSeverityCustomized`	Is the attack severity customized	Boolean	No
`severity`	Attack severity between 0 and 9	Number	No
`isThresholdValueCustomized`	Is threshold value customized	Boolean	No
`isThresholdDurationCustomized`	Is threshold duration customized	Boolean	No
`ThresholdValue`	Threshold value	Number	No
`ThresholdDuration`	Threshold interval (seconds)	Number	No
`isAlertCustomized`	Is alert customized	Boolean	No
`isSendAlertToManager`	Is alert notification to be sent to the Manager configured	Boolean	No
`notification`	Specifies the Manager's action for the attack.	Object	Yes **Note:** The value can be empty if no update is required. However, the key should be present in the payload.
`direction`	Attack direction can be: • Inbound • Outbound • Inbound and outbound	String	No

Details of object in ReconAttack List:

Field Name	Description	Data Type	Mandatory
`isAlertCustomized`	Is alert customized	Boolean	No
`nspId`	Network Security Platform if of the attack	String	No
`isSeverityCustomized`	Is the attack severity customized	Boolean	No
`severity`	Attack severity between 0 and 9	Number	No
`ThresholdValue`	Threshold value	Number	No
`isRemediateEnabled`	Is remediate enabled	Boolean	No

Field Name	Description	Data Type	Mandatory
`isAlertCustomized`	Is alert customized	Boolean	No
`isSendAlertToManager`	Is alert notification to be sent to the Manager configured	Boolean	No
`ThresholdDuration`	Threshold interval (seconds)	Number	No
`alertSuppressionTimer`	Alert suppression timer	Number	No
`isAlertSuppressionTimerCustomized`	Is alert suppression timer customized	Boolean	No
`isMcafeeNACNotificationEnabled`	Is NAC notification enabled	Boolean	No
`mcafeeNACNotification`	NAC notification configured, can be • Disabled • All hosts • McAfee NAC unmanaged hosts	String	No
`notification`	Specifies the Manager's action for the attack.	Object	Yes **Note:** The value can be empty if no update is required. However, the key should be present in the payload.
`isQuarantineCustomized`	Is quarantine customized	Boolean	No
`isThresholdDurationCustomized`	Is threshold duration customized	Boolean	No

Response Parameters

Following fields are returned if the operation was successful, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status of the request	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/ipspolicy/<policyid>

Payload:

```
{ "DosResponseSensitivityLevel": 1, "direction": 1, "Description": "Updated policy", "IsEditable": true,
"PolicyName": "ipstest", "ReconPolicy": { "ReconAttackList": [ { "IsAlertCustomized": true,
"isQuarantineCustomized": true, "severity": 6, "isThresholdDurationCustomized": true, "isSendAlertToManager":
true, "nspId": "0x43f00900", "ThresholdDuration": 5, "alertSuppressionTimer": 5,
"isAlertSuppressionTimerCustomized": true, "isMcAfeeNACNotificationEnabled": true, "ThresholdValue": 200,
"notification": { "isAutoAckCustomized": true, "isPager": true, "isSyslogCustomized": true, "isPagerCustomized":
true, "isEmail": true, "isScriptCustomized": true, "isSnmpCustomized": true, "isScript": true, "isSnmp": true,
"isEmailCustomized": true, "isAutoAck": true, "isSyslog": true }, "mcAfeeNACNotification": "ALL_HOSTS",
"isRemediateEnabled": true, "isSeverityCustomized": true, "isThresholdValueCustomized": true } ] }, "DosPolicy":
{ "LearningAttack": [ { "IsAlertCustomized": true, "direction": "INBOUND", "severity": 7, "isDropPacket": false,
"isSendAlertToManager": true, "nspId": "0x4000b600", "isBlockingSettingCustomized": true, "attackName": "Inbound
IP Fragment Volume Too High", "isSeverityCustomized": true, "notification": { "isAutoAckCustomized": true,
"isPager": true, "isSyslogCustomized": true, "isPagerCustomized": true, "isEmail": true, "isScriptCustomized":
true, "isSnmpCustomized": true, "isScript": true, "isSnmp": true, "isEmailCustomized": true, "isAutoAck": true,
"isSyslog": true } } ], "ThresholdAttack": [ { "isAlertCustomized": true, "direction": "INBOUND", "severity": 6,
"isThresholdDurationCustomized": true, "isSendAlertToManager": true, "nspId": "0x40018300", "ThresholdDuration":
5, "isSeverityCustomized": true, "Notification": { "isAutoAckCustomized": true, "isPager": true,
"isSyslogCustomized": true, "isPagerCustomized": true, "isEmail": true, "isScriptCustomized": true,
"isSnmpCustomized": true, "isScript": true, "isSnmp": true, "isEmailCustomized": true, "isAutoAck": true,
"isSyslog": true }, "attackName": "Too Many Outbound ICMP Packets", "ThresholdValue": 200,
"isThresholdValueCustomized": true } ] }, "IsVisibleToChildren": true, "OutboundAttackCategory":
{ "ExpolitAttackList": [ { "isAlertCustomized": true, "blockingType": "attack-packet", "direction": "OUTBOUND",
"severity": 5, "AttackResponse": { "isFlowCustomized": true, "isICMPSend": true, "blockingOption": "DISABLE",
"mcAfeeNACNotification": "DISABLED", "isAlertCustomized": true, "isCapturedPrior": true,
"numberOfBytesInEachPacket": { "CaptureNBytes": { "NumberOfBytes": 5 }, "LogEntirePacket": {} },
"isICMPSendCustomized": true, "isCapturedPriorCustomized": true, "TimeStamp": "None", "isQuarantineCustomized":
true, "TCPReset": "BOTH", "isLogCustomized": true, "isTcpResetCustomized": true, "isNbytesCustomized": true,
"flow": "SINGLE_FLOW", "isMcAfeeNACNotificationEnabled": false, "isAlert": true, "action":
"SEND_ALERT_AND_LOG_PACKETS", "loggingDuration": { "CaptureNPackets": { "npackets": 5 }, "AttackPacketOnly": {},
"RestOfFlow": null, "CaptureTimeDuration": { "timeUnit": "SECONDS", "time": "10" } }, "isRemediateEnabled":
true, "isBlockingOptionCustomized": true }, "nspId": "0x40254c00", "isEnabled": true,
"benignTriggerProbability": "1 (Low)", "notification": { "isAutoAckCustomized": true, "isPager": true,
"isSyslogCustomized": true, "isPagerCustomized": true, "isEmail": true, "isScriptCustomized": true,
"isSnmpCustomized": true, "isScript": true, "isSnmp": true, "isEmailCustomized": true, "isAutoAck": true,
"isSyslog": true }, "isRecommendedForSmartBlocking": true, "isSeverityCustomized": true, "subCategory":
"dos" } ] }, "AttackCategory": { "ExpolitAttackList": [ { "isAlertCustomized": true, "blockingType": "attack-
packet", "direction": "INBOUND", "severity": 5, "AttackResponse": { "isFlowCustomized": true, "isICMPSend":
true, "blockingOption": "DISABLE", "mcAfeeNACNotification": "DISABLED", "isAlertCustomized": true,
"isCapturedPrior": true, "numberOfBytesInEachPacket": { "CaptureNBytes": { "NumberOfBytes": 5 },
"LogEntirePacket": {} }, "isICMPSendCustomized": true, "isCapturedPriorCustomized": true, "TimeStamp": "None",
"isQuarantineCustomized": true, "TCPReset": "BOTH", "isLogCustomized": true, "isTcpResetCustomized": true,
"isNbytesCustomized": true, "flow": "SINGLE_FLOW", "isMcAfeeNACNotificationEnabled": false, "isAlert": true,
"action": "SEND_ALERT_AND_LOG_PACKETS", "loggingDuration": { "CaptureNPackets": {"npackets": 5},
"AttackPacketOnly": {}, "RestOfFlow": null, "CaptureTimeDuration": { "timeUnit": "SECONDS", "time": "10" } },
"isRemediateEnabled": true, "isBlockingOptionCustomized": true }, "nspId": "0x40254c00", "isEnabled": true,
"benignTriggerProbability": "1 (Low)", "notification": { "isAutoAckCustomized": true, "isPager": true,
"isSyslogCustomized": true, "isPagerCustomized": true, "isEmail": true, "isScriptCustomized": true,
"isSnmpCustomized": true, "isScript": true, "isSnmp": true, "isEmailCustomized": true, "isAutoAck": true,
"isSyslog": true }, "isRecommendedForSmartBlocking": true, "isSeverityCustomized": true, "subCategory":
"dos" } ] }, "OutboundRuleSet": "DMZ", "InboundRuleSet": "Default Prevention" }
```

Response

```
{ status :1 }
```

Delete IPS Policy

This URL deletes IPS policy.

Resource URL

DELETE /ipspolicy/<policyid>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
policyId	Policy id	Number	Yes

Response

```
{ createdResourceId :1 }
```

Add a New Attack Filter

This URL adds a new attack filter.

Resource URL

POST /attackfilter

Request Parameters

Field Name	Description	Data Type	Mandatory
`name`	Attack filter name	String	Yes
`attackFilterId`	Attack filter id, not required for POST	Number	No
`Description`	Description	String	No
`DomainId`	Id of domain to which this attack filter belongs to	Number	Yes
`LastModTs`	Last modified timestamp	String	No
`Type`	Attack filter type, can be "IPV_4" / "IPV_6" / "TCP_UDP_PORT" / "IPV_4_TCP_UDP_PORT" / "IPV_6_TCP_UDP_PORT"	String	Yes
`MatchCriteria`	Attack filter exclusion	Object	Yes

Details of MatchCriteria:

Field Name	Description	Data Type	Mandatory
`Exclusion`	List of IP - port exclusions	Array	Yes

Details of object in Exclusion (depends on the Type defined):

Field Name	Description	Data Type	Mandatory
`Ip`	IPv4 or IPv6 IP	Object	No
`Port`	TCP / UDP port	Object	No

Details of Ip:

Field Name	Description	Data Type	Mandatory
`srcStart`	Source start IP	String	No
`srcEnd`	Source end IP	String	No

Field Name	Description	Data Type	Mandatory
`destStart`	Destination start IP	String	No
`destEnd`	Destination end IP	String	No
`srcMode`	Source IP mode, can be "ANY_IP" / "ANY_EXTERNAL_IP" / "ANY_INTERNAL_IP" / "RANGE_IP" / "SINGLE_IP"	String	Yes
`destMode`	Destination IP mode, can be "ANY_IP" / "ANY_EXTERNAL_IP" / "ANY_INTERNAL_IP" / "RANGE_IP" / "SINGLE_IP"	String	Yes

Details of Port:

Field Name	Description	Data Type	Mandatory
`srcPort`	Source port	String	No
`destPort`	Destination port	String	No
`srcPortMode`	Source port mode, can be "ANY_PORT" / "TCP_OR_UDP" / "TCP" / "UDP"	String	Yes
`destPortMode`	Destination port mode, can be "ANY_PORT" / "TCP_OR_UDP" / "TCP" / "UDP"	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique ID of the created attack filter	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/attackfilter

```
Payload: { "DomainId": 0, "Description": "try ", "MatchCriteria": { "Exclusion": [ { "Ip": { "destEnd":
"1.1.1.18", "destMode": "RANGE_IP", "srcMode": "SINGLE_IP", "srcStart": "1.1.1.1", "destStart": "1.1.1.13",
"srcEnd": "1.1.1.11" }, "Port": { "srcPortMode": "TCP", "srcPort": "85", "destPort": "89", "destPortMode":
"TCP" } } ] }, "Type": "IPV_4_AND_TCP_UDP_PORT", "name": "test1" }
```

Response

```
{ "createdResourceId":419 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1001	Internal error
2	404	1105	Invalid domain
3	400	1409	Attack filter name should not be greater than 40 chars
4	400	1118	Please provide a name
5	400	1401	Unable to set attack filter type
6	400	1404	Please provide IP
7	400	1406	Invalid IP Format
8	400	1407	Please provide Port
9	400	1414	Invalid source and destination combination
10	400	1415	Port not valid, please enter a number between 1 and 65535
11	400	1416	IP mode not valid
12	400	1418	Start IP should be less than end IP

Update Attack Filter

This URL updates an attack filter.

Resource URL

PUT /attackfilter/<attackfilter_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
attackfilter_id	Attack filter id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
name	Attack filter name	String	Yes
attackFilterId	Attack filter id	Number	Yes
Description	Description	String	No

Field Name	Description	Data Type	Mandatory
`DomainId`	Id of domain to which this attack filter belongs to	Number	Yes
`LastModTs`	Last modified timestamp. For update, the LastModTs in PUT operation should be the same as returned by the GET operation for the same attack filter	String	Yes
`Type`	Attack filter type, can be "IPV_4" / "IPV_6" / "TCP_UDP_PORT" / "IPV_4_TCP_UDP_PORT" / "IPV_6_TCP_UDP_PORT"	String	Yes
`MatchCriteria`	Attack Filter Exclusion	Object	Yes

Details of MatchCriteria:

Field Name	Description	Data Type	Mandatory
`Exclusion`	List of IP - port exclusions	Array	Yes

Details of object in Exclusion (depends on the Type defined):

Field Name	Description	Data Type	Mandatory
`Ip`	IPv4 or IPv6 IP	Object	No
`Port`	TCP / UDP port	Object	No

Details of Ip:

Field Name	Description	Data Type	Mandatory
`srcStart`	Source start IP	String	No
`srcEnd`	Source end IP	String	No
`destStart`	Destination start IP	String	No
`destEnd`	Destination end IP	String	No
`srcMode`	Source IP mode, can be "ANY_IP" / "ANY_EXTERNAL_IP" / "ANY_INTERNAL_IP" / "RANGE_IP" / "SINGLE_IP"	String	Yes
`destMode`	Destination IP mode, can be "ANY_IP" / "ANY_EXTERNAL_IP" /	String	Yes

Field Name	Description	Data Type	Mandatory
	"ANY_INTERNAL_IP" / "RANGE_IP" / "SINGLE_IP"		

Details of port:

Field Name	Description	Data Type	Mandatory
`srcPort`	Source port	String	No
`destPort`	Destination port	String	No
`srcPortMode`	Source port mode, can be "ANY_PORT" / "TCP_OR_UDP" / "TCP" / "UDP"	String	Yes
`destPortMode`	Destination port mode, can be "ANY_PORT" / "TCP_OR_UDP" / "TCP" / "UDP"	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status after update	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/attackfilter/419

```
Payload: { "DomainId": 0, "Description": "try", "MatchCriteria": { "Exclusion": [ { "Ip": { "destEnd":
"1.1.1.17", "destMode": "RANGE_IP", "srcMode": "SINGLE_IP", "srcStart": "1.1.1.1", "destStart": "1.1.1.13",
"srcEnd": "1.1.1.11" }, "Port": { "srcPortMode": "TCP", "srcPort": "85", "destPort": "89", "destPortMode":
"TCP" } } ] }, "LastModTs": "2012-07-24 00:19:00", "attackFilterId": 419, "Type": "IPV_4_AND_TCP_UDP_PORT",
"name": "test1" }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1001	Internal error
2	404	1105	Invalid domain
3	400	1409	Attack filter name should not be greater than 40 chars
4	400	1118	Please provide a name
5	400	1401	Unable to set attack filter type
6	400	1404	Please provide IP
7	400	1406	Invalid IP format

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
8	400	1407	Please provide port
9	400	1408	Invalid attack filter id
10	400	1414	Invalid source and destination combination
11	400	1415	Port not valid, please enter a number between 1 and 65535
12	400	1416	IP mode not valid
13	400	1418	Start IP should be less than end IP

Delete Attack Filter

This URL deletes an attack filter.

Resource URL

DELETE /attackfilter/<attackfilter_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`attackfilter_id`	Attack filter id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status returned by deletion	Number

Request

Example

DELETE https://%3CNSM_IP%3E/sdkapi/attackfilter/419

Response

```
{ "status":1 }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1408	Invalid attack filter id

Get an Attack Filter

This URL gets the details of an attack filter.

Resource URL

GET /attackfilter/<attackfilter_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`attackfilter_id`	Attack filter id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`name`	Attack filter name	String
`attackFilterId`	Attack filter id	Number
`Description`	Description	String
`DomainId`	Id of domain to which this attack filter belongs to	Number
`LastModTs`	Last modified timestamp	String
`Type`	Attack filter type, can be "IPV_4" / "IPV_6" / "TCP_UDP_PORT" / "IPV_4_TCP_UDP_PORT" / "IPV_6_TCP_UDP_PORT"	String
`MatchCriteria`	Attack filter exclusion	Object

Details of MatchCriteria:

Field Name	Description	Data Type
`Exclusion`	List of IP - port exclusions	Array

Details of object in Exclusion (depends on the Type defined):

Field Name	Description	Data Type
`Ip`	IPv4 or IPv6 IP	Object
`Port`	TCP / UDP port	Object

Details of Ip:

Field Name	Description	Data Type
`srcStart`	Source start IP	String
`srcEnd`	Source end IP	String
`destStart`	Destination start IP	String
`destEnd`	Destination end IP	String
`srcMode`	Source IP mode, can be "ANY_IP" / "ANY_EXTERNAL_IP" / "ANY_INTERNAL_IP" / "RANGE_IP" / "SINGLE_IP"	String
`destMode`	Destination IP mode, can be "ANY_IP" / "ANY_EXTERNAL_IP" / "ANY_INTERNAL_IP" / "RANGE_IP" / "SINGLE_IP"	String

Details of port:

Field Name	Description	Data Type
`srcPort`	Source port	String
`destPort`	Destination port	String
`srcPortMode`	Source port mode, can be "ANY_PORT" / "TCP_OR_UDP" / "TCP" / "UDP"	String
`destPortMode`	Destination port mode, can be "ANY_PORT" / "TCP_OR_UDP" / "TCP" / "UDP"	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/%20attackfilter/420

Response

```
{ "DomainId": 0, "MatchCriteria": { "Exclusion": [ { "Ip": {}, "Port": { "srcPortMode": "TCP", "srcPort": "85",
"destPort": "89", "destPortMode": "TCP" } } ] }, "LastModTs": "2012-07-24 00:19:00", "attackFilterId": 420,
"Type": "TCP_UDP_PORT", "name": "test2" }
```

Error Information

Following error code isreturned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1408	Invalid attack filter id

Get Attack Filters Defined in a Domain

This URL gets all the attack filters defined in the specified domain.

Resource URL

GET /attackfilters?domain=<domain_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	ID of domain in which the attack filter has been created	Number	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
AttackFilterDescriptor	List of attack filters with basic details	Array

Details of object in AttackFilterDescriptor:

Field Name	Description	Data Type
VisibleToChild	Attack filter visible to child domain	Boolean
DomainId	ID of domain in which the attack filter was added	Number
IsEditable	If attack filter editable	Boolean
LastModTs	Last modified timestamp	String
filterId	Attack filter id	Number
name	Attack filter name	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/%20attackfilters?domain=0

Response

{ "AttackFilterDescriptor": [{ "VisibleToChild": false, "name": "test1", "IsEditable": false, "filterId": 419, "DomainId": 0, "LastModTs": "2012-07-24 00:14:00" }, { "VisibleToChild": false, "name": "test2", "IsEditable": false, "filterId": 420, "DomainId": 0, "LastModTs": "2012-07-24 00:19:00" }] }

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Assign an Attack Filter to a Domain and an Attack

This URL assigns the specified attack filters to a particular domain and an attack.

Resource URL

POST /domain/<domain_id>/attackfilter

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	ID of domain in which the attack filter is created	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`AssignAttackFilterRequest`	List of attack filters	Array	Yes

Details of object in AssignAttackFilterRequest:

Field Name	Description	Data Type	Mandatory
`AttackID`	Attack id	String	Yes
`Direction`	Attack direction, can be "INBOUND" / "OUTBOUND" / "BOTH" / "UNKNOWN"	String	Yes
`Overwrite`	Overwrite filter	Number	Yes
`FilterId`	List of attack filter id's	Array	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Assignment status	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/domain/0/attackfilter

```
Payload: { "AssignAttackFilterRequest": [ { "Direction": "INBOUND", "AttackId": "0x40503900", "FilterId": [ 419,
420 ], "Overwrite": true }, { "Direction": " INBOUND ", "AttackId": "0x48304e00", "FilterId": [ 419 ],
"Overwrite": true } ] }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	404	1402	Invalid attack id

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
3	404	1403	Invalid attack direction
4	404	1408	Invalid attack filter id

Get Attack Filters Assigned to a Domain and an Attack

This URL gets all the attack filters assigned to the domain for a specific attack.

Resource URL

GET /domain/<domain_id>/attackfilter/<attack_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	ID of domain in which the attack filter is created	Number	Yes
`attack_id`	Attack id to which attack filters are assigned	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`AttackFilterDescriptor`	List of attack filters with basic details	Array

Details of object in AttackFilterDescriptor:

Field Name	Description	Data Type
`VisibleToChild`	Attack filter visible to child domain	Boolean
`DomainId`	ID of domain in which the attack filter was added	Number
`IsEditable`	If attack filter editable	Boolean
`LastModTs`	Last modified time stamp	String
`filterId`	Attack filter id	Number
`name`	Attack filter name	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/domain/0/attackfilter/0x40503900

Response

```
{ "AttackFilterDescriptor": [ { "VisibleToChild": true, "name": "test1", "IsEditable": false, "filterId": 419,
"DomainId": 0, "LastModTs": "2012-07-24 00:14:00" }, { "VisibleToChild": true, "name": "test2", "IsEditable":
false, "filterId": 420, "DomainId": 0, "LastModTs": "2012-07-24 00:19:00" } ] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	404	1402	Invalid attack id

Unassign Attack Filters Assigned to a Domain and an Attack

This URL unassign all the attack filters to the domain for a specific attack.

Resource URL

DELETE /domain/<domain_id>/attackfilter/<attack_id>

Query Parameter: ?direction=

- INBOUND
- OUTBOUND

If the direction is not defined, it will throw error.

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	ID of domain in which the attack filter is created	Number	Yes
`attack_id`	Attack id to which attack filters are assigned	String	Yes
`direction`	Direction type can be INBOUND or OUTBOUND	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status returned by unassignment	Number

Example

Request

DELETE https://%3CNSM_IP%3E/sdkapi/domain/0/attackfilter/0x40503900%20?direction=INBOUND

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	404	1402	Invalid attack id
3	404	1403	Invalid attack direction

Assign an Attack Filter to a Sensor and an Attack

This URL assigns the specified attack filters to a particular Sensor and an attack.

Resource URL

POST /sensor/<sensor_id>/attackfilter

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`AssignAttackFilterRequest`	List of attack filters	Array	Yes

Details of object in AssignAttackFilterRequest:

Field Name	Description	Data Type	Mandatory
`AttackID`	Attack id	String	Yes
`Direction`	Attack direction, can be "INBOUND" / "OUTBOUND" / "BOTH" / "UNKNOWN"	String	Yes
`Overwrite`	Overwrite filter	Boolean	Yes
`FilterId`	List of attack filter Id's	Array	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Assignment status	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/sensor/1001/attackfilter

```
Payload: { "AssignAttackFilterRequest": [ { "Direction": " INBOUND ", "AttackId": "0x40503900", "FilterId":
[ 419, 420 ], "Overwrite": true }, { "Direction": " INBOUND ", "AttackId": "0x48304e00", "FilterId": [ 419 ],
"Overwrite": true } ] }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	404	1106	Invalid Sensor
3	404	1402	Invalid attack id
4	404	1403	Invalid attack direction

Get Attack Filters Assigned to a Sensor and an Attack

This URL gets all the attack filters assigned to the Sensor for a specific attack.

Resource URL

GET /sensor/<sensor_id>/attackfilter/<attack_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes
`attack_id`	Attack id to which the attack filters are assigned	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`AttackFilterDescriptor`	List of attack filters with basic details	Array

Details of object in AttackFilterDescriptor:

Field Name	Description	Data Type
`VisibleToChild`	Attack filter visible to child domain	Boolean
`DomainId`	ID of domain in which the attack filter was added	Number
`IsEditable`	If attack filter editable	Boolean

Field Name	Description	Data Type
LastModTs	Last modified time stamp	String
filterId	Attack filter id	Number
name	Attack filter name	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/sensor/1001/attackfilter/0x40503900

Response

{ "AttackFilterDescriptor": [{ "VisibleToChild": true, "name": "test1", "IsEditable": false, "filterId": 419, "DomainId": 0, "LastModTs": "2012-07-24 00:19:00" }, { "VisibleToChild": true, "name": "test2", "IsEditable": false, "filterId": 420, "DomainId": 0, "LastModTs": "2012-07-24 00:14:00" }] }

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	404	1402	Invalid attack id

Unassign Attack Filter to a Sensor and Attack

This URL unassign the specified attack filters to a particular Sensor and attack.

Resource URL

DELETE /sensor/<sensor_id>/attackfilter/<attack_id>

Query Parameter: ?direction=

- INBOUND
- OUTBOUND

If the direction is not defined, it will throw error

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensor_id	Sensor id	number	Yes
attack_id	Attack id to which the attack filters are assigned	String	Yes
direction	Direction type can be INBOUND or OUTBOUND	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status returned by unassignment	Number

Example

Request

DELETE https://%3CNSM_IP%3E/sdkapi/sensor/1001/attackfilter%20/0x40503900%20?direction=INBOUND

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	404	1402	Invalid attack id
3	404	1403	Invalid attack direction

Assign a Attack Filter to an Interface/SubInterface and Attack

This URL assigns the specified attack filters to a particular interface or subInterface and attack.

Resource URL

POST /sensor/<sensor_id>/interface/<interface_ id or subinterface-id>/attackfilter

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes
`interface_id or subinterface_id`	Interface/subinterface id to which the attack filter is to be assigned	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`AssignAttackFilterRequest`	List of attack filters	Array	Yes

Details of object in AssignAttackFilterRequest:

Field Name	Description	Data Type	Mandatory
`AttackID`	Attack id	String	Yes

Field Name	Description	Data Type	Mandatory
`Direction`	Attack direction, can be "INBOUND" / "OUTBOUND" / "BOTH" / "UNKNOWN"	String	Yes
`Overwrite`	Overwrite filter	Boolean	Yes
`FilterId`	List of attack filter Id's	Array	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status returned by deletion	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/sensor/1001/interface/105/attackfilter

```
Payload: { "AssignAttackFilterRequest": [ { "Direction": " INBOUND ", "AttackId": "0x40503900", "FilterId":
[ 419, 420 ], "Overwrite": true }, { "Direction": " INBOUND ", "AttackId": "0x48304e00", "FilterId": [ 419 ],
"Overwrite": true } ] }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	404	1107	Invalid interface or sub-interface id
3	404	1402	Invalid attack id
4	404	1403	Invalid attack direction
5	404	1408	Invalid attack filter id

Get Attack Filters Assigned to an Interface/SubInterface and Attack

This URL gets all the attack filters assigned to a particular interface or subinterface for a specific attack.

Resource URL

GET /sensor/<sensor_id>/interface/<interface_ id or subinterface_id>/attackfilter/<attack_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes
`interface_ id or subinterface_id`	Interface/subinterface id	Number	Yes
`attack_id`	Attack id to which the attack filters are assigned	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`AttackFilterDescriptor`	List of attack filters with basic details	Array

Details of object in AttackFilterDescriptor:

Field Name	Description	Data Type
`VisibleToChild`	Attack filter visible to child domain	Boolean
`DomainId`	ID of domain in which the attack filter was added	Number
`IsEditable`	If attack filter editable	Boolean
`LastModTs`	Last modified time stamp	String
`filterId`	Attack filter id	Number
`name`	Attack filter name	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/sensor/1001/interface/105/attackfilter/0x40503900

Response

```
{ "AttackFilterDescriptor": [ { "VisibleToChild": true, "name": "test1", "IsEditable": false, "filterId": 419,
"DomainId": 0, "LastModTs": "2012-07-24 00:19:00" }, { "VisibleToChild": true, "name": "test2", "IsEditable":
false, "filterId": 420, "DomainId": 0, "LastModTs": "2012-07-24 00:19:00" } ] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1402	Invalid attack id
2	404	1106	Invalid Sensor
3	404	1107	Invalid interface or sub-interface id

Unassign Attack Filters to an Interface/SubInterface

This URL unassign the attack filters assigned to a particular interface or subinterface for a specific attack.

Resource URL

GET /sensor/<sensor_id>/interface/<interface_id or subinterface_id>/attackfilter/<attack_id>

Query Parameter: ?direction=

- INBOUND
- OUTBOUND

If the direction is not defined, it will throw error

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensor_id	Sensor id	Number	Yes
interface_id or subinterface_id	interface/subinterface id	Number	Yes
attack_id	Attack id to which the attack filters are assigned	String	Yes
direction	Direction type can be INBOUND or OUTBOUND	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
Status	Status returned by unassignment	Number

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/sensor/1001/interface/105/attackfilter/0x40503900?direction=INBOUND

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1402	Invalid attack id
2	404	1106	Invalid Sensor
3	404	1107	Invalid interface or sub-interface id
4	404	1403	Invalid attack direction

Get Attack Filters Assignments

This URL gets the assignments of an attack filter across all attacks and resources.

Resource URL

GET /attackfilter/<attackfilter_id>/assignments

Request Parameters

Field Name	Description	Data Type	Mandatory
`attackfilter_id`	Attack filter id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`AssignmentDetails`	List of attack filter assignment details	Array

Details of object in AttackFilterDescriptor:

Field Name	Description	Data Type
`resourceName`	Resource (Domain/Sensor/Interface) name	String
`attackId`	Attack id	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/attackfilter/%3Cattackfilter_id/assignments

Response

```
{ "AssignmentDetails": [ { "resourceName": "My Company", "attackId": "0x40503900" }, { "resourceName": "My
Company", "attackId": "0x48304e00" } ] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1408	Invalid attack filter id

Add Rule Object

This URL adds a new rule object.

Resource URL

POST /ruleobject

Request Parameters

Field Name	Description	Data Type	Mandatory
`ruleobjId`	Rule object id	String	No
`ruleobjType`	Rule object type	String	Yes
`name`	Rule object name	String	Yes
`description`	Description	String	Yes
`domain`	ID of domain in which the rule object is defined	Number	Yes
`visibleToChild`	Is rule object visible to child	Boolean	Yes
`ApplicationGroup`	Application group object, should be defined if ruleobjType is "APPLICATION_GROUP"	Object	No
`ApplicationOnCustomPort`	Application defined on custom port object, should be defined if ruleobjType is "APPLICATION_ON_CUSTOM_PORT"	Object	No
`FiniteTimePeriod`	Finite time period object, should be defined if ruleobjType is "FINITE_TIME_PERIOD"	Object	No
`HostIPv4`	Host IPv4 address object, should be defined if ruleobjType is "HOST_IPV_4"	Object	No
`HostIPv6`	Host IPv6 address object, should be defined if ruleobjType is "HOST_IPV_6"	Object	No
`HostDNSName`	Host DNS name object, should be defined if ruleobjType is "HOST_DNS_NAME"	Object	No
`IPv4AddressRange`	IPv4 address range object, should be defined if	Object	No

Field Name	Description	Data Type	Mandatory
	ruleobjType is "IPV_4_ADDRESS_RANGE"		
IPv6AddressRange	IPv6 address range object, should be defined if ruleobjType is "IPV_6_ADDRESS_RANGE"	Object	No
NetworkIPv4	IPv4 network object, should be defined if ruleobjType is "NETWORK_IPV_4"	Object	No
NetworkIPv6	IPv6 network object, should be defined if ruleobjType is "NETWORK_IPV_6"	Object	No
NetworkGroup	Network group object, should be defined if ruleobjType is "NETWORK_GROUP"	Object	No
RecurringTimePeriod	Recurring time period object, should be defined if ruleobjType is "RECURRING_TIME_PERIOD"	Object	No
RecurringTimePeriodGroup	Recurring time period group object, should be defined if ruleobjType is "RECURRING_TIME_PERIOD_GROUP"	Object	No
Service	Service object, should be defined if ruleobjType is "CUSTOM_SERVICE"	Object	No
ServiceRange	Service range object, should be defined if ruleobjType is "SERVICE_RANGE"	Object	No
ServiceGroup	Service group object, should be defined if ruleobjType is "SERVICE_GROUP"	Object	No
NetworkGroupAF	Network group for exception objects should be defined if ruleobjType is "NETWORK_GROUP_AF". This type of rule object is applicable only for alert filter/ ignore rules.	Object	No

Details of ApplicationGroup:

Field Name	Description	Data Type	Mandatory
ApplicationIdentifier	List of applications identifier	Array	Yes

Details of object in ApplicationIdentifier:

Field Name	Description	Data Type	Mandatory
`applicationRuleObjId`	Application rule object id	String	Yes
`applicationType`	Application Type, can be "DEFAULT_APPLICATION" / "APPLICATION_ON_CUSTOM_PORT"	String	Yes

Details of ApplicationonCustomPort:

Field Name	Description	Data Type	Mandatory
`applicationId`	Application id	String	Yes
`portsList`	List of ports	Array	Yes

Details of object in portsList:

Field Name	Description	Data Type	Mandatory
`IPProtocol`	IP protocol, can be "TCP" / "UDP"	String	Yes
`port`	Port	Number	Yes

Details of FiniteTimePeriod:

Field Name	Description	Data Type	Mandatory
`from`	From time	String	Yes
`until`	To time	String	Yes

Details of HostIPv4:

Field Name	Description	Data Type	Mandatory
`hostIPv4AddressList`	List of IPv4 host address	Array	Yes

Details of HostIPv6:

Field Name	Description	Data Type	Mandatory
`hostIPv6AddressList`	List of IPv6 host address	Array	Yes

Details of HostDNSName

Field Name	Description	Data Type	Mandatory
`hostDNSNameList`	List of host DNS names	Array	Yes

Details of IPv4AddressRange:

Field Name	Description	Data Type	Mandatory
`IPV4RangeList`	List of IPv4 address range	Array	Yes

Details of object in rangeList:

Field Name	Description	Data Type	Mandatory
`FromAddress`	Start IP range	String	Yes
`ToAddress`	End IP range	String	Yes

Details of IPv6AddressRange:

Field Name	Description	Data Type	Mandatory
`IPV6RangeList`	List of IPv6 address range	Array	Yes

Details of object in rangeList:

Field Name	Description	Data Type	Mandatory
`FromAddress`	Start IPv6 range	String	Yes
`ToAddress`	End IPv6 range	String	Yes

Details of NetworkIPv4:

Field Name	Description	Data Type	Mandatory
`networkIPV4List`	List of network IPv4 addresses	Array	Yes

Details of NetworkIPv6:

Field Name	Description	Data Type	Mandatory
`networkIPV6List`	List of network IPv6 addresses	Array	Yes

Details of NetworkGroup:

Field Name	Description	Data Type	Mandatory
`NetworkGroupIdentifier`	List of network objects	Array	Yes

Details of object in NetworkGroupIdentifier:

Field Name	Description	Data Type	Mandatory
`RuleObjId`	Network rule object id	String	Yes
`type`	Network Type, can be "COUNTRY" / "HOST_IPV_4" / "HOST_IPV_6" / "HOST_DNS_NAME" /	String	Yes

Field Name	Description	Data Type	Mandatory
	"IPV_4_ADDRESS_RANGE" / "IPV_6_ADDRESS_RANGE" / "NETWORK_IPV_4" / "NETWORK_IPV_6"		

Details of RecurringTimePeriod:

Field Name	Description	Data Type	Mandatory
`entireDay`	Entire day object	Boolean	Yes
`duration`	Duration object	Object	No
`day`	List of days, can be "MONDAY", "TUESDAY", "WEDNESDAY", "THURSDAY", "FRIDAY", "SATURDAY", "SUNDAY"	String	Yes

Details of object in duration:

Field Name	Description	Data Type	Mandatory
`from`	From time	String	Yes
`until`	To time	String	Yes

Details of RecurringTimePeriodGroup:

Field Name	Description	Data Type	Mandatory
`recurringTimePeriodsId`	List of recurring time period rule object Id's	Array	Yes

Details of Service:

Field Name	Description	Data Type	Mandatory
`protocol`	Protocol, can be "TCP" / "UDP" / "PROTOCOL_NUMBER"	String	Yes
`portNumber`	Port number	String	Yes

Details of ServiceRange:

Field Name	Description	Data Type	Mandatory
`protocol`	Protocol, can be "TCP" / "UDP" / "PROTOCOL_NUMBER"	String	Yes
`From`	From port/protocol number	String	Yes

Field Name	Description	Data Type	Mandatory
`To`	To port/protocol number	String	Yes

Details of ServiceGroup:

Field Name	Description	Data Type	Mandatory
`ServiceIdentifier`	List of service objects	Array	Yes

Details of object in ServiceIdentifier:

Field Name	Description	Data Type	Mandatory
`ServiceRuleObjId`	Service rule object id	String	Yes
`ServiceType`	Service type, can be "DEFAULT_SERVICE" / "CUSTOM_SERVICE"	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique ID of the created rule object	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/ruleobject

Payload:

```
{ "RuleObjDef": { "domain": 0, "visibleToChild": true, "description": "try", "ruleobjId": 0, "name": "test_NTW",
"Network": { "networkList": [ "172.0.0.0/8", "172.16.0.0/16", "192.168.12.0/24" ] }, "ruleobjType":
"NETWORK", } }
```

Response

```
{ "createdResourceId":121 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1406	Invalid IP format
2	400	1418	Start IP should be less than end IP
3	400	1701	Invalid CIDR notation
4	400	1703	Please specify at least one day
5	400	1705	Port number should be between 1 and 65534
6	400	1706	Rule objects which are not visible to child admin domains

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
			cannot be added to a rule object visible to child admin domain
7	404	1707	Default rule objects cannot be created/updated/deleted
8	400	1708	Start time is greater than end time
9	400	1709	Invalid time format
10	400	1710	Invalid DNS name
11	400	1711	Rule object name is required
12	400	1712	From and To both are required
13	400	1713	list cannot be empty
14	400	1716	Protocol number should be between 0 and 255
15	400	1717	Start port should be less than the end port
16	400	1718	Duplicate entry found
17	400	1719	List size should be less than or equal to 10
18	400	1720	Invalid rule object id/ rule object not visible to this domain
19	400	1721	Network group rule object can contain either IPV4/IPV6 rule objects, but not both simultaneously

Update Rule Object

This URL updates a rule object.

Resource URL

PUT /ruleobject/<ruleobject_id>

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
`ruleobject_id`	Unique id of rule object	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`ruleobjId`	Rule object id	String	No
`ruleobjType`	Rule object name	String	Yes
`name`	Rule object type	String	Yes
`description`	Description	String	Yes
`domain`	ID of domain in which the rule object is defined	Number	Yes
`visibleToChild`	Is rule object visible to child	Boolean	Yes
`ApplicationGroup`	Application group object, should be defined if ruleobjType is "APPLICATION_GROUP"	Object	No
`ApplicationOnCustomPort`	Application defined on custom port object, should be defined if ruleobjType is "APPLICATION_ON_CUSTOM_PORT"	Object	No
`FiniteTimePeriod`	Finite time period object, should be defined if ruleobjType is "FINITE_TIME_PERIOD"	Object	No
`HostIPv4`	Host IPv4 address object, should be defined if ruleobjType is "HOST_IPV_4"	Object	No
`HostIPv6`	Host IPv6 address object, should be defined if ruleobjType is "HOST_IPV_6"	Object	No
`HostDNSName`	Host DNS name object, should be defined if ruleobjType is "HOST_DNS_NAME"	Object	No
`IPv4AddressRange`	IPv4 address range object, should be defined if ruleobjType is "IPV_4_ADDRESS_RANGE"	Object	No
`IPv6AddressRange`	IPv6 address range object, should be	Object	No

Field Name	Description	Data Type	Mandatory
	defined if ruleobjType is "IPV_6_ADDRESS_RANGE"		
NetworkIPv4	IPv4 network object, should be defined if ruleobjType is "NETWORK_IPV_4"	Object	No
NetworkIPv6	IPv6 network object, should be defined if ruleobjType is "NETWORK_IPV_6"	Object	No
NetworkGroup	Network group object, should be defined if ruleobjType is "NETWORK_GROUP"	Object	No
RecurringTimePeriod	Recurring time period object, should be defined if ruleobjType is "RECURRING_TIME_PERIOD"	Object	No
RecurringTimePeriodGroup	Recurring time period group object, should be defined if ruleobjType is "RECURRING_TIME_PERIOD_GROUP"	Object	No
Service	Service object, should be defined if ruleobjType is "CUSTOM_SERVICE"	Object	No
ServiceRange	Service range object, should be defined if ruleobjType is "SERVICE_RANGE"	Object	No
ServiceGroup	Service group object, should be defined if ruleobjType is "SERVICE_GROUP"	Object	No
NetworkGroupAF	Network group for exception objects should be defined if ruleobjType is "NETWORK_GROUP_AF". This type of rule object is applicable only for alert filter/Ignore rules.	Object	No

Details of ApplicationGroup:

Field Name	Description	Data Type	Mandatory
`ApplicationIdentifier`	List of applications identifier	Array	Yes

Details of object in ApplicationIdentifier:

Field Name	Description	Data Type	Mandatory
`applicationRuleObjId`	Application rule object id	String	Yes
`applicationType`	Application Type, can be "DEFAULT_APPLICATION" / "APPLICATION_ON_CUSTOM_PORT"	String	Yes

Details of ApplicationonCustomPort:

Field Name	Description	Data Type	Mandatory
`applicationId`	Application id	String	Yes
`portsList`	List of ports	Array	Yes

Details of object in portsList:

Field Name	Description	Data Type	Mandatory
`IPProtocol`	IP protocol, can be "TCP" / "UDP"	String	Yes
`port`	Port	Number	Yes

Details of FiniteTimePeriod:

Field Name	Description	Data Type	Mandatory
`from`	From time	String	Yes
`until`	To time	String	Yes

Details of HostIPv4:

Field Name	Description	Data Type	Mandatory
`hostIPAddressList`	List of IPv4 host address	Array	Yes

Details of HostIPv6:

Field Name	Description	Data Type	Mandatory
`hostIPAddressList`	List of IPv6 host address	Array	Yes

Details of HostDNSName:

Field Name	Description	Data Type	Mandatory
`hostDNSNameList`	List of host DNS names	Array	Yes

Details of IPv4AddressRange:

Field Name	Description	Data Type	Mandatory
`rangeList`	List of IPv4 address range	Array	Yes

Details of object in rangeList:

Field Name	Description	Data Type	Mandatory
`FromAddress`	Start IP range	String	Yes
`ToAddress`	End IP range	String	Yes

Details of IPv6AddressRange:

Field Name	Description	Data Type	Mandatory
`rangeList`	List of IPv6 address range	Array	Yes

Details of object in rangeList:

Field Name	Description	Data Type	Mandatory
`FromAddress`	Start IPv6 range	String	Yes
`ToAddress`	End IPv6 Range	String	Yes

Details of NetworkIPv4:

Field Name	Description	Data Type	Mandatory
`networkList`	List of network IPv4 addresses	Array	Yes

Details of NetworkIPv6:

Field Name	Description	Data Type	Mandatory
`networkList`	List of network IPv6 addresses	Array	Yes

Details of NetworkGroup:

Field Name	Description	Data Type	Mandatory
`NetworkGroupIdentifier`	List of network objects	Array	Yes

Details of object in NetworkGroupIdentifier:

Field Name	Description	Data Type	Mandatory
`RuleObjId`	Network rule object id	String	Yes
`type`	Network type, can be "COUNTRY" / "HOST_IPV_4" / "HOST_IPV_6" / "HOST_DNS_NAME" / "IPV_4_ADDRESS_RANGE" / "IPV_6_ADDRESS_RANGE" / "NETWORK_IPV_4" / "NETWORK_IPV_6"	String	Yes

Details of RecurringTimePeriod:

Field Name	Description	Data Type	Mandatory
`entireDay`	Entire day object	Boolean	Yes
`duration`	Duration object	Object	No
`day`	List of days, can be "MONDAY", "TUESDAY", "WEDNESDAY", "THURSDAY", "FRIDAY", "SATURDAY", "SUNDAY"	String	Yes

Details of object in duration:

Field Name	Description	Data Type	Mandatory
`from`	From time	String	Yes
`until`	To time	String	Yes

Details of RecurringTimePeriodGroup:

Field Name	Description	Data Type	Mandatory
`recurringTimePeriodsId`	List of recurring time period rule object Id's	Array	Yes

Details of Service:

Field Name	Description	Data Type	Mandatory
`protocol`	Protocol, can be "TCP" / "UDP" / "PROTOCOL_NUMBER"	String	Yes
`portNumber`	Port number	String	Yes

Details of ServiceRange:

Field Name	Description	Data Type	Mandatory
`protocol`	Protocol, can be "TCP" / "UDP" / "PROTOCOL_NUMBER"	String	Yes
`From`	From port/protocol number	String	Yes
`To`	To port/protocol number	String	Yes

Details of ServiceGroup:

Field Name	Description	Data Type	Mandatory
`ServiceIdentifier`	List of service objects	Array	Yes

Details of object in ServiceIdentifier:

Field Name	Description	Data Type	Mandatory
`ServiceRuleObjId`	Service rule object id	String	Yes
`ServiceType`	Service type, can be "DEFAULT_SERVICE" / "CUSTOM_SERVICE"	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status returned by deletion	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/ruleobject/121

Payload:

```
{ "RuleObjDef": { "visibleToChild": true, "description": "try", "ruleobjId": 0, "name": "test_NTW_new",
"Network": { "networkList": [ "172.0.0.0/8", "192.168.12.0/24" ] }, "ruleobjType": "NETWORK", } }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1406	Invalid IP format
2	400	1418	Start IP should be less than end IP
3	400	1701	Invalid CIDR notation

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
4	400	1702	Rule object type cannot be changed
5	400	1703	Please specify at least one day
6	400	1705	Port number should be between 1 and 65534
7	400	1706	Rule objects which are not visible to child admin domains cannot be added to a rule object visible to child admin domain
8	404	1707	Default rule objects cannot be created/updated/deleted
9	400	1708	Start time is greater than end time
10	400	1709	Invalid time format
11	400	1710	Invalid DNS name
12	400	1711	Rule object name is required
13	400	1712	From and to both are required
14	400	1713	list cannot be empty
15	400	1714	Domain Id cannot be changed
16	400	1716	Protocol number should be between 0 and 255
17	400	1717	Start port should be less than the end port
18	400	1718	Duplicate entry found
19	400	1719	List size should be less than or equal to 10
20	400	1720	Invalid rule object id/ rule object not visible to this domain
21	400	1721	Network group rule object can contain either IPV4/IPV6 rule objects, but not both simultaneously

Delete Rule Object

This URL deletes a rule object. If the rule object is in use, the rule object will not be deleted.

Resource URL

DELETE /ruleobject/<ruleobject_id>

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
`ruleobject_id`	Unique id of rule object	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status returned by deletion	Number

Example

Request

DELETE https://%3CNSM_IP%3E/sdkapi/ruleobject/121

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1707	Default rule objects cannot be created/updated/deleted
2	400	1715	Assigned rule object cannot be deleted
3	400	1720	Invalid rule object Id/ rule object not visible to this domain

Get Rule Object

This URL gets the details of a rule object.

Resource URL

GET /ruleobject/<ruleobject_id>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ruleobject_id`	Rule object id	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
ruleobjId	Rule object id	String
ruleobjType	Rule object name	String
name	Rule object type	String
description	Description	String
domain	ID of domain in which the rule object is defined	Number
visibleToChild	Is rule object visible to child	Boolean
ApplicationGroup	Application group object, should be defined if ruleobjType is "APPLICATION_GROUP"	Object
ApplicationOnCustomPort	Application defined on custom port object, should be defined if ruleobjType is "APPLICATION_ON_CUSTOM_PORT"	Object
FiniteTimePeriod	Finite time period object, should be defined if ruleobjType is "FINITE_TIME_PERIOD"	Object
HostIPv4	Host IPv4 address object, should be defined if ruleobjType is "HOST_IPV_4"	Object
HostIPv6	Host IPv6 address object, should be defined if ruleobjType is "HOST_IPV_6"	Object
HostDNSName	Host DNS name object, should be defined if ruleobjType is "HOST_DNS_NAME"	Object
IPv4AddressRange	IPv4 address range object, should be defined if ruleobjType is "IPV_4_ADDRESS_RANGE"	Object
IPv6AddressRange	IPv6 address range object, should be defined if ruleobjType is "IPV_6_ADDRESS_RANGE"	Object

Field Name	Description	Data Type
NetworkIPv4	IPv4 network object, should be defined if ruleobjType is "NETWORK_IPV_4"	Object
NetworkIPv6	IPv6 network object, should be defined if ruleobjType is "NETWORK_IPV_6"	Object
NetworkGroup	Network group object, should be defined if ruleobjType is "NETWORK_GROUP"	Object
RecurringTimePeriod	Recurring time period object, should be defined if ruleobjType is "RECURRING_TIME_PERIOD"	Object
RecurringTimePeriodGroup	Recurring time period group object, should be defined if ruleobjType is "RECURRING_TIME_PERIOD_GROUP"	Object
Service	Service object, should be defined if ruleobjType is "CUSTOM_SERVICE"	Object
ServiceRange	Service range object, should be defined if ruleobjType is "SERVICE_RANGE"	Object
ServiceGroup	Service group object, should be defined if ruleobjType is "SERVICE_GROUP"	Object
NetworkGroupAF	Network group for exception objects should be defined if ruleobjType is "NETWORK_GROUP_AF". This type of rule object is applicable only for alert filter/ Ignore rules.	Object

Details of ApplicationGroup:

Field Name	Description	Data Type
ApplicationIdentifier	List of applications identifier	Array

Details of object in ApplicationIdentifier:

Field Name	Description	Data Type
applicationRuleObjId	Application rule object id	String

Field Name	Description	Data Type
`applicationType`	Application type, can be "DEFAULT_APPLICATION" / "APPLICATION_ON_CUSTOM_PORT"	String

Details of ApplicationonCustomPort

Field Name	Description	Data Type
`applicationId`	Application id	String
`portsList`	List of ports	Array

Details of object in portsList:

Field Name	Description	Data Type
`IPProtocol`	IP protocol, can be "TCP" / "UDP"	String
`port`	Port	Number

Details of FiniteTimePeriod:

Field Name	Description	Data Type
`from`	From time	String
`until`	To time	String

Details of HostIPv4:

Field Name	Description	Data Type
`hostIPAddressList`	List of IPv4 host Address	Array

Details of HostIPv6:

Field Name	Description	Data Type
`hostIPAddressList`	List of IPv6 host Address	Array

Details of HostDNSName:

Field Name	Description	Data Type
`hostDNSNameList`	List of host DNS names	Array

Details of IPv4AddressRange:

Field Name	Description	Data Type
`rangeList`	List of IPv4 address range	Array

Details of object in rangeList:

Field Name	Description	Data Type
`FromAddress`	Start IP range	String
`ToAddress`	End IP range	String

Details of IPv6AddressRange:

Field Name	Description	Data Type
`rangeList`	List of IPv6 address range	Array

Details of object in rangeList:

Field Name	Description	Data Type
`FromAddress`	Start IPv6 range	String
`ToAddress`	End IPv6 range	String

Details of NetworkIPv4:

Field Name	Description	Data Type
`networkList`	List of network IPv4 addresses	Array

Details of NetworkIPv6

Field Name	Description	Data Type
`networkList`	List of network IPv6 addresses	Array

Details of NetworkGroup:

Field Name	Description	Data Type
`NetworkGroupIdentifier`	List of network objects	Array

Details of object in NetworkGroupIdentifier:

Field Name	Description	Data Type
`RuleObjId`	Network rule object id	String
`type`	Network type, can be "COUNTRY" / "HOST_IPV_4" / "HOST_IPV_6" / "HOST_DNS_NAME" / "IPV_4_ADDRESS_RANGE" / "IPV_6_ADDRESS_RANGE" / "NETWORK_IPV_4" / "NETWORK_IPV_6"	String

Details of RecurringTimePeriod:

Field Name	Description	Data Type
`entireDay`	Entire day object	Boolean
`duration`	Duration object	Object
`day`	List of days, can be "MONDAY", "TUESDAY", "WEDNESDAY", "THURSDAY", "FRIDAY", "SATURDAY", "SUNDAY"	String

Details of object in duration:

Field Name	Description	Data Type
`from`	From time	String
`until`	To time	String

Details of RecurringTimePeriodGroup

Field Name	Description	Data Type
`recurringTimePeriodsId`	List of recurring time period rule object Id's	Array

Details of Service

Field Name	Description	Data Type
`protocol`	Protocol, can be "TCP" / "UDP" / "PROTOCOL_NUMBER"	String
`portNumber`	Port number	String

Details of ServiceRange

Field Name	Description	Data Type
protocol	Protocol, can be "TCP" / "UDP" / "PROTOCOL_NUMBER"	String
From	From port/protocol number	String
To	To port/protocol number	String

Details of ServiceGroup

Field Name	Description	Data Type
`ServiceIdentifier`	List of service objects	Array

Details of object in ServiceIdentifier:

Field Name	Description	Data Type
`ServiceRuleObjId`	Service rule object id	String
`ServiceType`	Service Type, can be "DEFAULT_SERVICE" / "CUSTOM_SERVICE"	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ruleobject/%3Cruleobject_id%20%3E

Response

```
{ "RuleObjDef": { "domain": 0, "visibleToChild": true, "Network": { "networkList": [ "172.0.0.0/8",
"172.16.0.0/16", "192.168.12.0/24" ] }, "description": "try", "ruleobjId": "121", "ruleobjType": "NETWORK",
"name": "test_NTW" } }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1720	Invalid rule object Id/ rule object not visible to this domain

Get Rule Object Associations

This URL gets the associations of rule objects from all the modules where it is being used.

Resource URL

GET/ruleobject/<ruleobject_id>/assignments

Request Parameters

Field Name	Description	Data Type	Mandatory
`ruleobject_id`	Rule object id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`RuleObjectAssociationResponseList`	List of rule object association	Array

Details of object in RuleObjectAssociationResponseList:

Field Name	Description	Data Type
`usagePath`	Rule object usage path	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ruleobject/121/assignments

Response

```
{ "RuleObjectAssociationResponseList": [ { "usagePath": "My Company/NAC Settings/Network Setup/Network Access
Zones/Allow Public Networks and Private DNS/Rule 11/Destination" }, { "usagePath": "My Company/NAC Settings/
Network Setup/Network Access Zones/Allow Public Networks/Rule 01/Destination" } ] }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1720	Invalid rule object Id/ rule object not visible to this domain

Get Rule Objects in a Domain

This URL gets the list of rule objects defined in a particular domain.

Resource URL

GET /domain/<domain_id>/ruleobject?type=<ruleobject_type>

Request Parameters

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes
`type`	Rule object type, can be application, applicationgroup, applicationoncustomport, country, finitetimeperiod, hostdnsname, hostipv4, hostipv6, ipv4addressrange, ipv6addressrange, network ipv4, networkipv6, networkgroup, recurringtimeperiod, recurringtimeperiodgroup, service, servicerange, servicegroup	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`ruleobjId`	Rule object id	String
`ruleobjType`	Rule object name	String

Field Name	Description	Data Type
name	Rule object type	String
description	Description	String
domain	ID of domain in which the rule object is defined	Number
visibleToChild	Is rule object visible to child	Boolean
ApplicationGroup	Application group object, should be defined if ruleobjType is "APPLICATION_GROUP"	Object
ApplicationOnCustomPort	Application defined on custom port object, should be defined if ruleobjType is "APPLICATION_ON_CUSTOM_PORT"	Object
FiniteTimePeriod	Finite time period object, should be defined if ruleobjType is "FINITE_TIME_PERIOD"	Object
HostIPv4	Host IPv4 address object, should be defined if ruleobjType is "HOST_IPV_4"	Object
HostIPv6	Host IPv6 address object, should be defined if ruleobjType is "HOST_IPV_6"	Object
HostDNSName	Host DNS name object, should be defined if ruleobjType is "HOST_DNS_NAME"	Object
IPv4AddressRange	IPv4 address range object, should be defined if ruleobjType is "IPV_4_ADDRESS_RANGE"	Object
IPv6AddressRange	IPv6 address range object, should be defined if ruleobjType is "IPV_6_ADDRESS_RANGE"	Object
NetworkIPv4	IPv4 network object, should be defined if ruleobjType is "NETWORK_IPV_4"	Object
NetworkIPv6	IPv6 network object, should be defined if ruleobjType is "NETWORK_IPV_6"	Object

Field Name	Description	Data Type
`NetworkGroup`	Network group object, should be defined if ruleobjType is "NETWORK_GROUP"	Object
`RecurringTimePeriod`	Recurring time period object, should be defined if ruleobjType is "RECURRING_TIME_PERIOD"	Object
`RecurringTimePeriodGroup`	Recurring time period group object, should be defined if ruleobjType is "RECURRING_TIME_PERIOD_GROUP"	Object
`Service`	Service object, should be defined if ruleobjType is "CUSTOM_SERVICE"	Object
`ServiceRange`	Service range object, should be defined if ruleobjType is "SERVICE_RANGE"	Object
`ServiceGroup`	Service group object, should be defined if ruleobjType is "SERVICE_GROUP"	Object

Details of ApplicationGroup

Field Name	Description	Data Type
`ApplicationIdentifier`	List of applications identifier	Array

Details of object in ApplicationIdentifier:

Field Name	Description	Data Type
`applicationRuleObjId`	Application rule object id	String
`applicationType`	Application type, can be "DEFAULT_APPLICATION" / "APPLICATION_ON_CUSTOM_PORT"	String

Details of ApplicationonCustomPort

Field Name	Description	Data Type
`applicationId`	Application id	String
`portsList`	List of ports	Array

Details of object in portsList:

Field Name	Description	Data Type
IPProtocol	IP protocol, can be "TCP" / "UDP"	String
port	Port	Number

Details of FiniteTimePeriod:

Field Name	Description	Data Type
from	From time	String
until	To time	String

Details of HostIPv4:

Field Name	Description	Data Type
hostIPAddressList	List of IPv4 host address	Array

Details of HostIPv6:

Field Name	Description	Data Type
hostIPAddressList	List of IPv6 host address	Array

Details of HostDNSName:

Field Name	Description	Data Type
hostDNSNameList	List of Host DNS names	Array

Details of IPv4AddressRange:

Field Name	Description	Data Type
rangeList	List of IPv4 address range	Array

Details of object in rangeList:

Field Name	Description	Data Type
FromAddress	Start IP range	String
ToAddress	End IP range	String

Details of IPv6AddressRange:

Field Name	Description	Data Type
rangeList	List of IPv6 address range	Array

Details of object in rangeList:

Field Name	Description	Data Type
`FromAddress`	Start IPv6 range	String
`ToAddress`	End IPv6 range	String

Details of NetworkIPv4:

Field Name	Description	Data Type
`networkList`	List of network IPv4 addresses	Array

Details of NetworkIPv6:

Field Name	Description	Data Type
`networkList`	List of network IPv6 addresses	Array

Details of NetworkGroup

Field Name	Description	Data Type
`NetworkGroupIdentifier`	List of network objects	Array

Details of object in NetworkGroupIdentifier:

Field Name	Description	Data Type
`RuleObjId`	Network rule object id	String
`type`	Network type, can be "COUNTRY" / "HOST_IPV_4" / "HOST_IPV_6" / "HOST_DNS_NAME" / "IPV_4_ADDRESS_RANGE" / "IPV_6_ADDRESS_RANGE" / "NETWORK_IPV_4" / "NETWORK_IPV_6"	String

Details of RecurringTimePeriod:

Field Name	Description	Data Type
`entireDay`	Entire day object	Boolean
`duration`	Duration object	Object
`day`	List of days, can be "MONDAY", "TUESDAY", "WEDNESDAY", "THURSDAY", "FRIDAY", "SATURDAY", "SUNDAY"	String

Details of object in duration:

Field Name	Description	Data Type
`from`	From time	String

Field Name	Description	Data Type
`until`	To time	String

Details of RecurringTimePeriodGroup:

Field Name	Description	Data Type
`recurringTimePeriodsId`	List of recurring time period rule object Id's	Array

Details of Service:

Field Name	Description	Data Type
`protocol`	Protocol, can be "TCP" / "UDP" / "PROTOCOL_NUMBER"	String
`portNumber`	Port number	String

Details of ServiceRange:

Field Name	Description	Data Type
protocol	Protocol, can be "TCP" / "UDP" / "PROTOCOL_NUMBER"	String
From	From port/protocol number	String
To	To port/protocol number	String

Details of ServiceGroup:

Field Name	Description	Data Type
`ServiceIdentifier`	List of service objects	Array

Details of object in ServiceIdentifier:

Field Name	Description	Data Type
`ServiceRuleObjId`	Service rule object id	String
`ServiceType`	Service type, can be "DEFAULT_SERVICE" / "CUSTOM_SERVICE"	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/domain/0/ruleobject%20?type=
%20Application,ApplicationGroup,ApplicationOnCustomPort,Country,FiniteTimePeriod,HostDNSName,HostIpv4,IPV4AddressRange,Netwo

Response

```
{ "RuleObjDef": [ { "domain": 0, "visibleToChild": true, "name": "test2", "ruleobjId": "131",
"ApplicationOnCustomPort": { "portsList": [ { "IPProtocol": "TCP", "port": 310 }, { "IPProtocol": "UDP", "port":
320 }, ], "applicationId": "1375772672" }, "ruleobjType": "APPLICATION_ON_CUSTOM_PORT", "description": "try" },
{ "domain": 0, "visibleToChild": true, "name": "test2_SRV", "Service": { "protocol": "TCP", "portNumber": 100 },
"ruleobjId": "129", "ruleobjType": "SERVICE", "description": "try" }, { "domain": 0, "visibleToChild": true,
"name": "test2_SRVG", "ruleobjId": "130", "ServiceGroup": { "ServiceIdentifier": [ { "ServiceType":
"CUSTOM_SERVICE", "ServiceRuleObjId": "129" } ] }, "ruleobjType": "SERVICE_GROUP", "description": "try" },
{ "domain": 0, "visibleToChild": true, "name": "test_NG", "description": "try", "ruleobjId": "128",
"ruleobjType": "NETWORK_GROUP", "NetworkGroup": { "NetworkGroupIdentifier": [ { "RuleObjId": "121", "Type":
"NETWORK" }, { "RuleObjId": "KZ", "Type": "COUNTRY" }, { "RuleObjId": "125", "Type": "HOST_IPV_4" }, ] } },
{ "domain": 0, "visibleToChild": true, "name": "icmp-address mask reply", "Service": { "portNumber": 18 },
"ruleobjId": "27", "ruleobjType": "SERVICE", "description": "Default Network Object for ICMP Protocols" },
{ "domain": 0, "visibleToChild": true, "name": "test_IV4AR", "IPv4AddressRange": { "rangeList":
[ { "FromAddress": "1.2.3.4", "ToAddress": "2.3.4.5" }, { "FromAddress": "3.4.5.6", "ToAddress":
"4.5.6.7" } ] }, "ruleobjId": "127", "ruleobjType": "IPV_4_ADDRESS_RANGE", "description": "try" }, { "domain":
0, "visibleToChild": true, "name": "test_HDN", "ruleobjId": "126", "HostDNSName": { "hostDNSNameList":
[ "google.com", "facebook.com" ] }, "ruleobjType": "HOST_DNS_NAME", "description": "try" }, { "domain": 0,
"visibleToChild": true, "name": "test2_HI4", "ruleobjId": "125", "HostIPv4": { "hostIPAddressList":
[ "172.16.191.91", "172.16.232.91" ] }, "ruleobjType": "HOST_IPV_4", "description": "try" }, { "domain": 0,
"visibleToChild": true, "name": "test_RTPG", "ruleobjId": "124", "RecurringTimePeriodGroup":
{ "recurringTimePeriodsId": [ "122", "123" ] }, "ruleobjType": "RECURRING_TIME_PERIOD_GROUP", "description":
"try" }, { "domain": 0, "visibleToChild": true, "name": "test_RTP", "ruleobjId": "122", "ruleobjType":
"RECURRING_TIME_PERIOD", "RecurringTimePeriod": { "duration": { "from": "00:47", "until": "00:48" }, "day":
[ "SUNDAY", "MONDAY" ], "entireDay": false }, "description": "try" }, { "domain": 0, "visibleToChild": true,
"Network": { "networkList": [ "172.0.0.0/8", "172.16.0.0/16", "192.168.12.0/24" ] }, "description": "try",
"ruleobjId": "121", "ruleobjType": "NETWORK", "name": "test_NTW" }, { "domain": 0, "visibleToChild": true,
"description": "", "ruleobjId": "1090560000", "ruleobjType": "APPLICATION", "name": "Kerberos" }, { "domain": 0,
"visibleToChild": true, "name": "Web Conferencing", "ruleobjId": "-1", "ruleobjType": "APPLICATION_GROUP",
"ApplicationGroup": { "applicationIdentifier": [ { "applicationRuleObjId": "1107312640", "applicationType":
"DEFAULT_APPLICATION" }, { "applicationRuleObjId": "1107329024", "applicationType":
"DEFAULT_APPLICATION" }, ] }, "description": "" }, { "domain": 0, "visibleToChild": true, "description": "",
"ruleobjId": "VU", "ruleobjType": "COUNTRY", "name": "Vanuatu" }, ] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	404	1702	Invalid rule object type
3	404	1704	Rule object type is expected

Get User Rule Objects

This URL gets the user rule objects. If the filter string is provided, all the users matching to the given filter string will be returned. If more than one user matches the specified filter, maximum number of users will be restricted by max_entries_expected filter specified in the URL.

Resource URL

GET /ruleobject/user?filter=<user_name_filter>&maxcount=<max_entries_expected>

Request Parameters

Field Name	Description	Data Type	Mandatory
`user_name_filter`	User filter string	String	No
`max_entries_expected`	Maximum users to be displayed if more than 1 user match the user filter string	Number	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`UserRuleObjectResponseList`	List of user rule object	Array

Details of object in UserRuleObjectResponseList:

Field Name	Description	Data Type
`ruleObjectId`	Rule object id	String
`ruleObjectName`	Rule object name	String
`ruleObjectType`	Rule object type	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ruleobject/user?filter=user&max_count=10

Response

```
{ "userRuleObjectResponseList": [ { "ruleObjectId": "S-1-5-21-1459593717-2655996711-1404495803-3491",
"ruleObjectName": "user_32@rltest.com", "ruleObjectType": "User" }, { "ruleObjectId":
"S-1-5-21-1459593717-2655996711-1404495803-1177", "ruleObjectName": "user_48@rltest.com", "ruleObjectType":
"User" }, { "ruleObjectId": "S-1-5-21-1459593717-2655996711-1404495803-1123", "ruleObjectName":
"DFServ_user1@rltest.com", "ruleObjectType": "User" }, { "ruleObjectId":
"S-1-5-21-1459593717-2655996711-1404495803-1200", "ruleObjectName": "user_71@rltest.com", "ruleObjectType":
"User" }, { "ruleObjectId": "S-1-5-21-1459593717-2655996711-1404495803-3601", "ruleObjectName":
"myuser_15@rltest.com", "ruleObjectType": "User" }, { "ruleObjectId":
"S-1-5-21-1459593717-2655996711-1404495803-3430", "ruleObjectName": "user_103@rltest.com", "ruleObjectType":
"User" }, { "ruleObjectId": "S-1-5-21-1459593717-2655996711-1404495803-3560", "ruleObjectName":
"user_88_2@rltest.com", "ruleObjectType": "User" }, { "ruleObjectId":
"S-1-5-21-1459593717-2655996711-1404495803-3562", "ruleObjectName": "user_88_4@rltest.com", "ruleObjectType":
"User" }, { "ruleObjectId": "S-1-5-21-1459593717-2655996711-1404495803-3479", "ruleObjectName":
"user_20@rltest.com", "ruleObjectType": "User" }, { "ruleObjectId":
"S-1-5-21-1459593717-2655996711-1404495803-1188", "ruleObjectName": "user_59@rltest.com", "ruleObjectType":
"User" } ] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	internal error

Get User Group

This URL gets the user group rule objects.

Resource URL

GET /ruleobject/usergroup

Request Parameters

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
UserGroupRuleObjectResponseList	List of user group	Array

Details of object in UserRuleObjectResponseList:

Field Name	Description	Data Type
ruleObjectId	Rule object id	String
ruleObjectName	Rule object name	String
ruleObejctType	Rule object type	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ruleobject/usergroup

Response

```
{ "userGroupRuleObjectResponseList": [ { "ruleObjectId": "S-1-5-21-1459593717-2655996711-1404495803-520",
"ruleObjectName": "Group Policy Creator Owners@rltest.com", "ruleObjectType": "User Group" }, { "ruleObjectId":
"S-1-5-21-1459593717-2655996711-1404495803-3570", "ruleObjectName": "DFSgroup_2@rltest.com", "ruleObjectType":
"User Group" }, { "ruleObjectId": "S-1-5-21-1459593717-2655996711-1404495803-3606", "ruleObjectName":
"myDFSgroup_1@rltest.com", "ruleObjectType": "User Group" }, { "ruleObjectId":
"S-1-5-21-1459593717-2655996711-1404495803-498", "ruleObjectName": "Enterprise Read-only Domain
Controllers@rltest.com", "ruleObjectType": "User Group" }, { "ruleObjectId":
"S-1-5-21-1459593717-2655996711-1404495803-572", "ruleObjectName": "Denied RODC Password Replication
Group@rltest.com", "ruleObjectType": "User Group" }, { "ruleObjectId": "S-1-2-32-551-0-0-0", "ruleObjectName":
"Backup Operators@rltest.com", "ruleObjectType": "User Group" }, { "ruleObjectId": "S-1-2-32-562-0-0-0",
"ruleObjectName": "Distributed COM Users@rltest.com", "ruleObjectType": "User Group" } ] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	internal error

Add Firewall Policy

This URL adds a new firewall policy and access rules.

Resource URL

POST /firewallpolicy

Request Parameters

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`FirewallPolicyId`	Unique firewall policy id, not required for POST	Number	No
`Name`	Policy name	String	Yes
`DomainId`	Id of domain to which this firewall policy belongs to	Number	Yes
`VisibleToChild`	Policy visible to child domain	Boolean	Yes
`Description`	Firewall policy description	String	No
`LastModifiedTime`	Last modified time of the firewall policy, not required for POST	String	No
`IsEditable`	Policy is editable or not	Boolean	Yes
`PolicyType`	Policy type, can be "ADVANCED" / "CLASSIC"	String	Yes
`PolicyVersion`	Policy version, not required for POST	Number	No
`LastModifiedUser`	Latest user that modified the policy, not required for POST	String	No
`MemberDetails`	Firewall rules in the policy	Object	Yes

Details of MemberDetails:

Field Name	Description	Data Type	Mandatory
`MemberRuleList`	List of firewall rules in the policy	Array	Yes

Details of fields in MemberRuleList

Field Name	Description	Data Type	Mandatory
`Description`	Rule description	String	Yes

Field Name	Description	Data Type	Mandatory
`Enabled`	Is rule enabled or not	Boolean	Yes
`Response`	Action to be performed if the traffic matches this rule. Can be " SCAN" / "DROP" / "DENY" / "IGNORE" / "STATELESS_IGNORE" / "STATELESS_DROP" / "REQUIRE_AUTHENTICATION"	String	Yes
`isLogging`	Is logging enabled for this rule	Boolean	Yes
`Direction`	Rule direction, can be "INBOUND" / "OUTBOUND" / "EITHER"	String	Yes
`SourceAddressObjectList`	Source address rule object list	Array	Yes
`SourceUserObjectList`	Source user rule object list	Array	Yes
`DestinationAddressObjectList`	Destination address rule object list	Array	Yes
`ServiceObjectList`	Service rule object list	Array	Yes
`ApplicationObjectList`	Application rule object list	Array	Yes
`TimeObjectList`	Time rule object list	Array	Yes

Details of SourceAddressObjectList and DestinationAddressObjectList:

Field Name	Description	Data Type	Mandatory
`RuleObjectId`	Unique rule object id	String	Yes
`Name`	Rule object name	String	Yes
`RuleObjectType`	Source/destination mode. Can be "COUNTRY" / "HOST_DNS_NAME" / "HOST_IPV_4" / "HOST_IPV_6" / "IPV_4_ADDRESS_RANGE" / "IPV_6_ADDRESS_RANGE" / "NETWORK_IPV_4" / "NETWORK_IPV_6" / "NETWORK_GROUP"	String	Yes

Details of SourceUserObjectList:

Field Name	Description	Data Type	Mandatory
`RuleObjectId`	Unique rule object id	String	Yes
`Name`	Rule object name	String	Yes

Field Name	Description	Data Type	Mandatory
`RuleObjectType`	Source user. Can be "USER" / "USER_GROUP"	String	Yes

Details of ServiceObjectList and ApplicationObjectList:

Field Name	Description	Data Type	Mandatory
`RuleObjectId`	Unique service rule object id	String	Yes
`Name`	Rule object name	String	Yes
`RuleObjectType`	Servic/application mode. Can be "APPLICATION" / "APPLICATION_GROUP" / "APPLICATION_ON_CUSTOM_PORT" / "SERVICE" / "SERVICE_GROUP"	String	Yes
`ApplicationType`	Application type. Can be "DEFAULT" / "CUSTOM"	String	Yes

Details of TimeObjectList:

Field Name	Description	Data Type	Mandatory
`RuleObjectId`	Unique service rule object id	String	Yes
`Name`	Rule object name	String	Yes
`RuleObjectType`	Time mode. Can be "FINITE_TIME_PERIOD" / "RECURRING_TIME_PERIOD" / "RECURRING_TIME_PERIOD_GROUP"	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique ID of the created subinterface	Integer

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/firewallpolicy

```
{ "Name" : "TestFirewallPolicy", "DomainId" : 0, "VisibleToChild" : true, "Description" : "test the
firewallpolicy", "LastModifiedTime" : "2012-12-12 12:30:47", "IsEditable" : true, "PolicyType" : "ADVANCED",
"PolicyVersion" : 1, "LastModifiedUser" : "admin", "MemberDetails" : { "MemberRuleList" : [{ "Description" :
"Test Member Rule", "Enabled" : true, "Response" : "SCAN", "IsLogging" : false, "Direction" : "INBOUND",
"SourceAddressObjectList" : [{ "RuleObjectId" : "AF", "Name" : "Afghanistan", "RuleObjectType" : "COUNTRY" } ],
"DestinationAddressObjectList" : [{ "RuleObjectId" : "101", "Name" : "hostDNSRule", "RuleObjectType" :
"HOST_DNS_NAME" }, { "RuleObjectId" : "102", "Name" : "hostIpv4", "RuleObjectType" : "HOST_IPV_4" },
{ "RuleObjectId" : "103", "Name" : "ipv4Addressrange", "RuleObjectType" : "IPV_4_ADDRESS_RANGE" },
{ "RuleObjectId" : "104", "Name" : "networkgroup", "RuleObjectType" : "NETWORK_GROUP" } ],
"SourceUserObjectList" : [{ "RuleObjectId" : "-1", "Name" : "Any", "RuleObjectType" : "USER" } ],
"ServiceObjectList" : [], "ApplicationObjectList" : [{ "RuleObjectId" : "1308991488", "Name" : "100bao",
"RuleObjectType" : "APPLICATION", "ApplicationType" : "DEFAULT" }, { "RuleObjectId" : "106", "Name" :
"applicaionOncutomPort", "RuleObjectType" : "APPLICATION_ON_CUSTOM_PORT", "ApplicationType" : "CUSTOM" },
{ "RuleObjectId" : "105", "Name" : "applicationgroup", "RuleObjectType" : "APPLICATION_GROUP",
"ApplicationType" : "CUSTOM" } ], "TimeObjectList" : [{ "RuleObjectId" : "107", "Name" : "finiteTimePeriod",
"RuleObjectType" : "FINITE_TIMING_PERIOD" }, { "RuleObjectId" : "108", "Name" : "recuringTimePeriod",
"RuleObjectType" : "RECURRING_TIME_PERIOD" }, { "RuleObjectId" : "109", "Name" : "recurringTimeperiodGroup",
"RuleObjectType" : "RECURRING_TIME_PERIOD_GROUP" } ] } ] } }
```

Response

```
{ "createdResourceId":120 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	404	1105	Invalid domain
3	400	1702	Invalid rule object type
4	400	1804	Maximum of 10 rule objects are allowed in each object list of an advanced firewall/QoS policy
5	400	1805	Multiple rule objects in a single source/ destination object list is not supported for a classic firewall policy
6	400	1806	Only host IPV4/network IPV4 type rule objects are supported for classic firewall policy
7	400	1807	Only service type rule object is supported for classic firewall policy
8	400	1808	Time object list is not applicable for classic firewall policy
9	400	1809	Application object list is not applicable for classic firewall policy
10	400	1810	Multiple rule objects in a single service object list is not supported for a classic firewall policy
11	400	1811	Policy type cannot be modified from advanced to classic
12	400	1812	Deny response is applicable for TCP traffic only

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
13	400	1813	Source/destination object list is not provided
14	400	1814	Service/application object list is not provided
15	400	1815	Time object list is not provided
16	400	1816	Firewall policy name is required
17	400	1817	For stateless action, application object list is not applicable
18	400	1818	Unsupported firewall policy type
19	406	1819	Stateless response with any/TCP/IP protocol no. 6/default services are not allowed
20	400	1820	Is logging should not be enabled for stateless action
21	400	1821	Either application or service object list can be defined in a member rule for an advanced firewall policy
22	400	1822	Composite rule object(Multiple items in a rule object) is allowed for advanced firewall policy only
23	400	1824	Source user object list is not applicable for classic firewall policy
24	400	1825	Source address object list is not applicable for classic firewall policy
25	400	1826	Destination address object list is not applicable for classic firewall policy

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
26	400	1827	Firewall policy with the same name was defined
27	400	1829	Name must contain only letters, numerical, spaces, commas, periods, hyphens or underscore
28	400	1830	Firewall policy name should not be greater than 40 chars
29	400	1831	Firewall policy provided is not upto date
30	400	1832	Source address and destination address object list cannot combine IPV6 rule objects with host IPV4, network IPV4, IPV4 address range, country and host DNS name rule objects
31	400	1833	Require authentication is valid only when source user object list is set to any
32	400	1834	Require authentication is valid only when HTTP (default service) is selected
33	400	1835	Firewall policy description should not be greater than 255 chars
34	400	1836	Member rule description should not be greater than 64 chars
35	400	1837	Source user object list is not provided
36	400	1838	Time object list can contain one finite time period

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
37	400	1839	Stateless response with source user or source user group rule objects are not allowed

Update Firewall Policy

This URL updates the firewall policy details.

Resource URL

PUT /firewallpolicy/<policy_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`policy_id`	Firewall policy id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`FirewallPolicyId`	Unique firewall policy id	Number	No
`Name`	Policy name	String	Yes
`DomainId`	Id of domain to which this firewall policy belongs to	Number	Yes
`VisibleToChild`	Policy visible to child domain	Boolean	Yes
`Description`	Firewall policy description	String	No
`LastModifiedTime`	Last modified time of the firewall policy	String	Yes
`IsEditable`	Policy is editable or not	Boolean	Yes
`PolicyType`	Policy type, can be "ADVANCED" / "CLASSIC"	String	Yes
`PolicyVersion`	Policy version	Number	Yes
`LastModifiedUser`	Last user that modified the policy	String	Yes
`MemberDetails`	Member firewall rules in the policy	Object	Yes

Details of MemberDetails:

Field Name	Description	Data Type	Mandatory
MemberRuleList	List of firewall rules in the policy	Array	Yes

Details of fields in MemberRuleList

Field Name	Description	Data Type	Mandatory
Description	Rule description	String	Yes
Enabled	Is rule enabled or not	Boolean	Yes
Response	Action to be performed if the traffic matches this rule. Can be "SCAN" / "DROP" / "DENY" / "IGNORE" / "STATELESS_IGNORE" / "STATELESS_DROP" / "REQUIRE_AUTHENTICATION"	String	Yes
isLogging	Is logging enabled for this rule	Boolean	Yes
Direction	Rule direction, can be "INBOUND" / "OUTBOUND" / "EITHER"	String	Yes
SourceAddressObjectList	Source address rule object list	Array	Yes
SourceUserObjectList	Source user rule object list	Array	Yes
DestinationAddressObjectList	Destination address rule object list	Array	Yes
ServiceObjectList	Service rule object list	Array	Yes
ApplicationObjectList	Application rule object list	Array	Yes
TimeObjectList	Time rule object list	Array	Yes

Details of SourceAddressObjectList and DestinationAddressObjectList:

Field Name	Description	Data Type	Mandatory
RuleObjectId	Unique rule object id	String	Yes
Name	Rule object name	String	Yes
RuleObjectType	Source/destination mode. Can be "COUNTRY" / "HOST_DNS_NAME" / "HOST_IPV_4" / "HOST_IPV_6" / "IPV_4_ADDRESS_RANGE" / "IPV_6_ADDRESS_RANGE" / "NETWORK_IPV_4" /	String	Yes

Field Name	Description	Data Type	Mandatory
	"NETWORK_IPV_6" / "NETWORK_GROUP"		

Details of SourceUserObjectList:

Field Name	Description	Data Type	Mandatory
RuleObjectId	Unique rule object id	String	Yes
Name	Rule object name	String	Yes
RuleObjectType	Source user. Can be "USER" / "USER_GROUP"	String	Yes

Details of ServiceObjectList and ApplicationObjectList:

Field Name	Description	Data Type	Mandatory
`RuleObjectId`	Unique service rule object id	String	Yes
`Name`	Rule object name	String	Yes
`RuleObjectType`	Service/application mode. Can be "APPLICATION" / "APPLICATION_GROUP" / "APPLICATION_ON_CUSTOM_PORT" / "SERVICE" / "SERVICE_GROUP"	String	Yes
`ApplicationType`	Application type. Can be "DEFAULT" / "CUSTOM"	String	Yes

Details of TimeObjectList:

Field Name	Description	Data Type	Mandatory
`RuleObjectId`	Unique service rule object id	String	Yes
`Name`	Rule object name	String	Yes
`RuleObjectType`	Time mode. Can be "FINITE_TIME_PERIOD" / "RECURRING_TIME_PERIOD" / "RECURRING_TIME_PERIOD_GROUP"	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Update status	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/firewallpolicy/120

Payload:

```
{ "FirewallPolicyId" : 120, "Name" : "TestFirewallPolicy", "DomainId" : 0, "VisibleToChild" : true,
"Description" : "test the firewallpolicy", "LastModifiedTime" : "2012-12-12 12:32:44", "IsEditable" : true,
"PolicyType" : "ADVANCED", "PolicyVersion" : 1, "LastModifiedUser" : "admin", "MemberDetails" :
{ "MemberRuleList" : [{ "Description" : "Test Member Rule", "Enabled" : true, "Response" : "IGNORE",
"IsLogging" : false, "Direction" : "OUTBOUND", "SourceAddressObjectList" : [{ "RuleObjectId" : "AF", "Name" :
"Afghanistan", "RuleObjectType" : "COUNTRY" } ], "DestinationAddressObjectList" : [{ "RuleObjectId" : "101",
"Name" : "hostDNSRule", "RuleObjectType" : "HOST_DNS_NAME" }, { "RuleObjectId" : "102", "Name" : "hostIpv4",
"RuleObjectType" : "HOST_IPV_4" }, { "RuleObjectId" : "103", "Name" : "ipv4Addressrange", "RuleObjectType" :
"IPV_4_ADDRESS_RANGE" }, { "RuleObjectId" : "104", "Name" : "networkgroup", "RuleObjectType" :
"NETWORK_GROUP" } ], "SourceUserObjectList" : [{ "RuleObjectId" : "-1", "Name" : "ANY", "RuleObjectType" :
"USER" } ], "ServiceObjectList" : [], "ApplicationObjectList" : [{ "RuleObjectId" : "1308991488", "Name" :
"100bao", "RuleObjectType" : "APPLICATION", "ApplicationType" : "DEFAULT" }, { "RuleObjectId" : "106", "Name" :
"applicaionOncutomPort", "RuleObjectType" : "APPLICATION_ON_CUSTOM_PORT", "ApplicationType" : "CUSTOM" },
{ "RuleObjectId" : "105", "Name" : "applicationgroup", "RuleObjectType" : "APPLICATION_GROUP",
"ApplicationType" : "CUSTOM" } ], "TimeObjectList" : [{ "RuleObjectId" : "107", "Name" : "finiteTimePeriod",
"RuleObjectType" : "FINITE_TIMING_PERIOD" }, { "RuleObjectId" : "108", "Name" : "recuringTimePeriod",
"RuleObjectType" : "RECURRING_TIME_PERIOD" }, { "RuleObjectId" : "109", "Name" : "recurringTimeperiodGroup",
"RuleObjectType" : "RECURRING_TIME_PERIOD_GROUP" } ] } ] } }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	404	1105	Invalid domain
3	400	1702	Invalid rule object type
4	400	1801	Invalid firewall policy Id/ firewall policy not visible to this domain
5	400	1804	Maximum of 10 rule objects are allowed in each object list of an advanced firewall/QoS policy
6	400	1805	Multiple rule objects in a single source/destination object list is not supported for a classic firewall policy
7	400	1806	Only host IPV4/network IPV4 type rule objects are supported for classic firewall policy
8	400	1807	Only service type rule object is supported for classic firewall policy
9	400	1808	Time object list is not applicable for classic firewall policy

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
10	400	1809	Application object list is not applicable for classic firewall policy
11	400	1810	Multiple rule objects in a single Service object list is not supported for a classic firewall policy
12	400	1811	Policy type cannot be modified from advanced to classic
13	400	1812	Deny response is applicable for TCP traffic only
14	400	1813	Source/destination object list is not provided
15	400	1814	Service/application object list is not provided
16	400	1815	Time object list is not provided
17	400	1816	Firewall policy name is required
18	400	1817	For stateless action, application object list is not applicable
19	400	1818	Unsupported firewall policy type
20	406	1819	Stateless response with any/TCP/IP protocol no.6/ default services are not allowed
21	400	1820	Is logging should not enabled for stateless action
22	400	1821	Either application or service object list can be defined in a member rule for an advanced firewall policy
23	400	1822	Composite rule object(Multiple items in a rule object) is allowed for advanced firewall policy only
24	400	1824	Source user object list is not applicable for classic firewall policy

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
25	400	1825	Source address object list is not applicable for classic firewall policy
26	400	1826	Destination address object list is not applicable for classic firewall policy
27	400	1827	Firewall policy with the same name was defined
28	400	1828	Invalid firewall policy
29	400	1829	Name must contain only letters, numerical, spaces, commas, periods, hyphens or underscore
30	400	1830	Firewall policy name should not be greater than 40 chars
31	400	1831	Firewall policy provided is not upto date
32	400	1832	Source address and destination address object list cannot combine IPV6 rule objects with host IPV4, network IPV4, IPV4 address range, country and host DNS name rule objects
33	400	1833	Require authentication is valid only when source user object list is set to any
34	400	1834	Require authentication is valid only when HTTP (default service) is selected
35	400	1835	Firewall policy description should not be greater than 255 chars
36	400	1836	Member rule description should not be greater than 64 chars
37	400	1837	Source user object list is not provided
38	400	1838	Time object list can contain one finite time period
39	400	1839	Stateless response with source user or source user

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
			group rule objects are not allowed

Delete Firewall Policy

This URL deletes the specified firewall policy.

Resource URL

DELETE /firewallpolicy/<policy_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
policy_id	Policy id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Update status	Number

Example

Request

DELETE https://%3CNSM_IP%3E/sdkapi/firewallpolicy/120

Response

```
{ "status":1 }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1801	Invalid firewall policy id/ firewall policy not visible to this domain

Get Firewall Policy

This URL gets the firewall policy details.

Resource URL

GET /firewallpolicy/<policy_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
policy_id	Policy id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
FirewallPolicyId	Unique firewall policy id	Number
Name	Policy name	String
DomainId	Id of domain to which this firewall policy belongs to	Number
VisibleToChild	Policy visible to child domain	Boolean
Description	Firewall policy description	String
LastModifiedTime	Last modified time of the firewall policy	String
IsEditable	Policy is editable or not	Boolean
PolicyType	Policy type, can be "ADVANCED" / "CLASSIC"	String
PolicyVersion	Policy version	Number
LastModifiedUser	Last user that modified the policy	String
MemberDetails	Member firewall rules in the policy	String

Details of MemberDetails:

Field Name	Description	Data Type
MemberRuleList	List of firewall rules in the policy	Array

Details of fields in MemberRuleList:

Field Name	Description	Data Type
Description	Rule description	String
Enabled	Is rule enabled or not	Boolean
Response	Action to be performed if the traffic matches this rule. Can be "SCAN" / "DROP" / "DENY" / "IGNORE" / "STATELESS_IGNORE" / "STATELESS_DROP" / "REQUIRE_AUTHENTICATION"	String
IsLogging	Is logging enabled for this rule	Boolean

Field Name	Description	Data Type
Direction	Rule direction, can be "INBOUND" / "OUTBOUND" / "EITHER"	String
SourceAddressObjectList	Source address rule object list	Array
SourceUserObjectList	Source user rule object list	Array
DestinationAddressObjectList	Destination address rule object list	Array
ServiceObjectList	Service rule object list	Array
ApplicationObjectList	Application rule object list	Array
TimeObjectList	Time rule object list	Array

Details of SourceAddressObjectList and DestinationAddressObjectList:

Field Name	Description	Data Type
RuleObjectId	Unique rule object id	String
Name	Rule object name	String
RuleObjectType	Source/destination mode. Can be "COUNTRY" / "HOST_DNS_NAME" / "HOST_IPV_4" / "HOST_IPV_6" / "IPV_4_ADDRESS_RANGE" / "IPV_6_ADDRESS_RANGE" / "NETWORK_IPV_4" / "NETWORK_IPV_6" / "NETWORK_GROUP"	String

Details of SourceUserObjectList:

Field Name	Description	Data Type
RuleObjectId	Unique rule object id	String
Name	Rule object name	String
RuleObjectType	Source user. Can be "USER" / "USER_GROUP"	String

Details of ServiceObjectList and ApplicationObjectList:

Field Name	Description	Data Type
RuleObjectId	Unique service rule object id	String
Name	Rule object name	String
RuleObjectType	Service/application mode. Can be "APPLICATION" / "APPLICATION_GROUP" /	String

Field Name	Description	Data Type
	"APPLICATION_ON_CUSTOM_PORT" / "SERVICE" / "SERVICE_GROUP"	
`ApplicationType`	Application type. Can be "DEFAULT" / "CUSTOM"	String

Details of TimeObjectList:

Field Name	Description	Data Type
`RuleObjectId`	Unique service rule object id	String
`Name`	Rule object name	String
`RuleObjectType`	Time mode. Can be "FINITE_TIME_PERIOD" / "RECURRING_TIME_PERIOD" / "RECURRING_TIME_PERIOD_GROUP"	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/firewallpolicy/120

Response

```
{ "FirewallPolicyId" : 120, "Name" : "TestFirewallPolicy", "DomainId" : 0, "VisibleToChild" : true,
"Description" : "test the firewallpolicy", "LastModifiedTime" : "2012-12-12 12:43:54", "IsEditable" : true,
"PolicyType" : "ADVANCED", "PolicyVersion" : 1, "LastModifiedUser" : "admin", "MemberDetails" :
{ "MemberRuleList" : [{ "Description" : "Test Member Rule", "Enabled" : true, "Response" : "IGNORE",
"IsLogging" : false, "Direction" : "OUTBOUND", "SourceAddressObjectList" : [{ "RuleObjectId" : "AF", "Name" :
"Afghanistan", "RuleObjectType" : "COUNTRY" } ], "DestinationAddressObjectList" : [{ "RuleObjectId" : "101",
"Name" : "hostDNSRule", "RuleObjectType" : "HOST_DNS_NAME" }, { "RuleObjectId" : "102", "Name" : "hostIpv4",
"RuleObjectType" : "HOST_IPV_4" }, { "RuleObjectId" : "103", "Name" : "ipv4Addressrange", "RuleObjectType" :
"IPV_4_ADDRESS_RANGE" }, { "RuleObjectId" : "104", "Name" : "networkgroup", "RuleObjectType" :
"NETWORK_GROUP" } ], "SourceUserObjectList" : [{ "RuleObjectId" : "-1", "Name" : "ANY", "RuleObjectType" :
"USER" } ], "ServiceObjectList" : [], "ApplicationObjectList" : [{ "RuleObjectId" : "1308991488", "Name" :
"100bao", "RuleObjectType" : "APPLICATION", "ApplicationType" : "DEFAULT" }, { "RuleObjectId" : "106", "Name" :
"applicaionOncutomPort", "RuleObjectType" : "APPLICATION_ON_CUSTOM_PORT", "ApplicationType" : "CUSTOM" },
{ "RuleObjectId" : "105", "Name" : "applicationgroup", "RuleObjectType" : "APPLICATION_GROUP",
"ApplicationType" : "CUSTOM" } ], "TimeObjectList" : [{ "RuleObjectId" : "107", "Name" : "finiteTimePeriod",
"RuleObjectType" : "FINITE_TIMING_PERIOD" }, { "RuleObjectId" : "108", "Name" : "recuringTimePeriod",
"RuleObjectType" : "RECURRING_TIME_PERIOD" }, { "RuleObjectId" : "109", "Name" : "recurringTimeperiodGroup",
"RuleObjectType" : "RECURRING_TIME_PERIOD_GROUP" } ] } ] } }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	404	1801	Invalid firewall policy id/ firewall policy not visible to this domain

Get Firewall Policies in a Domain

This URL gets the list of firewall policies defined in a particular domain.

Resource URL

GET /domain/<domain_id>/ firewallpolicy

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`FirewallPoliciesForDomainResponseList`	List of firewall policies defined in the domain	Array

Details of FirewallPoliciesForDomainResponseList:

Field Name	Description	Data Type
`policyName`	Name of the firewall policy	String
`VisibleToChild`	Is policy visible to child domains	Boolean
`Description`	Policy description	String
`IsEditable`	Is policy editable or not	Number
`lastModUser`	Last user that modified the policy	String
`PolicyType`	Policy type, can be "ADVANCED" or "CLASSIC"	String
`policyId`	Firewall policy unique id	Number
`domainId`	Domain id	Number
`policyVersion`	Policy version	Number

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/domain/0/firewallpolicy

Response

```
{ "FirewallPoliciesForDomainResponseList": [{ "policyId": 107, "policyName": "Port_FirewallPolicy", "domainId":
0, "visibleToChild": false, "description": "Firewall Policy for Port", "isEditable": true, "policyType":
"CLASSIC", "policyVersion": 1, "lastModUser": "admin" }, { "policyId": 105, "policyName":
"Interface_FirewallPolicy", "domainId": 0, "visibleToChild": true, "description": "Firewall Policy for
Interface", "isEditable": true, "policyType": "ADVANCED", "policyVersion": 1, "lastModUser": "admin" },
{ "policyId": 103, "policyName": "Sensor_Post_FirewallPolicy", "domainId": 0, "visibleToChild": false,
"description": "Firewall Policy for Sensor Post", "isEditable": true, "policyType": "CLASSIC", "policyVersion":
1, "lastModUser": "admin" }, { "policyId": 101, "policyName": "Sensor_Pre_FirewallPolicy", "domainId": 0,
"visibleToChild": true, "description": "Firewall Policy for Sensor Pre", "isEditable": true, "policyType":
"ADVANCED", "policyVersion": 1, "lastModUser": "admin" }] }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Create a New Scanning Exception at Sensor

This URL creates a new scanning exception at specified domain.

Resource URL

```
POST /sensor/<sensor_id>/scanningexception
```

Request Parameters

URL Parameters:

Field Name	Description	Data Type
`sensor_id`	Sensor id	Number

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`ScanningExceptionDetailsElement`	Object that contains the details of the field to be sent	Object	Yes

Details of fields in ScanningExceptionDetailsElement:

Field Name	Description	Data Type	Mandatory
`scanningExceptionDetails`	Object that contains the details of the field to be sent	Object	Yes

Details of fields in scanningExceptionDetails:

Field Name	Description	Data Type	Mandatory
`forwardType`	Can be one of these: TCP/UDP/VLAN	String	Yes
`portInfo`	Contains the TCP/UDP port informations	Object	No
`vlanInfo`	Contains the VLAN information	Object	No

Either of portInfo or vlanInfo must be provided.

Details of fields in portInfo:

Field Name	Description	Data Type	Mandatory
portRange	Contains the port range information	Object	No
portNumber	Contains the port number information	Object	No

Either of portRange or portNumber must be given.

Details of fields in portRang :

Field Name	Description	Data Type	Mandatory
`from`	Object that contains start port value	Object	Yes
`To`	Object that contains end port value	Object	Yes

Details of fields in from:

Field Name	Description	Data Type	Mandatory
`value`	Start port value	Number	Yes

Details of fields in to:

Field Name	Description	Data Type	Mandatory
`value`	End port value	Number	Yes

Details of fields in portNumber:

Field Name	Description	Data Type	Mandatory
`value`	Specified port value	Number	Yes

Details of fields in vlanInfo:

Field Name	Description	Data Type	Mandatory
`portPairName`	Name of the port pair on which scanning exception of vlan type should be created	Object	Yes
`vlanIds`	Contains the vlan information	Object	Yes

Details of fields in vlanIds:

Field Name	Description	Data Type	Mandatory
`vlanRange`	Contains the vlan range information	Object	No
`vlanId`	Contains the vlan id information	Object	No

Either of vlanRange or vlanId must be given.

Details of fields in vlanRange:

Field Name	Description	Data Type	Mandatory
`from`	Object that contains start vlan id	Object	Yes
`To`	Object that contains end vlan id	Object	Yes

Details of fields in from:

Field Name	Description	Data Type	Mandatory
`value`	Start vlan id	Number	Yes

Details of fields in to:

Field Name	Description	Data Type	Mandatory
`value`	End vlan id	Number	Yes

Details of fields in vlanId:

Field Name	Description	Data Type	Mandatory
`value`	Specified vlan id	Number	Yes

Response Parameters

Following fields are returned if the request parameters and payload are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/sensor/%3Csensor_id%3E/scanningexception

Payload

```
{ "scanningExceptionDetails": { "forwardType":"TCP", "portInfo": { "portRange": { "from": { "value":"103" },
"to": { "value":"110" } } } } }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1501	Scanning exception is not supported for the specified Sensor

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
2	400	1502	Please provide port info object
3	400	1503	Please provide either port range or port id object
4	400	1504	Please provide from and to both objects
5	400	1505	FROM is greater than TO
6	400	1506	VLAN ID should be between 1 and 4095
7	400	1507	Please provide vlan ids object
8	400	1508	Please provide either vlan range or vlan id object
9	400	1509	Port number should be between 1 and 65535
10	400	1510	Please provide Vlan info object
11	400	1511	Invalid port pair name
12	400	1512	Port pair name is required
13	400	1106	Invalid Sensor

Get Scanning Exception details on a Sensor

This URL gets the scanning exception on a Sensor.

Resource URL

GET /sensor/<sensor_id>/scanningexception

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensor_id	Sensor Id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type
ScanningExceptionResponseElement	Object that contains the details of the field to be sent	Object

Details of fields in ScanningExceptionResponseElement:

Field Name	Description	Data Type
tcpRules	Object containing TCP rule settings	Object
udpRules	Object containing UDP rule settings	Object
vlanRules	Object containing VLAN rule settings	Object

Details of fields in tcpRules:

Field Name	Description	Data Type
tcpPortRangeList	List of objects containing TCP port range setting	Object

Details of object in tcpPortRangeList:

Field Name	Description	Data Type
tcpPortRange	TCP port range in format "from-to"	String

Details of fields in udpRules:

Field Name	Description	Data Type
udpPortRangeList	List of objects containing UDP port range setting	Object

Details of object in udpPortRangeList:

Field Name	Description	Data Type
udpPortRange	UDP port range in format "from-to"	String

Details of fields in vlanRules:

Field Name	Description	Data Type
vlanIdRangeList	List of objects containing UDP port range setting	Object

Details of object in vlanIdRangeList:

Field Name	Description	Data Type
vlanIdRange	Vlan Id range in format "from-to"	String

Field Name	Description	Data Type
portPairName	Name of the port pair	String

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/sensor/%3Csensor_id%3E/scanningexception

Payload

```
{ "tcpRules": { "tcpPortRangeList": [ { "tcpPortRange": "100-100" }, { "tcpPortRange": "103-110" } ] },
"udpRules": { "udpPortRangeList": [ { "udpPortRange": "10-10" } ] }, "vlanRules": { "vlanIdRangeList":
[ { "vlanIdRange": "15-20", "portPairName": "1A-1B" } ] } }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1501	Scanning exception is not supported for the specified Sensor
2	400	1106	Invalid Sensor

Delete Scanning Exception on a Sensor

This URL deletes the scanning exception on a Sensor.

Resource URL

DELETE /sensor/<sensor_id>/scanningexception

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensor_id	Sensor id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`ScanningExceptionDeleteElement`	Object that contains the details of the field to be sent	Object	Yes

Details of fields in ScanningExceptionResponseElement:

Field Name	Description	Data Type	Mandatory
`tcpPortRangeElement`	Object containing TCP port range	Object	No
`udpPortRangeElement`	Object containing UDP port range	Object	No
`vlanIdRangeElement`	Object containing VLAN id range	Object	No

Either of the above three fields be provided at a time.

Details of fields in tcpPortRangeElement:

Field Name	Description	Data Type	Mandatory
`tcpPortRange`	TCP port range in format "from-to"	String	Yes

Details of fields in udpPortRangeElement:

Field Name	Description	Data Type	Mandatory
`udpPortRange`	UDP port range in format "from-to"	String	Yes

Details of fields in vlanIdRangeElement:

Field Name	Description	Data Type	Mandatory
`vlanIdRange`	Vlan Id range in format "from-to"	String	Yes
`portPairName`	Name of the port pair	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/sensor/<sensor_id>/scanningexception

Payload

```
{ "tcpPortRangeElement": { "tcpPortRange":"10-20" } }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1501	Scanning exception is not supported for the specified Sensor
2	400	1106	Invalid Sensor
3	400	1503	Provided settings does not exists

Enable/Disable Scanning Exception on a Sensor

This URL enables/disables the scanning exception on a Sensor.

Resource URL

PUT /sensor/<sensor_id>/scanningexception/status

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`ScanningExceptionStatusElement`	Object that contains the details of the field to be sent	Object	Yes

Details of fields in ScanningExceptionStatusElement:

Field Name	Description	Data Type	Mandatory
`enabled`	Can be either true or false	Boolean	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/<sensor_id>/scanningexception/status

Payload

```
{ "enabled":true }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1501	Scanning exception is not supported for the specified Sensor
2	400	1106	Invalid Sensor

Get Scanning Exception Status on a Sensor

This URL gets the scanning exception status on a Sensor.

Resource URL

GET /sensor/<sensor_id>/scanningexception/status

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`ScanningExceptionStatusElement`	Object that contains the details of the field to be sent	Object

Details of fields in ScanningExceptionStatusElement:

Field Name	Description	Data Type
enabled	Can be either true or false	Boolean

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/<sensor_id>/scanningexception/status

Response

```
{ "enabled":true }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1501	Scanning exception is not supported for the specified Sensor
2	400	1106	Invalid Sensor

Quarantine Host

This URL quarantines a Host for a particular duration on the specified Sensor.

Resource URL

POST /sensor/<sensor_id>/action/quarantinehost

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`IPAddress`	IPV4/IPV6 to be quarantined	String	Yes
`Duration`	Duration for which the -IP is to be quarantined. Can be "FIFTEEN_MINUTES" / "THIRTY_MINUTES" / "FORTYFIVE_MINUTES" / "SIXTY_MINUTES" / "FOUR_HOURS" / "EIGHT_HOURS" / "UNTIL_EXPLICITLY_RELEASED"	String	Yes
`remediate`	Remediate the IP along with quarantine	Boolean	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status returned	Number

Example

Request

POST https://<NSM_IP>/sdkapi/sensor/1001/action/quarantinehost

Payload:

```
{ "IPAddress": "102.102.102.102", "Duration": “EIGHT_HOURS” "remediate": true }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive
3	400	1406	Invalid IP format
4	409	2301	IP already quarantined
5	400	2302	Invalid duration
6	400	2305	IPV6 is not enabled on Sensor

Update IPS Quarantine Duration for a Host

This URL will update the quarantine duration for the specified host.

Resource URL

PUT /sensor/<sensor_id>/action/quarantinehost

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`IPAddress`	IPV4/IPV6 to be quarantined	String	Yes
`Duration`	Duration for which the quarantine needs to be extended for the specified IP, Can be "FIVE_MINUTES" / "FIFTEEN_MINUTES" / "THIRTY_MINUTES" / "FORTYFIVE_MINUTES" / "SIXTY_MINUTES" / "UNTIL_EXPLICITLY_RELEASED"	String	Yes
`IsOverride`	Override the previous data if present for the IP provided	Boolean	No
`remediate`	Remediate the IP along with quarantine. Considered only when override is selected.	Boolean	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status returned	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/sensor/1001/action/quarantinehost

```
Payload { "IPAddress": "102.102.102.102", "Duration": "THIRTY_MINUTES", "IsOverride": true, "remediate": true }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive
3	400	1406	Invalid IP format
4	400	2302	Invalid duration
5	400	2303	IP not quarantined
6	400	2304	IP already quarantined for infinite duration
7	400	2305	IPV6 is not enabled on Sensor

Release Quarantined Host

This URL releases the specified quarantined host.

Resource URL

DELETE /sensor/<sensor_id>/action/quarantinehost/<IPAddress>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes
`IPAddress`	IPV4/IPV6 address	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Status returned by deletion	Number

Example

Request

DELETE https://%3CNSM_IP%3E/sensor/1001/action/quarantinehost/102.102.102.102

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is Inactive
3	400	1406	Invalid IP format

Get Quarantined Hosts

This URL provides the list of Quarantined Hosts on the specific Sensor.

Resource URL

GET /sensor/<sensor_id>/action/quarantinehost

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensor_id	Sensor Id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
QuarantineHostDescriptor	List of quarantined hosts	Array

Details of object in QuarantineHostDescriptor:

Field Name	Description	Data Type
IPAddress	IPV4/IPV6 to be quarantined	String
Duration	End time (in NSM Server Timezone) when the IP will be released from quarantine	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/sensor/1001/action/quarantinehost

Response

```
{ "QuarantineHostDescriptor": [ { "IPAddress": "102.102.102.122", "Duration": 1350630974000 }, { "IPAddress":
"2607:f0d0:1002:0051:0000:0000:0000:0604", "Duration": 1350631900000 } ] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is Inactive

Get Quarantined Host Details

This URL provides the list of quarantined host and their details.

Resource URL

GET /sensor/<sensor_id>/action/quarantinehost/details

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id. Give -1 if all the quarantine hosts are needed	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`QuarantineHostDetails`	List of quarantined host with details	Array

Details of object in QuarantineHostDetails:

Field Name	Description	Data Type
`QuarantineHostDetail`	Quarantine hosts with details	Object

Details of object in QuarantineHostDetail:

Field Name	Description	Data Type
`ipAddress`	Quarantine host IP	String
`hostname`	Quarantine host name	String

Field Name	Description	Data Type
`os`	Operating system	String
`user`	User	String
`quarantineDetails`	Quarantine details	Object
`addedToQuarantine`	Details of when the host was quarantined	Object
`remediate`	Whether the IP is remediated	Boolean
`pendingRelease`	When the host will be released	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/-1/action/quarantinehost/details

Response

```
{ 'quarantineHostDetail': [{ 'ipAddress': '1.1.1.13', 'quarantineDetails': { 'device': 'admalware-1450',
'quarantineZone': 'Allow DNS' }, 'addedToQuarantine': { 'by': 'TFTP: Wvtftp Remote Heap Overflow', 'time': 'Dec
31 16:00 PST' }, 'remediate': true, 'pendingRelease': 'Explicit Release Required' }] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is Inactive

Add a New Connection Limiting Policy

This URL adds a new connection limiting policy.

Resource URL

POST /connectionlimitingpolicy

Request Parameters

Payload Parameters:

Field Name	Description	Data Type
`properties`	Object that contains the basic properties of the policy	Object
`connectionLimitingRules`	List of object that contains rules	Array

Details of fields in properties:

Field Name	Description	Data Type	Mandatory
`policyId`	Policy Id	Number	No
`name`	Policy name	String	Yes
`description`	Description of the policy	String	No
`domainId`	Domain Id	Number	Yes
`visibleToChild`	Is policy visible to child	Boolean	Yes
`lastModTimestamp`	Last modified time	String	No
`lastModUser`	Last modified user	String	No

Details of fields in connectionLimitingRules:

Field Name	Description	Data Type	Mandatory
`enabled`	Is rule enabled	Boolean	Yes
`description`	Description of the rule	String	No
`direction`	Can be one of these: INBOUND/OUTBOUND/ EITHER	String	Yes
`ruleType`	Can be one of these: GTI/ PROTOCOL	String	Yes
`thresholdType`	Can be one of these: CONNECTION_RATE/ ACTIVE_CONNECTIONS	String	Yes

Field Name	Description	Data Type	Mandatory
`thresholdValue`	A valid threshold value between 1 and 65535	Number	Yes
`externalReputation`	Should be provided when ruleType is GTI Can be one of these: HIGH_RISK/ MEDIUM_OR_HIGH_RISK/ UNVERIFIED_MEDIUM_OR_HIGH_RISK/ ANY	String	Yes
`externalLocation`	Should be provided when ruleType is GTI Can be either "Any" or one of the country from the list of country obtained using the URL: https://<NSM_IP>/sdkapi/ connectionlimitingpolicy/ countrylist	String	Yes
`serviceType`	Should be provided when ruleType is PROTOCOL. Can be one of these: TCP/UDP/ PING_ICMP_ECHO_REQ/ ALL_TCP_AND_UDP	String	Yes
`portNumber`	Should be provided when serviceType is TCP/UDP. A valid port number between 1 and 65535	Number	Yes
`response`	Can be one of these: ALERT_ONLY/ ALERT_AND_DROP_EXCESS_CONNECTIONS/ ALERT_AND_DENY_EXCESS_CONNECTIONS/ ALERT_AND_QUARANTINE	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique ID of the created policy	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/connectionlimitingpolicy

Payload

```
{ "properties": { "name": "Test_CLP1", "description": "CLP of Child Domain", "domainId": 101, "visibleToChild":
true }, "connectionLimitingRules": [ { "enabled": true, "description": "", "direction": "EITHER", "ruleType":
"PROTOCOL", "thresholdType": "CONNECTION_RATE", "thresholdValue": 1000, "externalReputation": null,
"externalLocation": "Any", "serviceType": "ALL_TCP_AND_UDP", "portNumber": null, "response": "ALERT_ONLY" } ] }
```

Response

```
{ "createdResourceId":104 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1903	Threshold type must be CONNECTION_RATE for ruletype GTI
2	400	1904	Cannot specify response DENY_EXCESS_CONNECTION for UDP and ICMP protocol
3	400	1905	Invalid name provided
4	400	1906	Please provide a domain id
5	400	1907	Please provide "visibleToChild" field
6	400	1908	Please provide "isEnabled" field
7	400	1909	Please provide direction
8	400	1910	Please provide threshold value
9	400	1911	Please provide rule type
10	400	1912	Please provide threshold type
11	400	1913	Please provide response type
12	400	1914	Please provide external reputation
13	400	1915	Policy name already in use
14	400	1916	Please provide port number in range 1-65535
15	400	1917	Please provide external location
16	400	1918	Invalid country name

Update a Connection Limiting Policy

This URL updates a connection limiting policy.

Resource URL

PUT /connectionlimitingpolicy/<policy_id>

Request Parameters

Payload Parameters:

Field Name	Description	Data Type
`properties`	Object that contains the basic properties of the policy	Object
`connectionLimitingRules`	List of object that contains rules	Array

Details of fields in properties:

Field Name	Description	Data Type	Mandatory
`policyId`	Policy Id	Number	No
`name`	Policy name	String	Yes
`description`	Description of the policy	String	No
`domainId`	Domain Id	Number	Yes
`visibleToChild`	Is policy visible to child	Boolean	Yes
`lastModTimestamp`	Last modified time	String	No
`lastModUser`	Last modified user	String	No

Details of fields in connectionLimitingRules:

Field Name	Description	Data Type	Mandatory
`enabled`	Is rule enabled	Boolean	Yes
`description`	Description of the rule	String	No
`direction`	Can be one of these: INBOUND/OUTBOUND/ EITHER	String	Yes
`ruleType`	Can be one of these: GTI/ PROTOCOL	String	Yes
`thresholdType`	Can be one of these: CONNECTION_RATE/ ACTIVE_CONNECTIONS	String	Yes
`thresholdValue`	A valid threshold value between 1 and 65535	Number	Yes
`externalReputation`	Should be provided when ruleType is GTI. Can be one of these: HIGH_RISK/ MEDIUM_OR_HIGH_RISK/ UNVERIFIED_MEDIUM_OR_HIGH_RISK/ ANY	String	Yes
`externalLocation`	Should be provided when ruleType is GTI. Can be either "Any" or one of the country	String	Yes

Field Name	Description	Data Type	Mandatory
	from the list of country obtained using the URL: https://<NSM_IP>/sdkapi/connectionlimitingpolicy/countrylist		
`serviceType`	Should be provided when ruleType is PROTOCOL. Can be one of these: TCP/UDP/PING_ICMP_ECHO_REQ/ALL_TCP_AND_UDP	String	Yes
`portNumber`	Should be provided when serviceType is TCP/UDP A valid port number between 1 and 65535	Number	Yes
`response`	Can be one of these: ALERT_ONLY/ALERT_AND_DROP_EXCESS_CONNECTIONS/ALERT_AND_DENY_EXCESS_CONNECTIONS/ALERT_AND_QUARANTINE	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/connectionlimitingpolicy/104

Payload

```
{ "properties": { "name": "Updated_Test_CLP1", "description": "CLP of Child Domain1", "domainId": 101,
"visibleToChild": false }, "connectionLimitingRules": [ { "enabled": true, "description": "", "direction":
"EITHER", "ruleType": "PROTOCOL", "thresholdType": "CONNECTION_RATE", "thresholdValue": 100,
"externalReputation": null, "externalLocation": "Any", "serviceType": "UDP", "portNumber": 123, "response":
"ALERT_AND_QUARANTINE" } ] }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1903	Threshold type must be CONNECTION_RATE for ruletype GTI

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
2	400	1904	Cannot specify response DENY_EXCESS_CONNECTION for UDP and ICMP protocol
3	400	1905	Invalid name provided
4	400	1906	Please provide a domain id
5	400	1907	Please provide "visibleToChild" field
6	400	1908	Please provide "isEnabled" field
7	400	1909	Please provide direction
8	400	1910	Please provide threshold value
9	400	1911	Please provide rule type
10	400	1912	Please provide threshold type
11	400	1913	Please provide response type
12	400	1914	Please provide external reputation
13	400	1915	Policy name already in use
14	400	1916	Please provide port number in range 1-65535
15	400	1917	Please provide external location
16	400	1918	Invalid country name

Get a Connection Limiting Policy

This URL gets a connection limiting policy.

Resource URL

GET /connectionlimitingpolicy/<policy_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`policy_id`	Policy id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`properties`	Object that contains the basic properties of the policy	Object
`connectionLimitingRules`	List of object that contains rules	Array

Details of fields in properties:

Field Name	Description	Data Type
`policyId`	Policy Id	Number
`name`	Policy name	String
`description`	Description of the policy	String
`domainId`	Domain Id	Number
`visibleToChild`	Is policy visible to child	Boolean
`lastModTimestamp`	Last modified time	String
`lastModUser`	Last modified user	String

Details of fields in connectionLimitingRules:

Field Name	Description	Data Type
`enabled`	Is rule enabled	Boolean
`description`	Description of the rule	String
`direction`	Can be one of these: INBOUND/ OUTBOUND/EITHER	String
`ruleType`	Can be one of these: GTI/PROTOCOL	String
`thresholdType`	Can be one of these: CONNECTION_RATE/ ACTIVE_CONNECTIONS	String
`thresholdValue`	A valid threshold value between 1 and 65535	Number
`externalReputation`	Will be returned when ruleType is GTI. Can be one of these: HIGH_RISK/ MEDIUM_OR_HIGH_RISK/ UNVERIFIED_MEDIUM_OR_HIGH_RISK/ANY	String
`externalLocation`	Will be returned when ruleType is GTI. Can be either "Any" or one of the country from the list of country obtained using the URL: https://<NSM_IP>/sdkapi/ connectionlimitingpolicy/countrylist	String

Field Name	Description	Data Type
serviceType	Will be returned when ruleType is PROTOCOL Can be one of these: TCP/UDP/PING_ICMP_ECHO_REQ/ ALL_TCP_AND_UDP	String
portNumber	Will be returned when serviceType is TCP/UDP A valid port number between 1 and 65535	Number
response	Can be one of these: ALERT_ONLY/ ALERT_AND_DROP_EXCESS_CONNECTIONS/ ALERT_AND_DENY_EXCESS_CONNECTIONS/ ALERT_AND_QUARANTINE	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/connectionlimitingpolicy/104

Response

```
{ "properties": { "policyId": 104, "name": "Updated_Test_CLP1", "description": "CLP of Child Domain1",
"domainId": 101, "visibleToChild": false, "lastModTimestamp": "2013-05-08 09:32:41", "lastModUser": "admin" },
"connectionLimitingRules": [ { "enabled": true, "description": "", "direction": "EITHER", "ruleType":
"PROTOCOL", "thresholdType": "CONNECTION_RATE", "thresholdValue": 100, "externalReputation": null,
"externalLocation": "Any", "serviceType": "UDP", "portNumber": 123, "response": "ALERT_AND_QUARANTINE" } ] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1901	Invalid connection limiting policy id/connection limiting policy not visible in this domain

Delete a Connection Limiting Policy

This URL deletes a connection limiting policy.

Resource URL

DELETE /connectionlimitingpolicy/<policy_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
policy_id	Policy id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

DELETE https://%3CNSM_IP%3E/sdkapi/connectionlimitingpolicy/104

Response

```
{ "status": 1 }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1901	Invalid connection limiting policy id/connection limiting policy not visible in this domain

Get the List of Available Countries

This URL gets the list of available countries.

Resource URL

GET /connectionlimitingpolicy/countrylist

Request Parameters

URL Parameters:

N/A

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`countryList`	List of country	Array

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/connectionlimitingpolicy/countrylist

Response

```
{ "countryList": [ "Afghanistan", "Aland Islands", "Albania", "Algeria", "American Samoa", "Andorra", "Angola",
"Anguilla", "Antarctica", "Antigua and Barbuda", "Argentina", "Armenia", "Aruba", "Asia/Pacific Region",
"Australia", "Austria", "Azerbaijan", "Bahamas", "Bahrain", "Bangladesh", "Barbados", "Belarus", "Belgium",
"Belize", "Benin", "Bermuda", "Bhutan", "Bolivia", "Bosnia and Herzegovina", "Botswana", "Bouvet Island",
"Brazil", "British Indian Ocean Territory", "Brunei Darussalam", "Bulgaria", "Burkina Faso", "Burundi",
"Cambodia", "Cameroon", "Canada", "Cape Verde", "Cayman Islands", "Central African Republic", "Chad", "Chile",
"China", "Christmas Island", "Cocos (Keeling) Islands", "Colombia", "Comoros", "Congo", "Congo, The Democratic
Republic of the", "Cook Islands", "Costa Rica", "Cote D'Ivoire", "Croatia", "Cuba", "Cyprus", "Czech Republic",
"Denmark", "Djibouti", "Dominica", "Dominican Republic", "Ecuador", "Egypt", "El Salvador", "Equatorial Guinea",
"Eritrea", "Estonia", "Ethiopia", "Europe", "Falkland Islands (Malvinas)", "Faroe Islands", "Fiji", "Finland",
"France", "France, Metropolitan", "French Guiana", "French Polynesia", "French Southern Territories", "Gabon",
"Gambia", "Georgia", "Germany", "Ghana", "Gibraltar", "Greece", "Greenland", "Grenada", "Guadeloupe", "Guam",
"Guatemala", "Guernsey", "Guinea", "Guinea-Bissau", "Guyana", "Haiti", "Heard Island and McDonald Islands",
"Holy See (Vatican City State)", "Honduras", "Hong Kong", "Hungary", "Iceland", "India", "Indonesia", "Iran,
Islamic Republic of", "Iraq", "Ireland", "Isle of Man", "Israel", "Italy", "Jamaica", "Japan", "Jersey",
"Jordan", "Kazakhstan", "Kenya", "Kiribati", "Korea, Democratic People's Republic of", "Kuwait", "Kyrgyzstan",
"Lao People's Democratic Republic", "Latvia", "Lebanon", "Lesotho", "Liberia", "Libya", "Liechtenstein",
"Lithuania", "Luxembourg", "Macau", "Macedonia", "Madagascar", "Malawi", "Malaysia", "Maldives", "Mali",
"Malta", "Marshall Islands", "Martinique", "Mauritania", "Mauritius", "Mayotte", "Mexico", "Micronesia,
Federated States of", "Moldova, Republic of", "Monaco", "Mongolia", "Montenegro", "Montserrat", "Morocco",
"Mozambique", "Myanmar", "Namibia", "Nauru", "Nepal", "Netherlands", "Netherlands Antilles", "New Caledonia",
"New Zealand", "Nicaragua", "Niger", "Nigeria", "Niue", "Norfolk Island", "Northern Mariana Islands", "Norway",
"Oman", "Pakistan", "Palau", "Palestinian Territory", "Panama", "Papua New Guinea", "Paraguay", "Peru",
"Philippines", "Pitcairn Islands", "Poland", "Portugal", "Puerto Rico", "Qatar", "Reunion", "Romania", "Russia",
"Rwanda", "Saint Barthelemy", "Saint Helena", "Saint Kitts and Nevis", "Saint Lucia", "Saint Martin", "Saint
Pierre and Miquelon", "Saint Vincent and the Grenadines", "Samoa", "San Marino", "Sao Tome and Principe", "Saudi
Arabia", "Senegal", "Serbia", "Seychelles", "Sierra Leone", "Singapore", "Slovakia", "Slovenia", "Solomon
Islands", "Somalia", "South Africa", "South Georgia and the South Sandwich Islands", "South Korea", "Spain",
"Sri Lanka", "Sudan", "Suriname", "Svalbard and Jan Mayen", "Swaziland", "Sweden", "Switzerland", "Syria",
"Taiwan", "Tajikistan", "Tanzania, United Republic of", "Thailand", "Timor-Leste", "Togo", "Tokelau", "Tonga",
"Trinidad and Tobago", "Tunisia", "Turkey", "Turkmenistan", "Turks and Caicos Islands", "Tuvalu", "Uganda",
"Ukraine", "United Arab Emirates", "United Kingdom", "United States", "United States Minor Outlying Islands",
"Uruguay", "Uzbekistan", "Vanuatu", "Venezuela", "Vietnam", "Virgin Islands, British", "Virgin Islands, U.S.",
"Wallis and Futuna", "Western Sahara", "Yemen", "Zambia", "Zimbabwe" ] }
```

Error Information

N/A

Get Connection Limiting Policies in a Domain

This URL gets all the connection limiting policies defined in the specific domain.

Resource URL

GET /domain/<domain_id>/connectionlimitingpolicies

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
ConnectionLimitingPolicyList	List of connection limiting policies with brief details	Array

Details of object in ConnectionLimitingPolicyList:

Field Name	Description	Data Type
policyId	Connection limiting policy id	Number
name	Policy name	String
description	Policy description	String
domainId	Id of domain to which this policy belongs to	Number
lastModUser	Policy last modified by user	String

Field Name	Description	Data Type
`visibleToChild`	Policy visible to child domain	Boolean
`lastModTimestamp`	Last modified timestamp of the policy	String

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/sensor/1001/interface/105/connectionlimitingpolicy/101

Response

```
{ "ConnectionLimitingPolicyList": [ { "policyId": 101, "name": "Test_CLP1", "description": "CLP of Parent
Domain1", "domainId": 0, "visibleToChild": true, "lastModTimestamp": "2012-07-24 00:19:00", "lastModUser":
"admin" }, { "policyId": 102, "name": "Test_CLP2", "description": "CLP of Parent Domain2", "domainId": 0,
"visibleToChild": false, "lastModTimestamp": "2012-07-24 00:19:19", "lastModUser": "admin" } ] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404		Invalid connection limiting policy Id

Add a Non-Standard Port at Domain Level

This URL adds a non-standard port on the specified domain.

Resource URL

GET /domain/<domain_id>/nonstandardports

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
NonStandardPortRequestElement	Non-standard port details	Object	Yes

Details of NonStandardPortRequestElement:

Field Name	Description	Data Type	Mandatory
Protocol	Application Protocol, can be TELNET / FTP / SMTP / DNS / HTTP / POP3 / RPC / IMAP / SNMP / LDAP / REXEC / RLOGIN / RSH / NFS	String	Yes
sslEnabled	SSL to be enabled for HTTP protocol, for other protocols this field must be false	Boolean	Yes
Transport	Transport protocol, can be TCP / UDP	String	Yes
nonStandardPortNumber	Non-standard port number, should not be set to the standard port numbers defined for the protocols	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Status returned	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/domain/0/nonstandardports

Payload

```
{ "protocol": "TELNET", "sslEnabled": "false", "transport": "TCP", "nonStandardPortNumber": "15" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Cod	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	2001	Only UDP transport type is allowed for SNMP/NFS protocol type
3	400	2002	SSL can be enabled only for HTTP protocol type
4	400	2003	Port number can be between 1 and 65535
5	400	2004	Non-standard port number cannot be same as the standard port number
6	400	2005	Non-standard port setting with the given details already exists

Add a Non-Standard Port at Sensor Level

This URL adds a non-standard port on the specified Sensor.

Resource URL

POST /sensor/<sensor_id>/nonstandardports

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`NonStandardPortRequestElement`	Non-standard port details	Object	Yes

Details of NonStandardPortRequestElement:

Field Name	Description	Data Type	Mandatory
`Protocol`	Application protocol, can be TELNET / FTP / SMTP / DNS / HTTP / POP3 / RPC / IMAP / SNMP / LDAP / REXEC / RLOGIN / RSH / NFS	String	Yes
`sslEnabled`	SSL to be enabled for HTTP protocol, for other protocols this field must be false	Boolean	Yes
`Transport`	Transport protocol, can be TCP / UDP	String	Yes
`nonStandardPortNumber`	Non-standard port number, should not be set to the standard port numbers defined for the protocols	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status returned	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/sensor/1002/nonstandardports

Payload

```
{ "protocol": "HTTP", "sslEnabled": "true", "transport": "UDP", "nonStandardPortNumber": "63" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	2001	Only UDP transport type is allowed for SNMP/NFS protocol type
3	400	2002	SSL can be enabled only for HTTP protocol type
4	400	2003	Port number can be between 1 and 65535

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
5	400	2004	Non-standard port number cannot be same as the standard port number
6	400	2005	Non-standard port setting with the given details already exists

Get Non-Standard Ports at Domain Level

This URL gets all the non-standard ports configured on the specified domain.

Resource URL

GET /domain/<domain_id>/nonstandardports

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain Id	Number	Yes

Response Parameter

Field Name	Description	Data Type
`NonStandardPortResponseList`	List of non-standard ports	Array

Details of object in NonStandardPortResponseList:

Field Name	Description	Data Type
`protocol`	"Protocol/Transport" pair	String
`portAssignment`	Array of assigned port numbers	Array

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/domain/0/nonstandardports

Response

```
{ "NonStandardPortResponseList": [ { "protocol": "FTP/TCP", "portAssignmentList": [ 21, 12, 32 ] },
{ "protocol": "TELNET/UDP", "portAssignmentList": [ 23, 555 ] } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Get Non-Standard Ports at Sensor Level

This URL gets all the non-standard ports configured on the specified Sensor.

Resource URL

GET /sensor/< sensor _id>/nonstandardports

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensor_id	Sensor Id	Number	Yes

Response Parameter

Field Name	Description	Data Type
NonStandardPortResponseList	List of non-standard ports	Array

Details of object in NonStandardPortResponseList:

Field Name	Description	Data Type
protocol	"Protocol/Transport" pair	String
portAssignment	Array of assigned port numbers	Array

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/sensor/1002/nonstandardports

Response

```
{ "NonStandardPortResponseList": [ { "protocol": "FTP/TCP", "portAssignmentList": [ 21, 12, 32 ] },
{ "protocol": "TELNET/UDP", "portAssignmentList": [ 23, 555, 15 ] }, ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor

Delete a Non-Standard Port at Domain Level

This URL deletes a non-standard port configured on the specified domain.

Resource URL

DELETE /domain/<domain_id>/nonstandardports?transport=<transport_type>&nonStandardPortNumber=<port_number>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes
`transport_type`	Transport Protocol, can be TCP / UDP	String	Yes
`port_number`	The non-standard port number to be deleted	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status returned	Number

Example

Request

DELETE https://%3CNSM_IP%3E/sdkapi/domain/101/nonstandardports?transport=TCP&nonStandardPortNumber=32

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	2006	Provided port number does not exists
3	400	2007	Standard ports cannot be deleted

Delete a Non-Standard Port at Sensor Level

This URL deletes a non-standard port defined on the specified Sensor.

Resource URL

DELETE /sensor/<sensor_id>/nonstandardports?transport=<transport_type>&nonStandardPortNumber=<port_number>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes
`transport_type`	Can be either TCP or UDP	String	Yes

Field Name	Description	Data Type	Mandatory
`port_number`	The non-standard port number to be deleted	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status returned	Number

Example

Request

DELETE https://%3CNSM_IP%3E/sdkapi/sensor/1002/nonstandardports?transport=UDP&nonStandardPortNumber=15

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	2006	Provided port number does not exists
3	400	2007	Standard ports cannot be deleted

Import SSL Key to the Manager

This URL imports the SSL key to the Manager for the Sensors other than 9.2 NS-series.

Resource URL

POST /sensor/<sensor_id>/action/sslkey

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensor_id	Sensor id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
MultiPart	Holds the body part objects	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the user credential object	Application/json object	Yes

Details of user credential:

Field Name	Description	Data Type	Mandatory
Alias Name	Alias name for the key file	String	Yes
Passphrase	Passphrase	String	Yes

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
BodyPart[1]	Holds the .p12 file as input stream	Application/octet-stream	Yes

Details of .p12 file:

Field Name	Description	Data Type	Mandatory
File	SSL key input stream	ByteArrayInput Stream	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Resource Id`	Created resource id	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/sensor/1001/action/sslkey

Payload:

```
PUT /sdkapi/sensor/1001/action/sslkey HTTP/1.1 NSM-SDK-API: ODlGRkEwQzEwMTE4QkFFRDc5MUUwMDk5OTg3OTI0NDk6MQ==
Accept: application/vnd.nsm.v1.0+json Content-Type: multipart/form-data;
boundary=Boundary_5_29812760_1360143901032 MIME-Version: 1.0 User-Agent: Java/1.6.0_25 Host: localhost:8888
Connection: keep-alive Content-Length: 3974 --Boundary_5_29812760_1360143901032 Content-Type: application/json
{"AliasName":"test5","PassPhrase":"admin123"} --Boundary_5_29812760_1360143901032 Content-Type: application/
octet-stream ÒrÝ?ü0¥ÿ<^}c,¢eXœ^:4 JhÍ2µ□rDYñÇÚd¶/Â¿í□F~ ÆIc§¼éá©ÿ_8Öø« C6Ô654îÞg‘J6?x ,*T2¡qhã4ÎÅVµGƒo9ŸCÒª„í¹Ì
—Áë&1¹ì,Ú‹y ì^î‘Vö5U.kÝ$±Ñ g§zï0□ wÌ [:…œ`Žíì’ DŒ¾¸xŒ7è□L“t"á}ñÕùA‡B6W¦P!;Ð?j*;G¾=X¦Š1s(□ì_œ8•¯Ð"®ƒMîQ,®UÉÔ
`7»©2xN£o†¾$h;Õe ÆÄŸ0ÀÑÄ¦ûNü,1”1Sõ±œ'n¨$èŒ`I¤@ã¥?$^hé_gÙÎ□4L[gàÏ©:•ŒÔ òH‰KÃïÃÒ"ÑÆ*¼²žØ|r-Þ„”¶K¥*¾□k}ddZ¡□ßÔ
¥dK9¥Ð¾ýÎk“{Oj□¬ ¾€ýb3ÔÏ&«PƒTF âê¡,4Â{0ä!ÈÝ]ðä[”¿1•!;d³_ --Boundary_5_29812760_1360143901032--
```

Response

```
{ "createdResourceId":1002 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1001	internal error
3	400	2202	Input stream read error
4	400	2203	Alias name already exist

Delete SSL Key

This URL deletes the SSL key from the Manager for the Sensors other than 9.2 NS series.

Resource URL

DELETE /sensor/<sensor_id>/action/sslkey/<ssl_id>

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status returned by deletion	Number

Example

Request

DELETE https://%3CNSM_IP%3E/sdkapi/sensor/1001/action/sslkey/1002

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive
3	404	2201	SSL id is invalid

Get SSL Keys

This URL gets the list of SSL keys imported for the specified Sensor and is applicable for Sensors other than 9.2 NS-series.

Resource URL

GET /sensor/<sensor_id>/action/sslkey

Request Parameters

URL parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor Id	Number	Yes

Response Parameters

Details of GetSSLResponseList:

Field Name	Description	Data Type
`SSLDescriptor`	List of SSL descriptor	Array

Details of SSLDescriptor:

Field Name	Description	Data Type
`Aliasname`	SSL alias name	String
`Status`	Status of the key	String
`SslId`	ID of the SSL key	Number
`LastImport`	Latest SSL key import date	String
`LastUpdate`	Latest SSL key update time	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/sensor/1001/action/sslkey

Response

```
{ "SSLDescriptor": [ { "AliasName": "admin1", "SslId": 1015, "Status": "Valid", "LastImport": "Thu Aug 02
17:37:33 IST 2012", "LastUpdate": "Thu Aug 02 17:37:33 IST 2012" } ] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive

Get the SSL Configuration

This URL gets the SSL configuration on the Sensor and is applicable for Sensors other than 9.2 NS-series.

Resource URL

GET / sensor/<sensor_id>/sslconfiguration

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensor_id	Sensor Id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
enableSSl	Enable SSL on Sensor	Boolean
currentStatus	Current status of Sensor	String
enablePktLogging	Enable packet logging on Sensor	Boolean
sslFlows	SSL flows enabled on Sensor	String
sslCacheTimer	SSL cache timer	String
maxConcurrentTCPUDPFlows	Maximum concurrent TCP-UDP flows allowed on Sensor	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/sensor/1002/sslconfiguration

Response

```
{ "enableSSl": true, "currentStatus": "Enabled[25000]", "enablePktLogging": false, "sslFlows": "25000",
"sslCacheTimer": "5", "maxConcurrentTCPUDPFlows": null }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive

Update the SSL Configuration

This URL updates the SSL configuration on Sensor and is applicable for Sensors other than 9.2 NS series.

Resource URL

PUT / sensor/<sensor_id>/sslconfiguration

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`enableSSl`	Enable SSL on Sensor	Boolean	Yes
`enablePktLogging`	Enable packet logging on Sensor	Boolean	No
`sslFlows`	SSL flows enabled on Sensor	String	No
`sslCacheTimer`	SSL cache timer	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1002/sslconfiguration

Payload

```
{ "enableSSl": true, "enablePktLogging": false, "sslFlows": "25000", "sslCacheTimer": "5", }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive
3	400	5401	FIPS enabled on Sensor
4	400	5402	0 is invalid to enter in SSL flows. Please disable SSL directly
5	400	5403	Flow should be between 100 and (maxFlow)
6	400	5404	SSL flow and SSL cache timer are numeric fields
7	400	5405	Maximum cache timer allowed is 9999
8	400	1153	SSL key decryption is not supported for this Sensor

Get the SSL Configuration at the Domain Level

This URL gets the SSL configuration at the domain level.

Resource URL

GET /domain/<domainId>/sslconfiguration

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain ID	Number	Yes

Response Parameters

Following fields are returned:

Field Name	Description	Data Type
`inheritSettings`	Inherit settings from parent domain.	Boolean
`decryptionState`	SSL state. Values can be: • DISABLED • INBOUND • OUTBOUND • PROXY_INBOUND (For Inbound Proxy) • PROXY_INBOUND_OUTBOUND (For Inbound and Outbound Proxy)	String

Field Name	Description	Data Type
`anticipatedSSLTrafficUsage`	Anticipated inbound SSL traffic usage. Values can be: • VERY_LIGHT • LIGHT • MEDIUM • HEAVY • VERY_HEAVY	String
`maxFlow`	Maximum flow allowed in a Sensor.	Number
`decryptedFlow`	Flows allocated to Sensor.	Number
`sslInactivityTimeoutInMinutes`	The maximum amount of time a Sensor will keep an outbound SSL flow open when no data is seen on the Sensor.	Number
`includeDecryptedPCAPS`	Include decrypted packets while packet capture.	Boolean
`enableDhSupport`	DH support	Boolean
`maxConcurrent`	Maximum concurrent connections allowed between a McAfee agent and a Sensor. The value can range from 1 to 1024.	Number
`permittedIPv4CIDRBlocks`	IPv4 CIDR blocks	Object
`permittedIPv6CIDRBlocks`	IPv6 CIDR blocks	Object
`failureHandling`	Failure handling	Object

Details of `permittedIPv4CIDRBlocks` and `permittedIPv6CIDRBlocks`:

Field Name	Description	Data Type
`id`	ID of the CIDR added	Number
`cidr`	CIDR block	String

Details of `failureHandling`:

Field Name	Description	Data Type
`untrustedOrExpiredServerCertificate`	Action to take if the target Web server's certificate is not on the sensor's trusted CA list. Used only in case of outbound SSL. The values can be: • Block flow • Decrypt	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/sslconfiguration

Response

```
{ "inheritSettings": false, "decryptionState": "INBOUND", "anticipatedSSLTrafficUsage": "VERY_HEAVY",
"sslInactivityTimeoutInMinutes": 6, "enableDhSupport": true, "maxConcurrent": 210, "permittedIPv4CIDRBlocks":
[ { "id": 428, "cidr": "4.4.4.4/32", "action": null }, { "id": 366, "cidr": "1.1.1.1/32", "action": null } ],
"permittedIPv6CIDRBlocks": [ { "id": 429, "cidr": "2001:0DB9:0000:0000:0000:0000:0000:0000/123", "action":
null }, { "id": 367, "cidr": "2001:0DB9:0000:0000:0000:0000:0000:0000/128", "action": null } ],
"includeDecryptedPCAPS": true }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	500	1001	Internal error

Update the SSL Configuration at the Domain Level

This URL updates the SSL configuration at the domain level.

Resource URL

PUT /domain/<domainId>/sslconfiguration

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainID`	Domain id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`inheritSettings`	Inherit settings from parent domain.	Boolean	Yes
`decryptionState`	SSL state. Values can be: • DISABLED • INBOUND • OUTBOUND • PROXY_INBOUND (For Inbound Proxy) • PROXY_INBOUND_OUTBOUND (For Inbound and Outbound Proxy)	String	Yes
`anticipatedSSLTrafficUsage`	Anticipated inbound SSL traffic usage. Values can be: • VERY_LIGHT • LIGHT	String	Yes

Field Name	Description	Data Type	Mandatory
	• MEDIUM • HEAVY • VERY_HEAVY		
`sslInactivityTimeoutInMinutes`	The maximum amount of time a Sensor will keep an outbound SSL flow open when no data is seen on the Sensor.	Number	Yes
`includeDecryptedPCAPS`	Include decrypted packets while packet capture.	Boolean	Yes
`enableDhSupport`	DH support	Boolean	
`maxConcurrent`	Maximum concurrent connections allowed between a McAfee agent and a Sensor. The value can range from 1 to 1024.	Number	Yes
`permittedIPv4CIDRBlocks`	IPv4 CIDR blocks	Object	Yes
`permittedIPv6CIDRBlocks`	IPv6 CIDR blocks	Object	Yes
`failureHandling`	Failure handling	Object	Yes

Details of `permittedIPv4CIDRBlocks` and `permittedIPv6CIDRBlocks`.

Field Name	Description	Data Type	Mandatory
`action`	Action for the CIDR. The values can be "delete" for deletion.	Number	No
`cidr`	CIDR block	String	Yes

Details of `failureHandling`.

Field Name	Description	Data Type	Mandatory
`untrustedOrExpiredServerCertificate`	Action to take if the target web server's certificate is not on the Sensor's trusted CA list. Used only in case of outbound SSL. The values can be: • Block flow • Decrypt	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/sslconfiguration

Payload

```
{ "inheritSettings": false, "decryptionState": "INBOUND", "anticipatedSSLTrafficUsage": "HEAVY",
"sslInactivityTimeoutInMinutes": 1, "enableDhSupport": true, "maxConcurrent": 210, "permittedIPv4CIDRBlocks":
[{"cidr":"10.1.1.0/23"}], "permittedIPv6CIDRBlocks": [{"cidr":"2001:DB9::1/122"}], "decryptedFlow": 20,
"includeDecryptedPCAPS": false }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	500	1001	Internal error

Get the Re-sign Certificates on the Manager

This URL gets the re-sign certificates available on the Manager.

Resource URL

GET /domain/sslconfiguration/resigncert

Request Parameters

URL Parameters: None

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`certificate`	Re-sign certificate details	Object list

Details of `certificate`.

Field Name	Description	Data Type
`commonName`	Common name for certificate	String
`issuedBy`	Issued by name	String
`validity`	Validity duration of the certificate	String
`validityStatus`	Validity status of the certificate	String
`keyLength`	Key length of the certificate	String
`digest`	Digest for the certificate	String
`generated`	Generated by name	String

Field Name	Description	Data Type
`certType`	Type of the certificate. It can be "Default" or "Custom".	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/sslconfiguration/resigncert

Response

```
{ "certificate": [ { "commonName": "Default 1024-bit Trusted Re-Signing Certificate", "issuedBy": "Network
Security Platform", "validity": "2016-09-26 - 2020-09-25", "validityStatus": "VALID", "keyLength": "1024",
"digest": "SHA256withRSA", "generated": "2016-10-19 11:56:07.0 ( System )", "certType": "Defaut" } ] }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Regenerate the Default Re-sign Certificate

This URL regenerates the default re-sign certificate available on the Manager.

Resource URL

GET /domain/sslconfiguration/generateresigncert

Request Parameters

URL Parameters: None

Query Parameters: None

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation is successful	Number

Example

Request

GET https://<NSM_IP>/sdkapi/domain/sslconfiguration/generateresigncert

Response

```
{ "status": 1 }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Export the Public Key of the Active Re-sign Certificate

This URL exports the public key of the active re-sign certificate available on the Manager.

Resource URL

GET /domain/sslconfiguration/exportresigncert

Request Parameters

URL Parameters: None

Query Parameters: None

Response Parameters

Returns the public key.

Example

Request

GET https://<NSM_IP>/sdkapi/domain/sslconfiguration/exportresigncert

Response

<public key>

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Import a Custom Re-sign Certificate

This URL imports a custom re-sign certificate to the Manager.

Resource URL

PUT /domain/sslconfiguration/importresigncert

Request Parameters

URL Parameters: None

Query Parameters: None

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`MultiPart`	Holds the body part objects	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
`BodyPart[0]`	Holds the Import re-sign certificate object	Application/json object	Yes

Details of ImportResignCert:

Field Name	Description	Data Type	Mandatory
`fileName`	Name of the file	String	Yes
`passphrase`	Passphrase for the key	String	Yes

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
`BodyPart[1]`	Holds the .p12 file as an input stream	Application/octet-stream	Yes

Details of .p12 file:

Field Name	Description	Data Type	Mandatory
`File`	The SSL key file data	ByteArrayInputStream	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation is successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/sslconfiguration/importresigncert

Payload

```
----Boundary_1_12424925_1353496814940 Content-Type: application/json {"passPhrase": "admin123", "fileName":
"test.p12"} ----Boundary_1_12424925_1353496814940 Content-Type: application/octet-stream <file_data> ----
Boundary_1_12424925_1353496814940—
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	5301	Invalid file type given for import: The file name does not have any extension
3	400	5301	Invalid file type given for import expected is .p12 while <fileType> was provided

Get all the Trusted CA Certificates on the Manager

This URL gets all the trusted CA certificates available on the Manager.

Resource URL

GET /domain/sslconfiguration/trustedcerts

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`trustedCerts`	List of all the trusted certificates	Array

Details of objects in trustedCerts:

Field Name	Description	Data Type
`state`	State of the certificate. It can be enabled or disabled.	Boolean
`alias`	Alias for the SSL key	String
`issuedBy`	Name of the issuer	String
`fileName`	Certificate file name	String
`certType`	Type of the certificate. It can be "Default" or "Custom".	String
`validity`	Validity details	Object
`lastUpdated`	Last update details	Object

Details of the validity object:

Field Name	Description	Data Type
`from`	Validity from date	String
`to`	Validity end date	String
`status`	Status of the validity. The values can be: • VALID • EXPIRING • EXPIRED	String

Details of the lastUpdated object:

Field Name	Description	Data Type
`time`	Last update time	String
`by`	Last updated by user	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/sslconfiguration/trustedcerts

Response

```
{ "trustedCerts": [ { "state": true, "alias": "IGC/A", "issuedBy": "IGC/A", "fileName": null, "certType":
"Defaut", "validity": { "from": "2002-12-13 19:59:23.0", "to": "2020-10-17 19:59:22.0", "status": "VALID" },
"lastUpdated": { "time": "2016-10-20 11:48:15.0", "by": "System" } }, { "state": true, "alias": "EC-ACC",
"issuedBy": "EC-ACC", "fileName": null, "certType": "Defaut", "validity": { "from": "2003-01-08 04:30:00.0",
"to": "2031-01-08 04:29:59.0", "status": "VALID" }, "lastUpdated": { "time": "2016-10-20 11:48:15.0", "by":
"System" } }, ……. ] }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Get a Single Trusted CA Certificate on the Manager

This URL gets a single trusted CA certificate details available on the Manager.

Resource URL

GET /domain/sslconfiguration/trustedcert?alias=<alias>

Request Parameters

URL Parameters: None

Query Parameters:

Field Name	Description	Data Type	Mandatory
alias	The certificate alias	String	No

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
state	State of the certificate. It can be enabled or disabled.	Boolean
alias	Alias for the SSL key	String
issuedBy	Name of the issuer	String
fileName	Certificate file name	String
certType	Type of the certificate. It can be "Default" or "Custom".	String
validity	Validity details	Object
lastUpdated	Last update details	Object

Details of the validity object:

Field Name	Description	Data Type
`from`	Validity from date	String
`to`	Validity end date	String
`status`	Status of the validity. The values can be: • VALID • EXPIRING • EXPIRED	String

Details of the lastUpdated object:

Field Name	Description	Data Type
`time`	Last update time	String
`by`	Last updated by user	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/sslconfiguration/trustedcert?alias=EC-ACC

Response

```
{ "state": true, "alias": "EC-ACC", "issuedBy": "EC-ACC", "fileName": null, "certType": "Defaut", "validity":
{ "from": "2003-01-08 04:30:00.0", "to": "2031-01-08 04:29:59.0", "status": "VALID" }, "lastUpdated": { "time":
"2016-10-20 11:48:15.0", "by": "System" } }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Enable or Disable Multiple Trusted CA Certificates

This URL enables or disables multiple trusted CA certificates.

Resource URL

PUT /domain/sslconfiguration/updatetrustedcertstate

Request Parameters

URL Parameters: None

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`alias`	List of alias names which needs to be updated	Array	Yes
`state`	Enable or disable the alias	Boolean	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation is successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/sslconfiguration/updatetrustedcertstate

Payload

```
{ "alias": ["alias1", "alias2"], "state": true }
```

Response

```
{ "status:1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	2203	Alias does not exist

Update the Default Trusted CA Certificates

This URL updates the default trusted CA certificates available on the Manager.

Resource URL

GET /domain/sslconfiguration/updatedefaulttrustedcerts

Request Parameters

URL Parameters: None

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation is successful	Number

Example

Request

GET https://<NSM_IP>/sdkapi/domain/sslconfiguration/updatedefaulttrustedcerts

Response

```
{ "status:1 }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Import a Custom Trusted CA Certificate

This URL imports a custom trusted CA certificate to the Manager.

Resource URL

PUT /domain/sslconfiguration/importtrustedcert

Request Parameters

URL Parameters: None

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`MultiPart`	Holds the body part objects	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
`BodyPart[0]`	Holds the Import re-sign certificate object	Application/json object	Yes

Details of ImportResignCert:

Field Name	Description	Data Type	Mandatory
`fileName`	Name of the file	String	Yes

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
`BodyPart[1]`	Holds the .pem file as an input stream	Application/octet-stream	Yes

Details of .pem file:

Field Name	Description	Data Type	Mandatory
`File`	The SSL key file data	ByteArrayInputStream	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation is successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/sslconfiguration/importtrustedcert

Payload

```
----Boundary_1_12424925_1353496814940 Content-Type: application/json { "fileName": "test.pem"} ----
Boundary_1_12424925_1353496814940 Content-Type: application/octet-stream <file_data> ----
Boundary_1_12424925_1353496814940—
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	5301	Invalid file type given for import: The file name does not have any extension
3	400	5301	Invalid file type given for import expected is .pem while <fileType> was provided

Delete Multiple Trusted CA Certificates

This URL deletes multiple trusted CA certificates on the Manager.

Resource URL

DELETE /domain/sslconfiguration/deletetrustedcerts

Request Parameters

URL Parameters: None

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`alias`	List of alias names which needs to be deleted	Array	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation is successful	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/domain/sslconfiguration/deletetrustedcerts

Payload

```
{ "alias": [“alias1”, “alias2”] }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	2203	Certificates with following alias are not present: <alias_list>
3	400	2203	Following certificates are default and cannot be deleted: <alias_list>

Get all the Internal Web Server Certificates

This URL gets all the internal web server certificates available on the Manager.

Resource URL

GET /domain/sslconfiguration/internalwebservercerts

Request Parameters

URL Parameters: None

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`internalWebServerCerts`	List of all the internal web server certificates	Array

Details of objects in internalWebServerCerts:

Field Name	Description	Data Type
`id`	State of the certificate file. If enabled or not.	Boolean
`alias`	Alias for the SSL key	String
`issuedBy`	Name of the issuer	String
`fileName`	Certificate file name	String

Field Name	Description	Data Type
`validity`	Certificate validity details	Object
`installOn`	List of Sensors on which the key is installed	Array
`lastUpdated`	Last update details	Object

Details of validity:

Field Name	Description	Data Type
`from`	Validity from date	String
`to`	Validity end date	String
`status`	Status of the validity. Values can be: • VALID • EXPIRING • EXPIRED	String

Details of lastUpdated:

Field Name	Description	Data Type
`time`	Last update time	String
`by`	Last updated by user	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/sslconfiguration/internalwebservercerts

Response

```
{ "internalWebServerCerts": [ { "id": 1008, "alias": "a", "issuedBy": "a", "fileName": "KEYSTORE.p12",
"validity": { "from": "Thu Aug 11 00:00:00 IST 2016", "to": "Wed Nov 09 00:00:00 IST 2016", "status":
"EXPIRING" }, "installOn": [ "/My Company/NS-RD-7200" ], "lastUpdated": { "time": "Tue Oct 18 23:06:32 IST
2016", "by": "admin" } } ] }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Import Custom Internal Web Server Certificate

This URL imports custom internal web server certificate.

Resource URL

PUT /domain/sslconfiguration/importinternalwebservercerts

Request Parameters

URL Parameters: None

Payload Parameters:

Field Name	Description	Data Type	Mandatory
MultiPart	Holds the body part objects	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the import internal web server certificate (ImportIWSCert) object	Application/json object	Yes

Details of ImportIWSCert:

Field Name	Description	Data Type	Mandatory
fileName	List of names of the file	Array	Yes
passphrase	Passphrase for the files provided	String	Yes
sensorId	List of Sensor id's on which to import	Array	No

Details of BodyPart[1] to BodyPart[<length of filename list provided above>]:

Field Name	Description	Data Type	Mandatory
BodyPart[1]	Holds the .p12 file as input stream	Application/octet-stream	Yes

Details of .p12 file:

Field Name	Description	Data Type	Mandatory
File	The SSL key file data	ByteArrayInputStream	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	List of the status of imports	Array

Details of objects in status:

Field Name	Description	Data Type
fileName	File name which was imported	String

Field Name	Description	Data Type
status	Status is the import was successful	Boolean
comment	Comments regarding the import	String

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/sslconfiguration/importinternalwebservercerts

Payload

```
----Boundary_1_12424925_1353496814940 Content-Type: application/json { "fileName": [ "test.p12", “test1.p12”,
“test2.p12”]} ----Boundary_1_12424925_1353496814940 Content-Type: application/octet-stream <file_data for test.
12> ----Boundary_1_12424925_1353496814940 Content-Type: application/octet-stream <file_data for test1.12> ----
Boundary_1_12424925_1353496814940 Content-Type: application/octet-stream <file_data for test2.12> ----
Boundary_1_12424925_1353496814940—
```

Response

```
{ "status": [ { “filename”: “test.p12”, “status”: true, “comment”:”Operation successful for file : test.p12 on
following sensors : [1002, 1003]” }, { “filename”: “test1.p12”, “status”: true, “comment”:”Operation successful
for file : test1.p12 on following sensors : [1002, 1003]” }, { “filename”: “test2.p12”, “status”: true,
“comment”:”Operation successful for file : test2.p12 on following sensors : [1002, 1003]” } ] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	5301	Invalid file type given for import : The file name does not have any extension
3	400	5301	Invalid file type given for import expected is .pem while <fileType> was provided
4	400	2002	No outbound SSL supported Sensors present
5	400	2002	Issue with the payload. Number of file data provided is not same as the files provided

Delete Multiple Internal Web Server Certificates

This URL deletes multiple internal web server certificates.

Resource URL

DELETE /domain/sslconfiguration/deleteinternalwebservercerts

Request Parameters

URL Parameters: None

Payload parameters:

Field Name	Description	Data Type	Mandatory
`alias`	List of file names which needs to be deleted	Array	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation is successful	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/domain/sslconfiguration/deleteinternalwebservercerts

Payload

```
{ "alias": [“test.p12”, “test1.p12”] }
```

Response

```
{ "status:1 }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Get All Inbound Proxy Rules

This URL gets all the inbound proxy rules created on the Manager.

Resource URL

GET /domain/sslconfiguration/inboundproxyrules

Request Parameters

URL Parameters: None

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`sslInboundProxyRuleList`	List of all the SSL inbound proxy rule	Array

Details of objects in sslInboundProxyRuleList:

Field Name	Description	Data Type
`ruleId`	Rule id	Number

Field Name	Description	Data Type
`ruleName`	Rule name	String
`comment`	Comment	String
`destWebServerIPs`	Web server IPs	String
`webServerCerts`	List of web server certificates	Object
`installOn`	List of Sensors on which the list of web server certificates are installed	Array
`defaultKey`	Default list of web server certificates	Object
`lastUpdated`	Last update details.	Object

Details of the defaultKey:

Field Name	Description	Data Type
`validityStatus`	Validity status of web server certificate	String
`keyAlias`	Alias for web server certificate	String

Details of the lastUpdated:

Field Name	Description	Data Type
`time`	Last update time	String
`by`	Last updated by user	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/sslconfiguration/inboundproxyrules

Response

```
{ "SSLInboundProxyRuleList": [ { "ruleId": 5, "ruleName': "InboundProxyRule2", "comment": "Rule 2",
"destWebServerIPs": "10.213.0.0/16" "webServerCerts": [{"validityStatus": "VALID", "keyAlias":
"NSAT_521_1024_SHA384"}], "installedOn": ["/Test Child Domain 1/NS9500_2"], "defaultKey': {"validityStatus":
"VALID", "keyAlias": "NSAT_521_1024_SHA384"}, "lastUpdated": {"by": "admin", "time": "2019-10-22
12:50:58.0"}, }}, "ruleId": 6, "ruleName': "InboundProxyRule3", "comment": "Rule 3", "destWebServerIPs":
"10.213.23.0/24" "webServerCerts": [{"validityStatus": "VALID", "keyAlias": "NSAT_522_1024_SHA384"}],
"installedOn": ["/Test Child Domain 1/NS9500_1"], "defaultKey': {"validityStatus": "VALID", "keyAlias":
"NSAT_522_1024_SHA384"}, "lastUpdated": {"by": "admin", "time": "2019-10-23 12:54:58.0"}, }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Get Inbound Proxy Rule Details

This URL gets detail of the given inbound proxy rule id.

Resource URL

GET /domain/sslconfiguration/inboundproxyruledetail/<ruleId>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`ruleId`	Rule id	Integer	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`ruleId`	Rule id	Number
`ruleName`	Rule name	String
`comment`	Comment	String
`destWebServerIPs`	Web server IPs	String
`webServerCerts`	List of web server certificates	Object
`installOn`	List of Sensors on which the list of web server certificates are installed	Array
`defaultKey`	Default list of web server certificates	Object
`lastUpdated`	Last update details	Object

Details of the web server certificate and defaultKey:

Field Name	Description	Data Type
`validityStatus`	Validity status of web server certificate	String
`keyAlias`	Alias for web server certificate	String

Details of the lastUpdated:

Field Name	Description	Data Type
`time`	Last update time	String
`by`	Last updated by user	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/sslconfiguration/inboundproxyruledetail/5

Response

```
{ “ruleId”: 5, “ruleName': “InboundProxyRule2”, “comment”: “Rule 2”, “destWebServerIPs”: “10.213.0.0/16”
“webServerCerts”: [{“validityStatus”: “VALID”, “keyAlias”: “NSAT_521_1024_SHA384”}], “installedOn”: [“/Test
Child Domain 1/NS9500_2”], “defaultKey': {“validityStatus”: “VALID”, “keyAlias”: “NSAT_521_1024_SHA384”},
“lastUpdated”: {“by”: “admin”, “time”: “2019-10-22 12:50:58.0”}, }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	500	2002	Rule id is invalid
3	500	2002	Inbound proxy rule with given name not found

Add Inbound Proxy Rule

This URL adds an inbound proxy rule.

Resource URL

POST domain/sslconfiguration/inboundproxyrules

Request Parameters

URL Parameters: None

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`ruleName`	Rule name	String	Yes
`comment`	Comment	String	No
`destWebServerIPs`	Destination web server IPs (CIDR)	String	Yes
`webServerCerts`	List of web server certificates (All the web server certificates should be installed on exact same set of Sensors)	Object	Yes
`defaultKey`	Default web server certificates (should be one of the web server certificates. If not given, any one of the web server certificates will be considered as default key.)	Object	No

Details of the web server certificate and defaultKey:

Field Name	Description	Data Type
`validityStatus`	Validity status of web server certificate	String
`keyAlias`	Alias for web server certificate	String

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
createdResourceId	Unique id of the created inbound proxy rule	Number

Example

Request

POST https://<NSM_IP>/sdkapi/domain/sslconfiguration/inboundproxyrules

Payload

```
{ “ruleName': “InboundProxyRule2”, “comment”: “Rule 2”, “destWebServerIPs”: “10.213.0.0/16” “webServerCerts”:
[{“keyAlias”: “NSAT_521_1024_SHA384”}], “defaultKey': {“keyAlias”: “NSAT_521_1024_SHA384”} }
```

Response

```
{ "createdResourceId": 5 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	2002	Rule name already exist. Please add a unique name.
2	500	2002	Invalid destination web server IPs
3	500	2002	Destination web server IPs field is required
4	500	2002	Addition not allowed.
5	500	2002	Rule name: field should not be empty
6	500	2002	At least one web server certificate is required.
7	500	2002	Rule name: The maximum length for the field is 254
8	500	2002	Maximum length for the comment is 254
9	500	2002	Key Alias does not exist Invalid
10	500	2002	InstalledOn set does not match

Update Inbound Proxy Rule

This URL updates inbound proxy rule.

Resource URL

PUT domain/sslconfiguration/inboundproxyrules/<ruleId>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`ruleId`	Rule id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`ruleName`	Rule name	String	Yes
`comment`	Comment	String	No
`destWebServerIPs`	Destination web server IPs (CIDR)	String	Yes
`webServerCerts`	List of web server certificates (All the web server certificates should be installed on exact same set of sensors)	Object	Yes
`defaultKey`	Default web server certificates (should be one of the web server certificates. If not given, any one of the web server certificates will be considered as default key.)	Object	No

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number
`ruleId`	Rule id after update	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/sslconfiguration/inboundproxyrules/5

Payload

```
{ “ruleName': “InboundProxyRule2”, “comment”: “Rule 2”, “destWebServerIPs”: “10.213.0.0/16” “webServerCerts”:
[{“keyAlias”: “NSAT_521_1024_SHA384”}], “defaultKey': {“keyAlias”: “NSAT_521_1024_SHA384”} }
```

Response

```
{ "status": 1 “ruleId”: 10 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	2002	Rule name already exist. Please add a unique name.
2	500	2002	Invalid destination web server IPs
3	500	2002	Destination web server IPs field is required
4	500	2002	Addition not allowed.
5	500	2002	Rule name: field should not be empty
6	500	2002	At least one web server certificate is required.
7	500	2002	Rule name: The maximum length for the field is 254
8	500	2002	Maximum length for the comment is 254
9	500	2002	Key alias does not exist Invalid
10	500	2002	InstalledOn set does not match

Delete Multiple Inbound Proxy Rules

This URL deletes multiple inbound proxy rules.

Resource URL

DELETE /domain/sslconfiguration/inboundproxyrules

Request Parameters

URL Parameters: None

Payload parameters:

Field Name	Description	Data Type	Mandatory
`ruleIds`	List of rule Ids which needs to be deleted	Array	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation is successful	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/domain/sslconfiguration/inboundproxyrules

Payload

```
{ " ruleIds ": [5,6] }
```

Response

```
{ "status:1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	500	2002	Rule id is invalid

Get the SSL Configuration at the Sensor Level

This URL gets the SSL configuration at the Sensor level for 9.2 NS-series Sensors.

Resource URL

GET /sensor/<sensorId>/decryptionsettings

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Following fields are returned.

Field Name	Description	Data Type
`inheritSettings`	Inherit settings from parent domain	Boolean
`decryptionState`	SSL state. The values can be: • DISABLED • INBOUND • OTBOUND	String
`anticipatedSSLTrafficUsageAnticipate`	Anticipated inbound SSL traffic usage. The values can be: • VERY_LIGHT • LIGHT • MEDIUM • HEAVY • VERY_HEAVY	String
`maxFlow`	Maximum flow allowed in the Sensor.	Number

Field Name	Description	Data Type
`decryptedFlow`	Flows allocated to the Sensor.	Number
`sslInactivityTimeoutInMinutes`	The maximum amount of time a Sensor will keep an outbound SSL flow open when no data has been seen on the Sensor.	Number
`includeDecryptedPCAPS`	Include decrypted packets while packet capture.	Boolean
`enableDhSupport`	DH support	Boolean
`maxConcurrent`	Maximum concurrent connection allowed between a McAfee agent and a Sensor. The value can range from 1 to 1024.	Number
`permittedIPv4CIDRBlocks`	IPv4 CIDR blocks	Object
`permittedIPv6CIDRBlocks`	IPv6 CIDR blocks	Object

Details of permittedIPv4CIDRBlocks and permittedIPv6CIDRBlocks:

Field Name	Description	Data Type
`id`	ID of CIDR added	Number
`cidr`	CIDR block	String

Details of failureHandling:

Field Name	Description	Data Type
`untrustedOrExpiredServerCertificate`	Action to take if the target web server's certificate is not on the Sensor's trusted CA list. Used only in case of outbound SSL. The value can be: • Block flow • Decrypt	Number

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/decryptionsettings

Response

```
{ "inheritSettings": false, "decryptionState": "INBOUND", "anticipatedSSLTrafficUsage": "VERY_HEAVY",
"sslInactivityTimeoutInMinutes": 6, "maxFlow": 1600000, "enableDhSupport": true, "maxConcurrent": 210,
"permittedIPv4CIDRBlocks": [ { "id": 428, "cidr": "4.4.4.4/32", "action": null }, { "id": 366, "cidr":
"1.1.1.1/32", "action": null } ], "permittedIPv6CIDRBlocks": [ { "id": 429, "cidr":
"2001:0DB9:0000:0000:0000:0000:0000:0000/123", "action": null }, { "id": 367, "cidr":
"2001:0DB9:0000:0000:0000:0000:0000:0000/128", "action": null } ], "decryptedFlow": 1600000,
"includeDecryptedPCAPS": true }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive
3	500	1001	Internal error

Update the SSL Configuration at the Sensor Level

This URL updates the SSL configuration at sensor level for 9.2 NS-series Sensors.

Resource URL

PUT /sensor/<sensorId>/sslconfiguration

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`inheritSettings`	Inherit settings from parent domain	Boolean	Yes
`decryptionState`	SSL state. The values can be: • DISABLED • INBOUND • OTBOUND	String	Yes
`anticipatedSSLTrafficUsage`	Anticipated inbound SSL traffic usage. The values can be: • VERY_HIGH • LIGHT • MEDIUM • HEAVY • VERY_HEAVY	String	Yes
`sslInactivityTimeoutInMinutes`	The maximum amount of time a Sensor will keep an outbound SSL flow open when no data has been seen on the Sensor.	Number	Yes
`includeDecryptedPCAPS`	Include decrypted packets while packet capture.	Boolean	Yes

Field Name	Description	Data Type	Mandatory
`enableDhSupport`	DH support	Boolean	Yes
`maxConcurrent`	Maximum concurrent connection allowed between a McAfee agent and a Sensor. The value can range from 1 to 1024.	Number	Yes
`permittedIPv4CIDRBlocks`	IPv4 CIDR blocks	Object	Yes
`permittedIPv6CIDRBlocks`	IPv6 CIDR blocks	Object	Yes
`failureHandling`	Failure handling	Object	Yes

Details of permittedIPv4CIDRBlocks and permittedIPv6CIDRBlocks:

Field Name	Description	Data Type	Mandatory
`action`	Action for the CIDR. The value is `delete` for deletion.	String	No
`cidr`	CIDR block	String	Yes

Details of failureHandling:

Field Name	Description	Data Type	Mandatory
`untrustedOrExpiredServerCertificate`	Action to take if the target web server's certificate is not on the Sensor's trusted CA list. This is used only in case of outbound SSL. The values can be: • Block Flow • Decrypt	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation is successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1001/decryptionsettings

Payload

```
{ "inheritSettings": false, "decryptionState": "INBOUND", "anticipatedSSLTrafficUsage": "HEAVY",
"sslInactivityTimeoutInMinutes": 1, "enableDhSupport": true, "maxConcurrent": 210, "permittedIPv4CIDRBlocks":
[{"cidr":"10.1.1.0/23"}], "permittedIPv6CIDRBlocks": [{"cidr":"2001:DB9::1/122"}], "includeDecryptedPCAPS":
false }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive
3	500	1001	Internal error

Add Rate Limiting Profile

This URL adds a new rate limiting profile.

Resource URL

POST / ratelimitingprofile

Request Parameters

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`rateLimitingProfileId`	Unique rate limiting profile id, not required for POST	Number	No
`name`	Profile name	String	Yes
`domainId`	Id of domain to which this profile belongs to	Number	Yes
`visibleToChild`	Profile visible to child domain	Boolean	Yes
`description`	Rate limiting profile description	String	No
`lastModifiedTime`	Last modified time of the profile, not required for POST	String	No
`isEditable`	Profile is editable or not, not required for POST	Boolean	No
`lastModifiedUser`	Latest user that modified the profile, not required for POST	String	No
`bandwidthLimits`	Bandwidth limits in the profile	Object	Yes

Details of bandwidthLimits:

Field Name	Description	Data Type	Mandatory
`interfaceType`	Interface type, can be "MBPS_10" / "MBPS_100" / "GBPS_1" / "GBPS_100"	String	Yes
`classBandwidthDetails`	Bandwidth details for each class	Array	Yes

Details of object in ClassBandwidthDetails:

Field Name	Description	Data Type	Mandatory
`qosClass`	Class	Number	Yes

Field Name	Description	Data Type	Mandatory
`bandwidthLimit`	Bandwidth limit	Number	Yes
`bandwidthUnit`	Bandwidth unit, can be "KBPS" / "MBPS" / "GBPS"	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
createdResourceId	Unique id of the created profile	Number

Example

Request

```
POST https://<NSM_IP>/sdkapi/ratelimitingprofile Payload: { "name": "Profile10Mbps", "domainId": 0,
"visibleToChild": true, "description": "Profile Visible To Child Domain in Domain 0 ", "bandwidthLimits":
{ "interfaceType": "MBPS_10", "classBandwidthDetails": [ { "qosClass": 1, "bandwidthLimit": 1024,
"bandwidthUnit": "KBPS" }, { "qosClass": 2, "bandwidthLimit": 9, "bandwidthUnit": "MBPS" }, { "qosClass": 3,
"bandwidthLimit": 0, "bandwidthUnit": "KBPS" }, { "qosClass": 4, "bandwidthLimit": 0, "bandwidthUnit": "KBPS" },
{ "qosClass": 5, "bandwidthLimit": 0, "bandwidthUnit": "KBPS" }, { "qosClass": 6, "bandwidthLimit": 0,
"bandwidthUnit": "KBPS" }, { "qosClass": 7, "bandwidthLimit": 0, "bandwidthUnit": "KBPS" } ] } }
```

Response

```
{ "createdResourceId":1000 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1001	internal error
2	404	1105	Invalid domain
3	400	2401	Rate limiting profile name is required
4	400	2404	Bandwidth value cannot be greater than the configured port type
5	400	2406	Queue profile with the same name already exist
6	400	2407	Rate limiting profile name should not be greater than 40 chars
7	400	2408	Rate limiting profile description should not be greater than 250 char
8	400	2409	Only alpha numeric characters allowed in rate limiting profile name

Update Rate Limiting Profile

This URL updates the rate limiting profile details.

Resource URL

PUT /ratelimitingprofile/<profile_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`profile_id`	Rate limiting profile id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`rateLimitingProfileId`	Rate limiting profile id to be updated	Number	Yes
`name`	Profile name	String	Yes
`domainId`	Id of domain to which this profile belongs to	Number	Yes
`visibleToChild`	Profile visible to child domain	Boolean	Yes
`description`	Rate limiting profile description	String	No
`lastModifiedTime`	Last modified timestamp. For Update, the "lastModifiedTime" in PUT operation should be the same as returned by the GET operation for the same rate limiting profile	String	Yes
`isEditable`	Profile is editable or not, For update, the "isEditable" in PUT operation should be the same as returned by the GET operation for the same rate limiting profile	Boolean	Yes
`lastModifiedUser`	Latest user that modified the profile. For update, the "lastModifiedUser" in PUT operation should be the same as returned by the GET operation for the same rate limiting profile	String	Yes
`bandwidthLimits`	Bandwidth limits in the profile	Object	Yes

Details of bandwidthLimits:

Field Name	Description	Data Type	Mandatory
`interfaceType`	Interface type, can be "MBPS_10" / "MBPS_100" / "GBPS_1" / "GBPS_100"	String	Yes
`classBandwidthDetails`	Bandwidth details for each class	Array	Yes

Details of object in ClassBandwidthDetails:

Field Name	Description	Data Type	Mandatory
`qosClass`	Class	Number	Yes
`bandwidthLimit`	Bandwidth limit	Number	Yes
`bandwidthUnit`	Bandwidth unit, can be "KBPS" / "MBPS" / "GBPS"	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Update status	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/ratelimitingprofile/1003

Payload:

```
{ "rateLimitingProfileId": 1003, "name": "UpdateProfile", "domainId": 0, "visibleToChild": false, "description":
"Profile Not Visible To Child Domain ", "lastModifiedTime": "2012-10-09 13:32:56", "lastModifiedUser": "/admin",
"bandwidthLimits": { "interfaceType": "GBPS_10", "classBandwidthDetails": [ { "qosClass": 1, "bandwidthLimit":
1024, "bandwidthUnit": "MBPS" }, { "qosClass": 2, "bandwidthLimit": 0, "bandwidthUnit": "KBPS" }, { "qosClass":
3, "bandwidthLimit": 1, "bandwidthUnit": "MBPS" }, { "qosClass": 4, "bandwidthLimit": 1, "bandwidthUnit":
"GBPS" }, { "qosClass": 5, "bandwidthLimit": 0, "bandwidthUnit": "KBPS" }, { "qosClass": 6, "bandwidthLimit": 0,
"bandwidthUnit": "KBPS" }, { "qosClass": 7, "bandwidthLimit": 0, "bandwidthUnit": "KBPS" } ] } }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1001	internal error
2	400	2401	Rate limiting profile name is required
3	404	2403	Invalid rate limiting profile Id / profile not visible in this domain

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
4	400	2404	Bandwidth value cannot be greater than the configured port type
5	400	2406	Queue profile with the same name already exist
6	400	2407	Rate limiting profile name should not be greater than 40 chars
7	400	2408	Rate limiting profile description should not be greater than 250 char
8	400	2409	Only alpha numeric characters allowed in rate limiting profile name

Delete Rate Limiting Profile

This URL deletes the specified rate limiting profile.

Resource URL

DELETE /ratelimitingprofile/<profile_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`profile_id`	Profile id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status returned by deletion	Number

Example

Request

DELETE https://%3CNSM_IP%3E/sdkapi/ratelimitingprofile/1001

Response

```
{ "status":1 }
```

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1001	internal error

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
2	404	2403	Invalid rate limiting profile id / profile not visible in this domain
3	400	2410	Profile in use cannot be deleted. Remove current assignments for the profile before deleting

Get Rate Limiting Profile

This URL gets the rate limiting profile details.

Resource URL

GET /ratelimitingprofile/<profile_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`profile_id`	Profile id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Payload Request Parameters:

Field Name	Description	Data Type
`rateLimitingProfileId`	Unique rate limiting profile id, not required for POST	Number
`name`	Profile name	String
`domainId`	Id of domain to which this profile belongs to	Number
`visibleToChild`	Profile visible to child domain	Boolean
`description`	Rate limiting profile description	String
`lastModifiedTime`	Last modified time of the profile, not required for POST	String
`isEditable`	Profile is editable or not, not required for POST	Boolean
`lastModifiedUser`	Latest user that modified the profile, not required for POST	String
`bandwidthLimits`	Bandwidth limits in the profile	Object

Details of bandwidthLimits:

Field Name	Description	Data Type
`interfaceType`	Interface type, can be "MBPS_10" / "MBPS_100" / "GBPS_1" / "GBPS_100"	String
`classBandwidthDetails`	Bandwidth Details for each class	Array

Details of object in ClassBandwidthDetails:

Field Name	Description	Data Type
`qosClass`	Class	Number
`bandwidthLimit`	Bandwidth limit	Number
`bandwidthUnit`	Bandwidth unit, can be "KBPS" / "MBPS" / "GBPS"	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ratelimitingprofile/1003

Response

```
{ "rateLimitingProfileId": 1003, "name": "UpdateProfile", "domainId": 0, "visibleToChild": false, "description":
"Profile Not Visible To Child Domain ", "lastModifiedTime": "2012-10-09 13:32:56", "lastModifiedUser": "/admin",
"bandwidthLimits": { "interfaceType": "GBPS_10", "classBandwidthDetails": [ { "qosClass": 1, "bandwidthLimit":
1024, "bandwidthUnit": "MBPS" }, { "qosClass": 2, "bandwidthLimit": 0, "bandwidthUnit": "KBPS" }, { "qosClass":
3, "bandwidthLimit": 1, "bandwidthUnit": "MBPS" }, { "qosClass": 4, "bandwidthLimit": 1, "bandwidthUnit":
"GBPS" }, { "qosClass": 5, "bandwidthLimit": 0, "bandwidthUnit": "KBPS" }, { "qosClass": 6, "bandwidthLimit": 0,
"bandwidthUnit": "KBPS" }, { "qosClass": 7, "bandwidthLimit": 0, "bandwidthUnit": "KBPS" } ] } }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1001	internal error
2	404	2403	Invalid rate limiting profile Id / profile not visible in this domain

Get Rate Limiting Profiles in a Domain

This URL gets the list of rate limiting profiles defined in a particular domain.

Resource URL

GET /domain/<domain_id>/ratelimitingprofiles

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`RateLimitingProfilesForDomainResponseList`	List of rate limiting profiles defined in the domain	Array

Details of RateLimitingProfilesForDomainResponseList:

Field Name	Description	Data Type
`profileId`	Rate limiting profile unique id	Number
`name`	Name of the rate limiting profile	String
`domainId`	Domain id	Number
`visibleToChild`	Is profile visible to child domains	Boolean
`description`	Profile description	String
`isEditable`	Is profile editable	Number
`lastModifiedUser`	Last user that modified the profile	String
`lastModifiedTime`	Last time the profile was modified	String
`interfaceType`	Interface type, can be "MBPS_10" / "MBPS_100" / "GBPS_1" / "GBPS_100"	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/domain/0/ratelimitingprofile

Response

```
{ "RateLimitingProfilesForDomainResponseList": [ { "profileId": 1003, "name": "Profile10Mbps", "domainId": 0,
"visibleToChild": true, "description": "Profile Visible To Child Domain in Domain 0 ", "isEditable": true,
"lastModifiedUser": "admin", "lastModifiedTime": "2012-10-09 13:32:56", "interfaceType": "MBPS_10" },
{ "profileId": 1000, "name": "UpdateTestProfile1", "domainId": 0, "visibleToChild": false, "description":
"Updated Test Profile Not visible to child domain", "isEditable": true, "lastModifiedUser": "admin",
"lastModifiedTime": "2012-10-09 13:32:57", "interfaceType": "GBPS_10" } ] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1001	internal error
2	404	1105	Invalid domain

Add QoS Policy

This URL adds a new QoS policy and rules.

Resource URL

POST /qospolicy

Request Parameters

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`QoSPolicyId`	Unique QoS policy id, not required for POST	Number	No
`Name`	Policy name	String	Yes
`DomainId`	Id of domain to which this QoS policy belongs to	Number	Yes
`VisibleToChild`	Policy visible to child domain	Boolean	Yes
`Description`	QoS policy description	String	No
`LastModifiedTime`	Last modified time of the QoS Policy, not required for POST	String	No
`IsEditable`	Policy is editable or not	Boolean	Yes
`PolicyType`	Policy type, can be "ADVANCED" / "CLASSIC"	Number	Yes
`PolicyVersion`	Policy version, not required for POST	Number	No
`LastModifiedUser`	Last user that modified the policy, not required for POST	String	Yes
`IsDiffServSettoZero`	Default value is true	Boolean	No
`IsVlanSettoZero`	Default value is true	Boolean	No
`MemberDetails`	QoS rules in the policy	Object	Yes

Details of MemberDetails:

Field Name	Description	Data Type	Mandatory
`QoSMemberRuleList`	List of QoS rules in the policy	Array	Yes

Details of object in QoSMemberRuleList:

Field Name	Description	Data Type	Mandatory
`Description`	Rule description	String	Yes
`Enabled`	Is rule enabled or not	Boolean	Yes
`RuleType`	Rule Type, can be "DIFFSERV" / "VLAN" / "BANDWIDTH"	String	Yes
`SourceAddressObjectList`	Source address rule object list	Array	Yes
`SourceUserObjectList`	Source user rule object list	Array	Yes
`DestinationAddressObjectList`	Destination address rule object list	Array	Yes
`ServiceObjectList`	Service rule object list	Array	Yes
`ApplicationObjectList`	Application rule object list	Array	Yes
`TimeObjectList`	Time rule object list	Array	Yes
`TagOrClass`	Tag/class value, For Diffserv, tag value should be between 0 - 63 For VLAN, tag value should be between 0 - 7 For bandwidth, tag value should be between 1 - 7	Number	Yes

Details of SourceAddressObjectList and DestinationAddressObjectList:

Field Name	Description	Data Type	Mandatory
`RuleObjectId`	Unique rule object id	String	Yes
`Name`	Rule object name	String	Yes
`RuleObjectType`	Source/destination mode, can be "COUNTRY" / "HOST_DNS_NAME" / "HOST_IPV_4" / "HOST_IPV_6" / "IPV_4_ADDRESS_RANGE" / "IPV_6_ADDRESS_RANGE" / "NETWORK_IPV_4" / "NETWORK_IPV_6" / "NETWORK_GROUP"	String	Yes

Details of SourceUserObjectList:

Field Name	Description	Data Type	Mandatory
`RuleObjectId`	Unique rule object id	String	Yes
`Name`	Rule object name	String	Yes

Field Name	Description	Data Type	Mandatory
`RuleObjectType`	Source user, can be "USER" / "USER_GROUP"	String	Yes

Details of ServiceObjectList and ApplicationObjectList:

Field Name	Description	Data Type	Mandatory
`RuleObjectId`	Unique rule object id	String	Yes
`Name`	Rule object name	String	Yes
`RuleObjectType`	Service/application mode, can be "APPLICATION" / "APPLICATION_GROUP" / "APPLICATION_ON_CUSTOM_PORT" / "SERVICE" / "SERVICE_RANGE" / "SERVICE_GROUP"	String	Yes
`ApplicationType`	Application type, can be "DEFAULT" / "CUSTOM"	String	Yes

Details of TimeObjectList:

Field Name	Description	Data Type	Mandatory
`RuleObjectId`	Unique rule object id	String	Yes
`Name`	Rule object name	String	Yes
`RuleObjectType`	Time mode, can be "FINITE_TIME_PERIOD" / "RECURRING_TIME_PERIOD" / "RECURRING_TIME_PERIOD_GROUP"	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique id of the created QoS policy	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/qospolicy

Payload:

```
{ "Name" : "QoSPolicyTest", "DomainId" : 0, "VisibleToChild" : true, "Description" : "To Test the QoS Policy",
"IsEditable" : true, "PolicyType" : "ADVANCED", "IsDiffServSettoZero" : false, "IsVlanSettoZero" : true,
"MemberDetails" : { "QoSMemberRuleList" : [{ "Description" : "QoSpolicyRatelimiting", "Enabled" : true,
"RuleType" : "RATE_LIMITING", "TagOrClass" : 3, "SourceAddressObjectList" : [{ "RuleObjectId" : "AX", "Name" :
"Aland Islands", "RuleObjectType" : "COUNTRY" }, { "RuleObjectId" : "101", "Name" : "hostDNSRule",
"RuleObjectType" : "HOST_DNS_NAME" }, { "RuleObjectId" : "102", "Name" : "hostIpv4", "RuleObjectType" :
"HOST_IPV_4" }, { "RuleObjectId" : "103", "Name" : "ipv4Addressrange", "RuleObjectType" :
"IPV_4_ADDRESS_RANGE" }, { "RuleObjectId" : "104", "Name" : "networkgroup", "RuleObjectType" :
"NETWORK_GROUP" } ], "DestinationAddressObjectList" : [{ "RuleObjectId" : "AL", "Name" : "Albania",
"RuleObjectType" : "COUNTRY" }, { "RuleObjectId" : "DZ", "Name" : "Algeria", "RuleObjectType" : "COUNTRY" },
{ "RuleObjectId" : "AS", "Name" : "American Samoa", "RuleObjectType" : "COUNTRY" } ], "SourceUserObjectList" :
```

```
[{ "RuleObjectId" : "-1", "Name" : "Any", "RuleObjectType" : "USER" } ], "ServiceObjectList" :
[{ "RuleObjectId" : "110", "Name" : "serviceCustom", "RuleObjectType" : "SERVICE", "ApplicationType" :
"CUSTOM" }, { "RuleObjectId" : "112", "Name" : "serviceGroup", "RuleObjectType" : "SERVICE_GROUP",
"ApplicationType" : "CUSTOM" }, { "RuleObjectId" : "111", "Name" : "serviceRange", "RuleObjectType" :
"SERVICE_RANGE", "ApplicationType" : "CUSTOM" } ], "ApplicationObjectList" : [], "TimeObjectList" :
[{ "RuleObjectId" : "107", "Name" : "finiteTimePeriod", "RuleObjectType" : "FINITE_TIMING_PERIOD" } ] },
{ "Description" : "DiffServ Rules", "Enabled" : true, "RuleType" : "DIFFSERV", "TagOrClass" : 3,
"SourceAddressObjectList" : [{ "RuleObjectId" : "AF", "Name" : "Afghanistan", "RuleObjectType" : "COUNTRY" } ],
"DestinationAddressObjectList" : [{ "RuleObjectId" : "VG", "Name" : "Virgin Islands, British",
"RuleObjectType" : "COUNTRY" } ], "SourceUserObjectList" : [{ "RuleObjectId" : "-1", "Name" : "Any",
"RuleObjectType" : "USER" } ], "ServiceObjectList" : [], "ApplicationObjectList" : [{ "RuleObjectId" :
"1627607040", "RuleObjectType" : "APPLICATION", "ApplicationType" : "DEFAULT" }, { "RuleObjectId" :
"1543598080", "RuleObjectType" : "APPLICATION", "ApplicationType" : "DEFAULT" } ], "TimeObjectList" :
[{ "RuleObjectId" : "109", "Name" : "recurringTimeperiodGroup", "RuleObjectType" :
"RECURRING_TIME_PERIOD_GROUP" } ] }, { "Description" : "", "Enabled" : true, "RuleType" : "VLAN", "TagOrClass" :
0, "SourceAddressObjectList" : [{ "RuleObjectId" : "-1", "Name" : "Any" } ], "DestinationAddressObjectList" :
[{ "RuleObjectId" : "-1", "Name" : "Any" } ], "SourceUserObjectList" : [{ "RuleObjectId" : "-1", "Name" : "Any",
"RuleObjectType" : "USER" } ], "ServiceObjectList" : [{ "RuleObjectId" : "-1", "Name" : "Any" } ],
"ApplicationObjectList" : [], "TimeObjectList" : [{ "RuleObjectId" : "-1", "Name" : "Always" } ] } ] } }
```

Response

```
{ "createdResourceId": 183 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	404	1105	Invalid domain
3	400	1704	Rule object type is expected
4	400	1720	Invalid rule object Id/ rule object not visible to this domain
5	400	1804	Maximum of 10 rule objects are allowed in each object list of an advanced firewall/QoS policy
6	400	1813	Source/destination object list is not provided
7	400	1814	Service/application object list is not provided
8	400	1815	Time object list is not provided
9	400	1821	Either application or service object list can be defined in a member rule for an advanced firewall/QoS policy
10	400	1832	Source address and destination address object list cannot combine IPV6 rule objects with host IPV4, network IPV4, IPV4 address range, country and host DNS name rule objects

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
11	400	2701	Invalid QoS policy type
12	400	2704	Diffserv tag value should be between 0 to 63
13	400	2705	Rate limiting class value should be between 1 to 7
14	400	2706	Vlan tag value should be between 0 to 7
15	400	2707	QoS policy name is required
16	400	2710	Time object list is not applicable for classic QoS policy
17	400	2711	Application object list is not applicable for classic QoS policy
18	400	2712	Source address object list is not applicable for classic QoS policy
19	400	2713	Source address object list is not applicable for classic QoS policy
20	400	2714	Source user object list is not applicable for classic QoS policy
21	400	2716	Only service type rule object is supported for classic QoS policy
22	400	2717	Name must contain only letters, numerals, spaces, commas, periods, hyphens or underscores
23	400	2718	QoS policy name should not be greater than 40 chars
24	400	2719	Classic QoS policy should have at least one service object list
25	400	2720	QoS policy with the same name was defined
26	400	2721	QoS policy provided is not up to date
27	400	2722	Policy type cannot be modified

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
28	400	2723	Either application or service object list can be defined in a member rule for an advanced QoS policy
29	400	2724	QoS policy description should not be greater than 255 chars
30	400	2725	Member rule description should not be greater than 64 chars

Update QoS Policy

This URL updates the QoS policy details.

Resource URL

PUT /qospolicy/<policy_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`policy_id`	QoS policy id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`QoSPolicyId`	Unique QoS policy id	Number	No
`Name`	Policy name	String	Yes
`DomainId`	Id of domain to which this QoS policy belongs to	Number	Yes
`VisibleToChild`	Policy visible to child domain	Boolean	Yes
`Description`	QoS policy description	String	No
`LastModifiedTime`	Last modified time of the QoS policy	String	Yes
`IsEditable`	Policy is editable or not	Boolean	Yes
`PolicyType`	Policy type, can be "ADVANCED" / "CLASSIC"	Number	Yes
`PolicyVersion`	Policy version	Number	Yes
`LastModifiedUser`	Latest user that modified the policy	String	Yes

Field Name	Description	Data Type	Mandatory
`IsDiffServSettoZero`	Default value is true	Boolean	No
`IsVlanSettoZero`	Default value is true	Boolean	No
`MemberDetails`	QoS rules in the policy	Object	Yes

Details of MemberDetails:

Field Name	Description	Data Type	Mandatory
`QoSMemberRuleList`	List of QoS rules in the policy	Array	Yes

Details of object in QoSMemberRuleList:

Field Name	Description	Data Type	Mandatory
`Description`	Rule description	String	Yes
`Enabled`	Is rule enabled or not	Boolean	Yes
`RuleType`	Rule type, can be "DIFFSERV" / "VLAN" / "BANDWIDTH"	String	Yes
`SourceAddressObjectList`	Source address rule object list	Array	Yes
`SourceUserObjectList`	Source user rule object list	Array	Yes
`DestinationAddressObjectList`	Destination address rule object list	Array	Yes
`ServiceObjectList`	Service rule object rlst	Array	Yes
`ApplicationObjectList`	Application rule object list	Array	Yes
`TimeObjectList`	Time rule object list	Array	Yes
`TagOrClass`	Tag/class value, For Diffserv, tag value should be between 0 - 63 For VLAN, tag value should be between 0 - 7 For Bandwidth, tag value should be between 1 - 7	Number	Yes

Details of SourceAddressObjectList and DestinationAddressObjectList:

Field Name	Description	Data Type	Mandatory
`RuleObjectId`	Unique rule object id	String	Yes
`Name`	Rule object name	String	Yes
`RuleObjectType`	Source/destination mode, can be "COUNTRY" / "HOST_DNS_NAME" / "HOST_IPV_4" /	String	Yes

Field Name	Description	Data Type	Mandatory
	"HOST_IPV_6" / "IPV_4_ADDRESS_RANGE" / "IPV_6_ADDRESS_RANGE" / "NETWORK_IPV_4" / "NETWORK_IPV_6" / "NETWORK_GROUP"		

Details of SourceUserObjectList:

Field Name	Description	Data Type	Mandatory
`RuleObjectId`	Unique rule object id	String	Yes
`Name`	Rule object name	String	Yes
`RuleObjectType`	Source user, can be "USER" / "USER_GROUP"	String	Yes

Details of ServiceObjectList and ApplicationObjectList:

Field Name	Description	Data Type	Mandatory
`RuleObjectId`	Unique service rule object id	String	Yes
`Name`	Rule object name	String	Yes
`RuleObjectType`	Service/application mode, can be "APPLICATION" / "APPLICATION_GROUP" / "APPLICATION_ON_CUSTOM_PORT" / "SERVICE" / "SERVICE_RANGE" / "SERVICE_GROUP"	String	Yes
`ApplicationType`	Application type, can be "DEFAULT" / "CUSTOM"	String	Yes

Details of TimeObjectList:

Field Name	Description	Data Type	Mandatory
`RuleObjectId`	Unique service rule object id	String	Yes
`Name`	Rule object name	String	Yes
`RuleObjectType`	Time mode, can be "FINITE_TIME_PERIOD" / "RECURRING_TIME_PERIOD" / "RECURRING_TIME_PERIOD_GROUP"	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Update status	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/qospolicy/183

```
{ "QoSPolicyId" : 183, "Name" : "QoSPolicyTest", "DomainId" : 0, "VisibleToChild" : true, "Description" : "To
Test the QoS Policy", "LastModifiedTime" : "2012-12-12 16:24:28", "IsEditable" : true, "PolicyType" :
"ADVANCED", "PolicyVersion" : 1, "LastModifiedUser" : "admin", "IsDiffServSettoZero" : false,
"IsVlanSettoZero" : false, "MemberDetails" : { "QoSMemberRuleList" : [{ "Description" : "QoSpolicyRatelimiting",
"Enabled" : true, "RuleType" : "RATE_LIMITING", "TagOrClass" : 3, "SourceAddressObjectList" :
[{ "RuleObjectId" : "AX", "Name" : "Aland Islands", "RuleObjectType" : "COUNTRY" }, { "RuleObjectId" : "101",
"Name" : "hostDNSRule", "RuleObjectType" : "HOST_DNS_NAME" }, { "RuleObjectId" : "102", "Name" : "hostIpv4",
"RuleObjectType" : "HOST_IPV_4" }, { "RuleObjectId" : "103", "Name" : "ipv4Addressrange", "RuleObjectType" :
"IPV_4_ADDRESS_RANGE" }, { "RuleObjectId" : "104", "Name" : "networkgroup", "RuleObjectType" :
"NETWORK_GROUP" } ], "DestinationAddressObjectList" : [{ "RuleObjectId" : "AL", "Name" : "Albania",
"RuleObjectType" : "COUNTRY" }, { "RuleObjectId" : "DZ", "Name" : "Algeria", "RuleObjectType" : "COUNTRY" },
{ "RuleObjectId" : "AS", "Name" : "American Samoa", "RuleObjectType" : "COUNTRY" } ], "SourceUserObjectList" :
[{ "RuleObjectId" : "-1", "Name" : "Any", "RuleObjectType" : "USER" } ], "ServiceObjectList" :
[{ "RuleObjectId" : "110", "Name" : "serviceCustom", "RuleObjectType" : "SERVICE", "ApplicationType" :
"CUSTOM" }, { "RuleObjectId" : "112", "Name" : "serviceGroup", "RuleObjectType" : "SERVICE_GROUP",
"ApplicationType" : "CUSTOM" }, { "RuleObjectId" : "111", "Name" : "serviceRange", "RuleObjectType" :
"SERVICE_RANGE", "ApplicationType" : "CUSTOM" } ], "ApplicationObjectList" : [], "TimeObjectList" :
[{ "RuleObjectId" : "107", "Name" : "finiteTimePeriod", "RuleObjectType" : "FINITE_TIMING_PERIOD" } ] },
{ "Description" : "DiffServ Rules", "Enabled" : true, "RuleType" : "DIFFSERV", "TagOrClass" : 3,
"SourceAddressObjectList" : [{ "RuleObjectId" : "AF", "Name" : "Afghanistan", "RuleObjectType" : "COUNTRY" } ],
"DestinationAddressObjectList" : [{ "RuleObjectId" : "VG", "Name" : "Virgin Islands, British",
"RuleObjectType" : "COUNTRY" } ], "SourceUserObjectList" : [{ "RuleObjectId" : "-1", "Name" : "Any",
"RuleObjectType" : "USER" } ], "ServiceObjectList" : [], "ApplicationObjectList" : [{ "RuleObjectId" :
"1627607040", "RuleObjectType" : "APPLICATION", "ApplicationType" : "DEFAULT" }, { "RuleObjectId" :
"1543598080", "RuleObjectType" : "APPLICATION", "ApplicationType" : "DEFAULT" } ], "TimeObjectList" :
[{ "RuleObjectId" : "109", "Name" : "recurringTimeperiodGroup", "RuleObjectType" :
"RECURRING_TIME_PERIOD_GROUP" } ] }, { "Description" : "", "Enabled" : true, "RuleType" : "VLAN", "TagOrClass" :
0, "SourceAddressObjectList" : [{ "RuleObjectId" : "-1", "Name" : "Any" } ], "DestinationAddressObjectList" :
[{ "RuleObjectId" : "-1", "Name" : "Any" } ], "SourceUserObjectList" : [{ "RuleObjectId" : "-1", "Name" : "Any",
"RuleObjectType" : "USER" } ], "ServiceObjectList" : [{ "RuleObjectId" : "-1", "Name" : "Any" } ],
"ApplicationObjectList" : [], "TimeObjectList" : [{ "RuleObjectId" : "-1", "Name" : "Always" } ] } ] } }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	404	1105	Invalid domain
3	400	1704	Rule object type is expected
4	400	1720	Invalid rule object id/ rule object not visible to this domain
5	400	1804	Maximum of 10 rule objects are allowed in each object list of an advanced firewall/QoS policy
6	400	1813	Source/destination object list is not provided

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
7	400	1814	Service/application object list is not provided
8	400	1815	Time object list is not provided
9	400	1821	Either application or service object list can be defined in a member rule for an advanced firewall/QoS policy
10	400	1832	Source address and destination address object list cannot combine IPV6 rule objects with host IPV4, network IPV4, IPV4 address range, country and host DNS name rule objects
11	400	2701	Invalid QoS policy type
12	400	2702	Invalid QoS policy id/ QoS policy not visible to this domain
13	400	2704	Diffserv tag value should be between 0 to 63
14	400	2705	Rate limiting class value should be between 1 to 7
15	400	2706	Vlan tag value should be between 0 to 7
16	400	2707	QoS policy name is required
17	400	2710	Time object list is not applicable for classic QoS policy
18	400	2711	Application object list is not applicable for classic QoS policy
19	400	2712	Source address object list is not applicable for classic QoS policy
20	400	2713	Source address object list is not applicable for classic QoS policy
21	400	2714	Source user object list is not applicable for classic QoS policy

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
22	400	2716	Only service type rule object is supported for classic QoS policy
23	400	2717	Name must contain only letters, numerals, spaces, commas, periods, hyphens or underscores
24	400	2718	QoS policy name should not be greater than 40 chars
25	400	2719	Classic QoS policy should have at least one service object list
26	400	2720	QoS policy with the same name was defined
27	400	2721	QoS policy provided is not up to date
28	400	2722	Policy type cannot be modified
29	400	2723	Either application or service object list can be defined in a member rule for an advanced QoS policy
30	400	2724	QoS policy description should not be greater than 255 chars
31	400	2725	Member rule description should not be greater than 64 chars

Delete QoS Policy

This URL deletes the specified QoS policy.

Resource URL

DELETE /qospolicy/<policy_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`Policy_id`	Policy id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
Status	Status returned by deletion	Number

Example

Request

DELETEhttps://%3CNSM_IP%3E/sdkapi/qospolicy/183

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	2702	Invalid QoS policy Id/QoS policy not visible to this domain
2	400	2703	QoS policy in use, cannot be deleted

Get QoS Policy

This URL gets the QoS policy details.

Resource URL

GET /qospolicy/<policy_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
Policy_id	Policy id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
QoSPolicyId	Unique QoS policy id	Number
Name	Policy name	String
DomainId	Id of domain to which this QoS policy belongs to	Number
VisibleToChild	Policy visible to child domain	Boolean
Description	QoS policy description	String

Field Name	Description	Data Type
LastModifiedTime	Last modified time of the QoS policy	String
IsEditable	Policy is editable or not	Boolean
PolicyType	Policy type, can be "ADVANCED" / "CLASSIC"	Number
PolicyVersion	Policy version	Number
LastModifiedUser	Last user that modified the policy	String
IsDiffServSettoZero	Default value is true	Boolean
IsVlanSettoZero	Default value is true	Boolean
MemberDetails	QoS rules in the policy	Object

Details of MemberDetails:

Field Name	Description	Data Type
QoSMemberRuleList	List of QoS rules in the policy	Array

Details of object in QoSMemberRuleList:

Field Name	Description	Data Type
Description	Rule description	String
Enabled	Is rule enabled or not	Boolean
RuleType	Rule type, can be "DIFFSERV" / "VLAN" / "BANDWIDTH"	String
SourceAddressObjectList	Source address rule object list	Array
SourceUserObjectList	Source user rule object list	Array
DestinationAddressObjectList	Destination address rule object list	Array
ServiceObjectList	Service rule object list	Array
ApplicationObjectList	Application rule object list	Array
TimeObjectList	Time rule object list	Array
TagOrClass	Tag/class value, For Diffserv, tag value should be between 0 - 63 For VLAN, tag value should be between 0 - 7 For Bandwidth, tag value should be between 1 - 7	Number

Details of SourceAddressObjectList and DestinationAddressObjectList:

Field Name	Description	Data Type
`RuleObjectId`	Unique rule object id	String
`Name`	Rule object name	String
`RuleObjectType`	Source/destination mode, can be "COUNTRY" / "HOST_DNS_NAME" / "HOST_IPV_4" / "HOST_IPV_6" / "IPV_4_ADDRESS_RANGE" / "IPV_6_ADDRESS_RANGE" / "NETWORK_IPV_4" / "NETWORK_IPV_6" / "NETWORK_GROUP"	String

Details of SourceUserObjectList:

Field Name	Description	Data Type
`RuleObjectId`	Unique rule object id	String
`Name`	Rule object name	String
`RuleObjectType`	Source User, can be "USER" / "USER_GROUP"	String

Details of ServiceObjectList and ApplicationObjectList:

Field Name	Description	Data Type
`RuleObjectId`	Unique service rule object id	String
`Name`	Rule object name	String
`RuleObjectType`	Service/application mode, can be "APPLICATION" / "APPLICATION_GROUP" / "APPLICATION_ON_CUSTOM_PORT" / "SERVICE" / "SERVICE_RANGE" / "SERVICE_GROUP"	String
`ApplicationType`	Application type, can be "DEFAULT" / "CUSTOM"	String

Details of TimeObjectList:

Field Name	Description	Data Type
`RuleObjectId`	Unique service rule object id	String
`Name`	Rule object name	String
`RuleObjectType`	Time mode, can be "FINITE_TIME_PERIOD" / "RECURRING_TIME_PERIOD" / "RECURRING_TIME_PERIOD_GROUP"	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/qospolicy/183

Response

```
{ "QoSPolicyId" : 183, "Name" : "QoSPolicyTest", "DomainId" : 0, "VisibleToChild" : true, "Description" : "To
Test the QoS Policy", "LastModifiedTime" : "2012-12-12 16:24:28", "IsEditable" : true, "PolicyType" :
"ADVANCED", "PolicyVersion" : 1, "LastModifiedUser" : "admin", "IsDiffServSettoZero" : false,
"IsVlanSettoZero" : true, "MemberDetails" : { "QoSMemberRuleList" : [{ "Description" : "QoSpolicyRatelimiting",
"Enabled" : true, "RuleType" : "RATE_LIMITING", "TagOrClass" : 3, "SourceAddressObjectList" :
[{ "RuleObjectId" : "AX", "Name" : "Aland Islands", "RuleObjectType" : "COUNTRY" }, { "RuleObjectId" : "101",
"Name" : "hostDNSRule", "RuleObjectType" : "HOST_DNS_NAME" }, { "RuleObjectId" : "102", "Name" : "hostIpv4",
"RuleObjectType" : "HOST_IPV_4" }, { "RuleObjectId" : "103", "Name" : "ipv4Addressrange", "RuleObjectType" :
"IPV_4_ADDRESS_RANGE" }, { "RuleObjectId" : "104", "Name" : "networkgroup", "RuleObjectType" :
"NETWORK_GROUP" } ], "DestinationAddressObjectList" : [{ "RuleObjectId" : "AL", "Name" : "Albania",
"RuleObjectType" : "COUNTRY" }, { "RuleObjectId" : "DZ", "Name" : "Algeria", "RuleObjectType" : "COUNTRY" },
{ "RuleObjectId" : "AS", "Name" : "American Samoa", "RuleObjectType" : "COUNTRY" } ], "SourceUserObjectList" :
[{ "RuleObjectId" : "-1", "Name" : "Any", "RuleObjectType" : "USER" } ], "ServiceObjectList" :
[{ "RuleObjectId" : "110", "Name" : "serviceCustom", "RuleObjectType" : "SERVICE", "ApplicationType" :
"CUSTOM" }, { "RuleObjectId" : "112", "Name" : "serviceGroup", "RuleObjectType" : "SERVICE_GROUP",
"ApplicationType" : "CUSTOM" }, { "RuleObjectId" : "111", "Name" : "serviceRange", "RuleObjectType" :
"SERVICE_RANGE", "ApplicationType" : "CUSTOM" } ], "ApplicationObjectList" : [], "TimeObjectList" :
[{ "RuleObjectId" : "107", "Name" : "finiteTimePeriod", "RuleObjectType" : "FINITE_TIMING_PERIOD" } ] },
{ "Description" : "DiffServ Rules", "Enabled" : true, "RuleType" : "DIFFSERV", "TagOrClass" : 3,
"SourceAddressObjectList" : [{ "RuleObjectId" : "AF", "Name" : "Afghanistan", "RuleObjectType" : "COUNTRY" } ],
"DestinationAddressObjectList" : [{ "RuleObjectId" : "VG", "Name" : "Virgin Islands, British",
"RuleObjectType" : "COUNTRY" } ], "SourceUserObjectList" : [{ "RuleObjectId" : "-1", "Name" : "Any",
"RuleObjectType" : "USER" } ], "ServiceObjectList" : [], "ApplicationObjectList" : [{ "RuleObjectId" :
"1627607040", "RuleObjectType" : "APPLICATION", "ApplicationType" : "DEFAULT" }, { "RuleObjectId" :
"1543598080", "RuleObjectType" : "APPLICATION", "ApplicationType" : "DEFAULT" } ], "TimeObjectList" :
[{ "RuleObjectId" : "109", "Name" : "recurringTimeperiodGroup", "RuleObjectType" :
"RECURRING_TIME_PERIOD_GROUP" } ] }, { "Description" : "", "Enabled" : true, "RuleType" : "VLAN", "TagOrClass" :
0, "SourceAddressObjectList" : [{ "RuleObjectId" : "-1", "Name" : "Any" } ], "DestinationAddressObjectList" :
[{ "RuleObjectId" : "-1", "Name" : "Any" } ], "SourceUserObjectList" : [{ "RuleObjectId" : "-1", "Name" : "Any",
"RuleObjectType" : "USER" } ], "ServiceObjectList" : [{ "RuleObjectId" : "-1", "Name" : "Any" } ],
"ApplicationObjectList" : [], "TimeObjectList" : [{ "RuleObjectId" : "-1", "Name" : "Always" } ] } ] } }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	2702	Invalid QoS policy Id/ QoS policy not visible to this domain

Get QoS Policies in a Domain

This URL gets the list of QoS policies defined in a particular domain.

Resource URL

GET /domain/<domain_id>/ qospolicy

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`QoSPoliciesForDomainResponseList`	List of QoS policies defined in the domain	Array

Details of object in QoSPoliciesForDomainResponseList:

Field Name	Description	Data Type
`policyName`	Name of the QoS policy	String
`visibleToChild`	Is policy visible to child domains	Boolean
`description`	Policy description	String
`isEditable`	Is policy editable	Number
`lastModUser`	Last user that modified the policy	String
`policyType`	Policy type, can be "ADVANCED" or "CLASSIC"	String
`policyId`	QoS policy unique id	Number
`domainId`	Domain id	Number
`policyVersion`	Policy version	Number

Example

Request

GEThttps://%3CNSM_IP%3E/sdkapi/domain/0/qospolicy

Response

```
{ "QoSPoliciesForDomain": [ { "policyName": "TestQosPolicy", "visibleToChild": true, "isEditable": true,
"description": "To test the QOSPolicy", "lastModUser": "admin", "policyType": "ADVANCED", "policyId": 179,
"domainId": 0, "policyVersion": 1 }, { "policyName": "QosPolicy", "visibleToChild": true, "isEditable": true,
"description": "To test the QOSPolicy", "lastModUser": "admin", "policyType": "ADVANCED", "policyId": 175,
"domainId": 0, "policyVersion": 1 } ] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Add Advanced Malware Policy

This URL adds a new advanced malware policy.

Resource URL

POST /malwarepolicy

Request Parameters

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`properties`	Basic properties of the malware policy	Object	Yes
`scanningOptions`	List of scanning options per file type	Array	No

Details of properties:

Field Name	Description	Data Type	Mandatory
`policyName`	Policy name	String	Yes
`description`	Description	String	No
`domainId`	Domain id	Number	Yes
`visibleToChild`	Is the policy visible to child	Boolean	Yes
`protocolsToScan`	List of protocols supported	Array	No

Details of object in protocolsToScan:

Field Name	Description	Data Type	Mandatory
`protocolName`	Protocol name	String	Yes
`protocolNumber`	Protocol number	Number	Yes
`enabled`	Protocol status	Boolean	Yes

Details of object in scanningOptions:

Field Name	Description	Data Type	Mandatory
`fileType`	Type of the file	String	Yes
`malwareEngines`	List of malware engines supported	Array	Yes
`actionThresholds`	Action threshold details	Object	Yes

Field Name	Description	Data Type	Mandatory
`maximumFileSizeScannedInKB`	Maximum file size scanned in KB	Number	Yes

Details of object in malwareEngines:

Field Name	Description	Data Type	Mandatory
`name`	Malware engine name	String	Yes
`status`	Status can be DISABLED/ UNCHECKED/CHECKED	String	Yes
`id`	Malware engine id	Number	Yes

Details of actionThresholds:

Field Name	Description	Data Type	Mandatory
`alert`	Alert to be sent, can be "DISABLED" / "VERY_LOW" / "LOW" / "MEDIUM" / "HIGH" / "VERY_HIGH"	String	Yes
`block`	Blocking settings, can be "DISABLED" / "VERY_LOW" / "LOW" / "MEDIUM" / "HIGH" / "VERY_HIGH"	String	Yes
`sendTcpReset`	Send TCP reset, can be "DISABLED" / "VERY_LOW" / "LOW" / "MEDIUM" / "HIGH" / "VERY_HIGH"	String	Yes
`saveFile`	Save file can be "DISABLED" / "ALWAYS" /"VERY_LOW" / "LOW" / "MEDIUM" / "HIGH" / "VERY_HIGH"	String	Yes
`addToBlockList`	Add to block list can be "DISABLED" / "VERY_LOW" / "LOW" / "MEDIUM" / "HIGH" / "VERY_HIGH"	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique id of the created malware policy	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/malwarepolicy

```
{ "properties": { "policyName": "Test", "description": "Add Malware Policy", "domainId": 0, "visibleToChild":
true, "protocolsToScan": [ { "protocolName": "HTTP", "protocolNumber": 16, "enabled": true }, { "protocolName":
"SMTP", "protocolNumber": 12, "enabled": true } ] }, "scanningOptions": [ { "fileType": "Executables",
"maximumFileSizeScannedInKB": 5120, "malwareEngines": [ { "name": "GTI File Reputation", "id": 1, "status":
"UNCHECKED" }, { "name": " Blocklist and Allowlist", "id": 2, "status": "UNCHECKED" }, { "name": "PDF
Emulation", "id": 8, "status": "DISABLED" }, { "name": "NTBA", "id": 16, "status": "CHECKED" }, { "name":
"Advanced Threat Defense", "id": 64, "status": "CHECKED" } ], "actionThresholds": { "alert": "LOW", "block":
"HIGH", "sendTcpReset": "HIGH", "saveFile": "DISABLED", "addToBlockList": "DISABLED" } }, { "fileType": "MS
Office Files", "maximumFileSizeScannedInKB": 1024, "malwareEngines": [ { "name": "GTI File Reputation", "id": 1,
"status": "DISABLED" }, { "name": "Blocklist and Allowlist ", "id": 2, "status": "CHECKED" }, { "name": "PDF
Emulation", "id": 8, "status": "DISABLED" }, { "name": "NTBA", "id": 16, "status": "CHECKED" }, { "name":
"Advanced Threat Defense", "id": 64, "status": "CHECKED" } ], "actionThresholds": { "alert": "MEDIUM", "block":
"HIGH", "sendTcpReset": "HIGH", "saveFile": "DISABLED", "addToBlockList": "DISABLED" } }, { "fileType": "PDF
Files", "maximumFileSizeScannedInKB": 1024, "malwareEngines": [ { "name": "GTI File Reputation", "id": 1,
"status": "UNCHECKED" }, { "name": " Blocklist and Allowlist ", "id": 2, "status": "UNCHECKED" }, { "name": "PDF
Emulation", "id": 8, "status": "CHECKED" }, { "name": "NTBA", "id": 16, "status": "CHECKED" }, { "name":
"Advanced Threat Defense", "id": 64, "status": "CHECKED" } ], "actionThresholds": { "alert": "VERY_LOW",
"block": "HIGH", "sendTcpReset": "HIGH", "saveFile": "DISABLED", "addToBlockList": "DISABLED" } }, { "fileType":
"Compressed Files", "maximumFileSizeScannedInKB": 5120, "malwareEngines": [ { "name": "GTI File Reputation",
"id": 1, "status": "DISABLED" }, { "name": " Blocklist and Allowlist ", "id": 2, "status": "UNCHECKED" },
{ "name": "PDF Emulation", "id": 8, "status": "DISABLED" }, { "name": "NTBA", "id": 16, "status": "UNCHECKED" },
{ "name": "Advanced Threat Defense", "id": 64, "status": "CHECKED" } ], "actionThresholds": { "alert":
"VERY_LOW", "block": "HIGH", "sendTcpReset": "HIGH", "saveFile": "DISABLED", "addToBlockList": "DISABLED" } },
{ "fileType": "Android Application Package", "maximumFileSizeScannedInKB": 2048, "malwareEngines": [ { "name":
"GTI File Reputation", "id": 1, "status": "CHECKED" }, { "name": " Blocklist and Allowlist ", "id": 2, "status":
"UNCHECKED" }, { "name": "PDF Emulation", "id": 8, "status": "DISABLED" }, { "name": "NTBA", "id": 16, "status":
"DISABLED" }, { "name": "Advanced Threat Defense", "id": 64, "status": "CHECKED" } ], "actionThresholds":
{ "alert": "VERY_LOW", "block": "HIGH", "sendTcpReset": "HIGH", "saveFile": "DISABLED", "addToBlockList":
"DISABLED" } }, { "fileType": "Java Archive", "maximumFileSizeScannedInKB": 2048, "malwareEngines": [ { "name":
"GTI File Reputation", "id": 1, "status": "DISABLED" }, { "name": " Blocklist and Allowlist ", "id": 2,
"status": "UNCHECKED" }, { "name": "PDF Emulation", "id": 8, "status": "DISABLED" }, { "name": "NTBA", "id": 16,
"status": "UNCHECKED" }, { "name": "Advanced Threat Defense", "id": 64, "status": "CHECKED" } ],
"actionThresholds": { "alert": "VERY_LOW", "block": "HIGH", "sendTcpReset": "HIGH", "saveFile": "DISABLED",
"addToBlockList": "DISABLED" } } ] }
```

Response

```
{ "createdResourceId": 301 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1105	Invalid domain
2	400	2508	Malware policy name is required
3	400	2509	Invalid protocol list
4	400	2513	Name must contain only letters, numerical, spaces, commas, periods, hyphens or underscore
5	400	2514	Name already in use
6	400	2516	Length of name field cannot exceed 40 characters
7	400	2517	Length of description field cannot exceed 149 characters

Update Malware Policy

This URL updates the malware policy details.

Resource URL

PUT /malwarepolicy/<policy_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
policy_id	Malware policy id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
properties	Basic properties of the malware policy	Object	Yes
scanningOptions	List of scanning options per file type	Array	Yes

Details of properties:

Field Name	Description	Data Type	Mandatory
policyName	Policy name	String	Yes
description	Description	String	No
domainId	Domain id	Number	Yes
lastModifiedTime	Last modified time	String	Yes
lastModifiedUser	Last user that modified the policy	String	Yes
isEditable	Is policy editable	Boolean	Yes
visibleToChild	Is the policy visible to child	Boolean	Yes
protocolsToScan	List of protocols supported	Array	No

Details of object in protocolsToScan:

Field Name	Description	Data Type	Mandatory
protocolName	Protocol name	String	Yes
protocolNumber	Protocol number	Number	Yes
enabled	Protocol status	Boolean	Yes

Details of object in scanningOptions:

Field Name	Description	Data Type	Mandatory
fileType	Type of the file	String	Yes

Field Name	Description	Data Type	Mandatory
malwareEngines	List of malware engines supported	Array	Yes
actionThresholds	Action threshold details	Object	Yes
maximumFileSizeScannedInKB	Maximum file size scanned in KB	Number	Yes

Details of object in malwareEngines:

Field Name	Description	Data Type	Mandatory
name	Malware engine name	String	Yes
status	Status can be DISABLED/ UNCHECKED/CHECKED	String	Yes
id	Malware engine id	Number	Yes

Details of actionThresholds:

Field Name	Description	Data Type	Mandatory
alert	Alert to be sent, can be "DISABLED" / "VERY_LOW" / "LOW" / "MEDIUM" / "HIGH" / "VERY_HIGH"	String	Yes
block	Blocking settings, can be "DISABLED" / "VERY_LOW" / "LOW" / "MEDIUM" / "HIGH" / "VERY_HIGH"	String	Yes
sendTcpReset	Send TCP reset, can be "DISABLED" / "VERY_LOW" / "LOW" / "MEDIUM" / "HIGH" / "VERY_HIGH"	String	Yes
saveFile	Save file can be "DISABLED" / "ALWAYS" /"VERY_LOW" / "LOW" / "MEDIUM" / "HIGH" / "VERY_HIGH"	String	Yes
addToBlockList	Add to blocklist can be "DISABLED" / "VERY_LOW" / "LOW" / "MEDIUM" / "HIGH" / "VERY_HIGH"	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Update status	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/malwarepolicy/301

```
PUT https://<NSM_IP>/sdkapi/malwarepolicy/301 { "properties": { "policyName": "Test", "description": "Add
Malware Policy", "domainId": 0, "visibleToChild": true, "protocolsToScan": [ { "protocolName": "HTTP",
"protocolNumber": 16, "enabled": true }, { "protocolName": "SMTP", "protocolNumber": 12, "enabled": true } ] },
"scanningOptions": [ { "fileType": "Executables", "maximumFileSizeScannedInKB": 5120, "malwareEngines":
[ { "name": "GTI File Reputation", "id": 1, "status": "UNCHECKED" }, { "name": " Blocklist and Allowlist", "id":
2, "status": "UNCHECKED" }, { "name": "PDF Emulation", "id": 8, "status": "DISABLED" }, { "name": "NTBA", "id":
16, "status": "CHECKED" }, { "name": "Advanced Threat Defense", "id": 64, "status": "CHECKED" } ],
"actionThresholds": { "alert": "LOW", "block": "HIGH", "sendTcpReset": "HIGH", "saveFile": "DISABLED",
"addToBlockList": "DISABLED" } }, { "fileType": "MS Office Files", "maximumFileSizeScannedInKB": 1024,
"malwareEngines": [ { "name": "GTI File Reputation", "id": 1, "status": "DISABLED" }, { "name": "Blocklist and
Allowlist ", "id": 2, "status": "CHECKED" }, { "name": "PDF Emulation", "id": 8, "status": "DISABLED" },
{ "name": "NTBA", "id": 16, "status": "CHECKED" }, { "name": "Advanced Threat Defense", "id": 64, "status":
"CHECKED" } ], "actionThresholds": { "alert": "MEDIUM", "block": "HIGH", "sendTcpReset": "HIGH", "saveFile":
"DISABLED", "addToBlockList": "DISABLED" } }, { "fileType": "PDF Files", "maximumFileSizeScannedInKB": 1024,
"malwareEngines": [ { "name": "GTI File Reputation", "id": 1, "status": "UNCHECKED" }, { "name": " Blocklist and
Allowlist ", "id": 2, "status": "UNCHECKED" }, { "name": "PDF Emulation", "id": 8, "status": "CHECKED" },
{ "name": "NTBA", "id": 16, "status": "CHECKED" }, { "name": "Advanced Threat Defense", "id": 64, "status":
"CHECKED" } ], "actionThresholds": { "alert": "VERY_LOW", "block": "HIGH", "sendTcpReset": "HIGH", "saveFile":
"DISABLED", "addToBlockList": "DISABLED" } }, { "fileType": "Compressed Files", "maximumFileSizeScannedInKB":
5120, "malwareEngines": [ { "name": "GTI File Reputation", "id": 1, "status": "DISABLED" }, { "name": "
Blocklist and Allowlist ", "id": 2, "status": "UNCHECKED" }, { "name": "PDF Emulation", "id": 8, "status":
"DISABLED" }, { "name": "NTBA", "id": 16, "status": "UNCHECKED" }, { "name": "Advanced Threat Defense", "id":
64, "status": "CHECKED" } ], "actionThresholds": { "alert": "VERY_LOW", "block": "HIGH", "sendTcpReset": "HIGH",
"saveFile": "DISABLED", "addToBlockList": "DISABLED" } }, { "fileType": "Android Application Package",
"maximumFileSizeScannedInKB": 2048, "malwareEngines": [ { "name": "GTI File Reputation", "id": 1, "status":
"CHECKED" }, { "name": " Blocklist and Allowlist ", "id": 2, "status": "UNCHECKED" }, { "name": "PDF Emulation",
"id": 8, "status": "DISABLED" }, { "name": "NTBA", "id": 16, "status": "DISABLED" }, { "name": "Advanced Threat
Defense", "id": 64, "status": "CHECKED" } ], "actionThresholds": { "alert": "VERY_LOW", "block": "HIGH",
"sendTcpReset": "HIGH", "saveFile": "DISABLED", "addToBlockList": "DISABLED" } }, { "fileType": "Java Archive",
"maximumFileSizeScannedInKB": 2048, "malwareEngines": [ { "name": "GTI File Reputation", "id": 1, "status":
"DISABLED" }, { "name": " Blocklist and Allowlist ", "id": 2, "status": "UNCHECKED" }, { "name": "PDF
Emulation", "id": 8, "status": "DISABLED" }, { "name": "NTBA", "id": 16, "status": "UNCHECKED" }, { "name":
"Advanced Threat Defense", "id": 64, "status": "CHECKED" } ], "actionThresholds": { "alert": "VERY_LOW",
"block": "HIGH", "sendTcpReset": "HIGH", "saveFile": "DISABLED", "addToBlockList": "DISABLED" } } ] }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1105	Invalid domain
2	404	2501	Invalid advanced malware policy id/ policy not visible to this domain
3	400	2508	Malware policy name is required
4	400	2509	Invalid protocol list
5	400	2512	Policy provided is not up to date
6	400	2513	Name must contain only letters, numerical, spaces, commas, periods, hyphens or underscore
7	400	2514	Name already in use
8	400	2515	Default malware policy cannot be updated

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
9	400	2516	Length of name field cannot exceed 40 characters
10	400	2517	Length of description field cannot exceed 149 characters

Delete Malware Policy

This URL deletes the specified malware policy

Resource URL

DELETE /malwarepolicy/<policy_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`policy_id`	Policy id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status returned by deletion	Number

Example

Request

DELETEhttps://%3CNSM_IP%3E/sdkapi/malwarepolicy/301

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	2501	Invalid advanced malware policy id/ policy not visible to this domain
2	400	2503	Assigned malware policy cannot be deleted

Get Malware Policy

This URL gets the malware policy details.

Resource URL

GET /malwarepolicy/<policy_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`Policy_id`	Policy id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`properties`	Basic properties of the malware policy	Object
`scanningOptions`	List of scanning options per file type	Array

Details of properties:

Field Name	Description	Data Type
`policyId`	Policy id	Number
`policyName`	Policy name	String
`description`	Description	String
`domainId`	Domain Id	Number
`lastModifiedTime`	Last modified time	String
`lastModifiedUser`	Last user that modified the policy	String
`isEditable`	Is policy editable	Boolean
`visibleToChild`	Is the policy visible to child	Boolean
`protocolsToScan`	List of protocols supported	Array

Details of object in protocolsToScan:

Field Name	Description	Data Type
`protocolName`	Protocol name	String
`protocolNumber`	Protocol number	Number
`enabled`	Protocol status	Boolean

Details of object in scanningOptions:

Field Name	Description	Data Type
`fileType`	Type of the file	String

Field Name	Description	Data Type
`malwareEngines`	List of malware engines supported	Array
`actionThresholds`	Action threshold details	Object

Details of object in malwareEngines:

Field Name	Description	Data Type
`name`	Malware engine name	String
`status`	Status can be DISABLED/UNCHECKED/ CHECKED	String
`id`	Malware engine id	Number

Details of actionThresholds:

Field Name	Description	Data Type
`alert`	Alert to be sent, can be "DISABLED" / "VERY_LOW" / "LOW" / "MEDIUM" / "HIGH" / "VERY_HIGH"	String
`block`	Blocking settings, can be "DISABLED" / "VERY_LOW" / "LOW" / "MEDIUM" / "HIGH" / "VERY_HIGH"	String
`sendTcpReset`	Send TCP reset, can be "DISABLED" / "VERY_LOW" / "LOW" / "MEDIUM" / "HIGH" / "VERY_HIGH"	String
`saveFile`	Save file, can be "DISABLED" / "ALWAYS" /"VERY_LOW" / "LOW" / "MEDIUM" / "HIGH" / "VERY_HIGH"	String

Example

Request

GEThttps://%3CNSM_IP%3E/sdkapi/malwarepolicy/301

Response

```
{ "properties": { "policyId": 301, "policyName": "Test", "description": "", "domainId": 0, "lastModifiedTime":
"2012-10-08 13:39:56", "lastModifiedUser": "admin", "isEditable": true, "visibleToChild": true,
"protocolsToScan": [ { "protocolName": "HTTP", "protocolNumber": 16, "enabled": true }, { "protocolName":
"SMTP", "protocolNumber": 12, "enabled": true } ] }, "scanningOptions": [ { "fileType": "Executables",
"malwareEngines": [ { "name": "GTI File Reputation", "id": 1, "status": "CHECKED" }, { "name": "Custom
Fingerprints", "id": 2, "status": "UNCHECKED" }, { "name": "PDF Analysis", "id": 8, "status": "DISABLED" },
{ "name": "Anti-Malware Analysis", "id": 16, "status": "UNCHECKED" } ], "actionThresholds": { "alert": "LOW",
"block": "HIGH", "sendTcpReset": "HIGH", "saveFile": "DISABLED" } }, { "fileType": "MS Office Files",
"malwareEngines": [ { "name": "GTI File Reputation", "id": 1, "status": "DISABLED" }, { "name": "Custom
Fingerprints", "id": 2, "status": "CHECKED" }, { "name": "PDF Analysis", "id": 8, "status": "DISABLED" },
{ "name": "Anti-Malware Analysis", "id": 16, "status": "CHECKED" } ], "actionThresholds": { "alert": "MEDIUM",
"block": "HIGH", "sendTcpReset": "HIGH", "saveFile": "DISABLED" } }, { "fileType": "PDF Files",
"malwareEngines": [ { "name": "GTI File Reputation", "id": 1, "status": "CHECKED" }, { "name": "Custom
Fingerprints", "id": 2, "status": "UNCHECKED" }, { "name": "PDF Analysis", "id": 8, "status": "CHECKED" },
{ "name": "Anti-Malware Analysis", "id": 16, "status": "CHECKED" } ], "actionThresholds": { "alert": "VERY_LOW",
"block": "HIGH", "sendTcpReset": "HIGH", "saveFile": "DISABLED" } }, { "fileType": "Compressed Files",
"malwareEngines": [ { "name": "GTI File Reputation", "id": 1, "status": "DISABLED" }, { "name": "Custom
Fingerprints", "id": 2, "status": "DISABLED" }, { "name": "PDF Analysis", "id": 8, "status": "DISABLED" },
{ "name": "Anti-Malware Analysis", "id": 16, "status": "UNCHECKED" } ], "actionThresholds": { "alert":
"VERY_LOW", "block": "HIGH", "sendTcpReset": "HIGH", "saveFile": "DISABLED" } } ] }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	2501	Invalid advanced malware policy id/ policy not visible to this domain

Get Malware Policies in a Domain

This URL gets the list of malware policies defined in a particular domain.

Resource URL

GET /domain/<domain_id>/malwarepolicy

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`advancedMalwareListAtDomain`	List of malware policies defined in the domain	Array

Details of object in advancedMalwareListAtDomain:

Field Name	Description	Data Type
`policyId`	Malware policy unique id	Number
`policyName`	Name of the malware policy	String
`visibleToChild`	Is policy visible to child domains	Boolean
`description`	Policy description	String
`isEditable`	Is policy editable	Boolean
`lastModUser`	Last user that modified the policy	String
`lastModTime`	Last time the policy was modified	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/domain/0/malwarepolicy

Response

```
{ "advancedMalwareListAtDomain": [ { "policyId": 1, "policyName": "Default Malware Policy", "lastModifiedUser":
"admin", "visibleToChild": true, "isEditable": true, "lastModifiedTime": "2012-09-13 15:11:21.0" },
{ "policyId": 301, "policyName": "Test1", "description": "Desc1", "lastModifiedUser": "admin", "visibleToChild":
true, "isEditable": true, "lastModifiedTime": "2012-09-13 16:06:06.0" }, { "policyId": 302, "policyName":
"Test2", "description": "Desc2", "lastModifiedUser": "admin", "visibleToChild": false, "isEditable": true,
"lastModifiedTime": "2012-09-13 16:06:14.0" } ] }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Get Default Protocol List

This URL gets the default protocol list.

Resource URL

GET /malwarepolicy/malwareprotocols

Request Parameters

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`advancedMalwareProtocols`	List of objects containing protocol details	Array

Details of object in advancedMalwareProtocols:

Field Name	Description	Data Type
`protocolName`	Type of the file	String
`enabled`	Is protocol enabled	Boolean
`protocolNumber`	Protocol number	Number

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/malwarepolicy/malwareprotocols

Response

```
{ "advancedMalwareProtocols": [ { "protocolName": "HTTP", "protocolNumber": 16, "enabled": true },
{ "protocolName": "SMTP", "protocolNumber": 12, "enabled": false } ] }
```

Error Information

None

Get Default Scanning Option Configuration List

This URL gets the default scanning option configuration list.

Resource URL

GET /malwarepolicy/defaultscanningoptions

Request Parameters

None

Response Parameters

Following fields are returned

Field Name	Description	Data Type
`defaultscanningoptions`	List of objects containing scanning option details	Array

Details of object in defaultscanningoptions:

Field Name	Description	Data Type
`fileType`	Type of the file	String
`malwareEngines`	List of malware engines supported	Array
`actionThresholds`	Action threshold details	Object

Details of object in malwareEngines:

Field Name	Description	Data Type
`Name`	Malware engine name	String
`Status`	Status can be DISABLED/UNCHECKED/ CHECKED	String
`id`	Malware engine id	Number

Details of actionThresholds:

Field Name	Description	Data Type
`alert`	Alert to be sent, can be "DISABLED" / "VERY_LOW" number/ "LOW" / "MEDIUM" / "HIGH" / "VERY_HIGH"	String
`block`	Blocking settings, can be "DISABLED" / "VERY_LOW" / "LOW" / "MEDIUM" / "HIGH" / "VERY_HIGH"	String
`sendTcpReset`	Send TCP reset, can be "DISABLED" / "VERY_LOW" / "LOW" / "MEDIUM" / "HIGH" / "VERY_HIGH"	String
`saveFile`	Save file can be "DISABLED" / "ALWAYS" /"VERY_LOW" / "LOW" / "MEDIUM" / "HIGH" / "VERY_HIGH"	String

Field Name	Description	Data Type
`addToBlockList`	Add to block list can be "DISABLED" / "VERY_LOW" / "LOW" / "MEDIUM" / "HIGH" / "VERY_HIGH"	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/malwarepolicy/defaultscanningoptions

Response

```
{ "scanningOptions": [ { "fileType": "Executables", "malwareEngines": [ { "name": "GTI File Reputation", "id":
1, "status": "CHECKED" }, { "name": "Custom Fingerprints", "id": 2, "status": "UNCHECKED" }, { "name": "PDF
Analysis", "id": 8, "status": "DISABLED" }, { "name": "Anti-Malware Analysis", "id": 16, "status":
"UNCHECKED" } ], "actionThresholds": { "alert": "LOW", "block": "HIGH", "sendTcpReset": "HIGH", "saveFile":
"DISABLED" } }, { "fileType": "MS Office Files", "malwareEngines": [ { "name": "GTI File Reputation", "id": 1,
"status": "DISABLED" }, { "name": "Custom Fingerprints", "id": 2, "status": "CHECKED" }, { "name": "PDF
Analysis", "id": 8, "status": "DISABLED" }, { "name": "Anti-Malware Analysis", "id": 16, "status":
"CHECKED" } ], "actionThresholds": { "alert": "MEDIUM", "block": "HIGH", "sendTcpReset": "HIGH", "saveFile":
"DISABLED" } }, { "fileType": "PDF Files", "malwareEngines": [ { "name": "GTI File Reputation", "id": 1,
"status": "CHECKED" }, { "name": "Custom Fingerprints", "id": 2, "status": "UNCHECKED" }, { "name": "PDF
Analysis", "id": 8, "status": "CHECKED" }, { "name": "Anti-Malware Analysis", "id": 16, "status": "CHECKED" } ],
"actionThresholds": { "alert": "VERY_LOW", "block": "HIGH", "sendTcpReset": "HIGH", "saveFile": "DISABLED" } },
{ "fileType": "Compressed Files", "malwareEngines": [ { "name": "GTI File Reputation", "id": 1, "status":
"DISABLED" }, { "name": "Custom Fingerprints", "id": 2, "status": "DISABLED" }, { "name": "PDF Analysis", "id":
8, "status": "DISABLED" }, { "name": "Anti-Malware Analysis", "id": 16, "status": "UNCHECKED" } ],
"actionThresholds": { "alert": "VERY_LOW", "block": "HIGH", "sendTcpReset": "HIGH", "saveFile":
"DISABLED" } } ] }
```

Error Information

None

Get Blocked Hashes

This URL gets the list of blocked hashes.

Resource URL

GET / advancedmalware/blockedhashes?search=<search_string>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`Search`	Search string	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`blockedHashList`	List of blocked hashes	Array

Details of blockedHashList:

Field Name	Description	Data Type
`filehash`	File hash	String
`fileName`	File name	String

Field Name	Description	Data Type
`lastUpdated`	Last updated details. Contains the username and the time under which the file hash was added.	String
`comment`	Comment	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi%20advancedmalware/blockedhashes

Response

```
{ "blockedHashList": [ { "fileHash":"1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa16", "fileName":"file1", “lastUpdated”:
“2018-01-17 20:30:34.0 (Administrator)” "comment":"Blocked based on user request "},
{ "fileHash":"1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa18", "fileName":"file2", “lastUpdated”: “2018-01-17 20:35:36.0
(Administrator)” "comment":"Blocked based on user request "}, ]} }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4904	Failed to retrieve data

Get Allowed Hashes

This URL gets the list of allowed hashes.

Resource URL

GET /advancedmalware/allowedhashes?search=<search_string>

Request Parameters

Field Name	Description	Data Type	Mandatory
`Search`	Search string	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`allowedHashList`	List of allowed hashes	Array

Details of allowedHashList:

Field Name	Description	Data Type
`filehash`	File hash	String
`fileName`	File name	String
`classifier`	Classifier	String

Field Name	Description	Data Type
`classified`	Classified	String
`commet`	Comment	String

Example

Request

GET https://%3C%20NSM_IP%3E/sdkapi%20advancedmalware/allowedhashes

Response

```
{ "allowedHashList": [{ "fileHash":"1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa17",
"fileName":"1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa17", "classifier":"Manually updated by Administrator",
"classified":"2013-09-03 12:56:48.0", "comment":"allowed based on user request "}]} }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4904	Failed to retrieve data

Action on Blocked Hash

This URL moves the given hashes into allow.

Resource URL

PUT /advancedmalware/blockedhashes/<hash>/takeaction/allow

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`hash`	Hash	String	Yes

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status	Number

Example

Request

PUT

https://<NSM_IP>/sdkapi/advancedmalware/blockedhashes/1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa16/takeaction/allow

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4903	Invalid action
2	400	3401	Invalid hash

Action on Allowed Hash

This URL to perform the action, move the hashes into blocked or unclassified.

Resource URL

PUT /advancedmalware/allowedhashes/<hash>/takeaction/<action>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`hash`	Hash	String	Yes
`action`	Action can be block/ unclassified	String	Yes

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/advancedmalware/allowedhashes/1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa17/takeaction/block

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4903	Invalid action
2	400	3401	Invalid hash

Action on Multiple Blocked Hashes

This URL moves the given hashes into allow list.

Resource URL

PUT /advancedmalware/blockedhashes/multipleHash/takeaction/allow

Request Parameters

URL Parameters: None

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`hashes`	List of file hashes	StringList	Yes

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/advancedmalware/blockedhashes/multipleHash/takeaction/allow

Payload

```
{ "hashes": ["1aaaaaaaaaaaaaaaaaaaaaaaaaaaa16, "1aaaaaaaaaaaaaaaaaaaaaaaaaaaa17",
"1aaaaaaaaaaaaaaaaaaaaaaaaaaaa18"] }
```

Response

```
{ “status”:1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4903	Invalid action
2	400	3401	Invalid hash

Action on Multiple Allowed Hashes

This URL moves the given hashes into block list.

Resource URL

PUT /advancedmalware/allowedhashes/multipleHash/takeaction/block

Request Parameters

URL Parameters: None

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`hashes`	List of file hashes	StringList	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/advancedmalware/allowedhashes/multipleHash/takeaction/block

Payload

```
{ "hashes": ["1aaaaaaaaaaaaaaaaaaaaaaaaaaaa16, "1aaaaaaaaaaaaaaaaaaaaaaaaaaaa17",
"1aaaaaaaaaaaaaaaaaaaaaaaaaaaa18"] }
```

Error Information

Response

```
{ "status": 1 }
```

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4903	Invalid action
2	400	3401	Invalid hash

Remove All Blocked Hashes

This URL to removes all the blocked hashes.

Resource URL

PUT /advancedmalware/blockedhashes/takeaction/removeall

Request Parameters

N/A

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/advancedmalware/blockedhashes/takeaction/removeall

Response

```
{ “status”:1 }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4903	Invalid action

Remove All Allowed Hashes

This URL removes all the allowed hashes.

Resource URL

PUT /advancedmalware/allowedhashes/takeaction/removeall

Request Parameters

N/A

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/advancedmalware/allowedhashes/takeaction/removeall

Response

```
{ "status":1 }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4903	Invalid action

Add FileHash to Blocklist or Allowlist

This URL adds the filehash to either the blocklist or allowlist.

Resource URL

POST /advancedmalware?type=<hashtype>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`type`	Hashtype. Can be allow or block.	String	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`filehash`	File hash	String	Yes
`Filename`	File name	String	No
`comment`	Comment	String	No

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	CreatedResourceId: Set to 1 if the operation was successful.	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/advancedmalware?type=block

Payload

```
{ "fileHash":"1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa16", "fileName":"file1", "comment":"Blocked filehash " }
```

Error Information

Response

```
{ "createdResourceId": 1 }
```

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Hash value is required
2	500	1003	Invalid file hash. It should be a 32-digit hexadecimal value.
3	500	1005	This hash already exists on the allowlist/blocklist.
4	500	1004	Duplicate hash detected. A file with the same hash already exists on this list.
5	500	1001	File hashes entries has exceeded the maximum support limit of 99,000.

Update Details of File Hash

This URL updates details of the allowed or blocked file hash.

Resource URL

PUT /advancedmalware?type=<hashtype>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`type`	Hashtype. Can be allow or block.	String	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`oldFileHash`	Old file hash value	String	Yes
`filehash`	New file hash value	String	No
`filename`	File name	String	No
`comment`	Comment	String	No

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status. Set to 1 if the operation was successful.	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/advancedmalware?type=block

Payload

```
{ “oldFileHash”: "1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa16" "fileHash":"1aaaaaaaaaaaaaaaaaaaaaaaaaaa1116",
"fileName":"file1", "comment":"updated Blocked filehash " }
```

Error Information

Response

```
{ "status": 1 }
```

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Hash value is required
2	500	1003	Invalid file hash. It should be 32-digit hexadecimal value.
3	500	1005	This hash already exists on the allowlist/blocklist.
4	500	1004	Duplicate hash detected. A file with same hash already exists on this list.
5	500	1001	Please provide old hash value.

Delete Some File Hashes from Blocklist or Allowlist

This URL deletes the domain name exceptions specified in the string list.

Resource URL

DELETE /advancedmalware?type=block

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`type`	Hashtype. Can be allow or block.	String	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`hashes`	List of file hashes	StringList	Yes

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status. Set to 1 if the operation was successful.	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/advancedmalware?type=block

Payload

```
{ "hashes": ["1aaaaaaaaaaaaaaaaaaaaaaaaaaaa16, "1aaaaaaaaaaaaaaaaaaaaaaaaaaaa17",
"1aaaaaaaaaaaaaaaaaaaaaaaaaaaa18"] }
```

Error Information

Response

```
{ "status": 1 }
```

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: Internal server error

Import GTI Configuration

This URL updates the severity for GTI.

Resource URL

PUT /domain/<domain_id>/filereputation/gti

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`Sensitivity`	Sensitivity type can be "VERY_LOW"/"LOW"/"MEDIUM"" /"HIGH"/"VERY_HIGH"	String	Yes
`inheritSettings`	Inherit settings from parent domain. Default is true	Boolean	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status returned by updation	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/domain/0/filereputation/gti

Payload:

```
{ "Sensitivity":"LOW" "inheritSettings":false }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	404	3101	Cannot inherit setting for root domain

Import Allowed Fingerprints

This URL imports the list of allowed fingerprints to the Manager.

Resource URL

PUT /domain/<domain_id>/filereputation/allowedfingerprints

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
MultiPart	It holds the body parts object	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	It holds the finger print action object	Application/json	Yes

Details of FingerPrintAction:

Field Name	Description	Data Type	Mandatory
Action	Action type, can be "APPEND"/ "REPLACE"	String	Yes

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
BodyPart1]	It holds the .csv file as input stream	Application/octet-stream	Yes

Details of file:

Field Name	Description	Data Type	Mandatory
File	Input Stream of the csv file	ByteArrayInput Stream	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Status returned by updation	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/domain/0/filereputation/allowedfingerprints

Payload:

```
NSM-SDK-API: RERFNUIyODFCQTdGRDM1MTRBQTA4QzAwQUQ4MzAwQjE6MQ== Accept: application/vnd.nsm.v1.0+json Content-
Type: multipart/form-data; boundary=Boundary_6_13995234_1360146256146 MIME-Version: 1.0 User-Agent: Java/
1.6.0_25 Host: 127.0.0.1:8888 Connection: keep-alive Content-Length: 3949 --Boundary_6_13995234_1360146256146
Content-Type: application/json {"Action":"REPLACE"} --Boundary_6_13995234_1360146256146 Content-Type:
application/octet-stream H¡EÀ¶¡Qoø¼Ä¨tTÐc[pbñšB=ã ¥Lh;bê²gà-*Äe#ÈÃñõ-1€>!´Øùþ&ck¾â•)9R-ë?0Ÿ¡°]‘3 9 ütþù9o
\Ð…'ãž¦}à!ÿDŠ-Wå‡´ê¬_”v`©BÈ□e8Ã□J=L=ÕÝc□¤Â˜ˆ¸‡u%§?,Sämá†6AÕôŽ¹‰×L-•e«®ÖôÔ©Ä®àýò□ŒI5)‰5a7¥P¾£□Öñú□,xœÕEieÓ°
«Q{îB□□9¬ëX†®%‰-îlÄ/9□q¸ÑÞð3;ËZNq(é{h+ò7Y,á‰«ËvOâazÎGöi"à‘êŒâª6õ]²BÈ,…KU[Šâ«FA^□[gÝI”•F|ý Qe□’Y},6Ø¾m ÒQ£VÄ’
°É«ûú >\'HÐ › ;¥žód»,‡,3oÉæßõe,òöd[®Ýg-ðËÝE '0•+Õµ(-Ú›íKSöö•□eß>ß”Z6l2¸"Âä±ÄR+ |g ¿□P,ÝÑÄú4jÆ¡ÒO’îOi+^VaÄO
±K8ØáTÙè□_ˆY=êN¼?ÞµÏ¬£+Óo÷~uNvG=†•»ËÉ.†ŒÓ¬>vðA?\®°È—(Mc¯U,¼tXÊ¡+|)¶úV€²"e¿Z¬]‘□z-Jó\]Iõ€□Ô sµ ŸT\°ÿ”…¸ÇiVˆíˆÒÆü
¥}Tç÷Íõ„›ĪcoM,_1>¾□‡¢]¨£/ôÈ—}ÞÁ8NA□j m…JÇÇc•í <□eÚ+Å□Ya --Boundary_6_13995234_1360146256146 Response
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1101	Internal server error
2	404	1105	Invalid domain

Delete Allowed Fingerprints

This URL deletes the allowed fingerprints imported in the Manager.

Resource URL

DELETE /domain/<domain_id>/filereputation/allowedfingerprints

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status returned by deletion	Number

Example

Request

DELETE https://%3CNSM_IP%3E/sdkapi/domain/0/filereputation/allowedfingerprints

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1105	Invalid domain
2	400	2801	No custom finger prints to delete

Import Custom Fingerprints

This URL imports the list of blocked fingerprints to the Manager.

Resource URL

PUT /domain/<domain_id>/filereputation/customfingerprints

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`MultiPart`	It holds the body parts object	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
`BodyPart[0]`	It holds the finger print action object	Application/json	Yes

Details of finger print action:

Field Name	Description	Data Type	Mandatory
`Action`	Action type can be "APPEND"/ "REPLACE"	String	Yes

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
`BodyPart1]`	It holds the .csv file as input stream	Application/octet-stream	Yes

Details of file:

Field Name	Description	Data Type	Mandatory
`File`	Input stream of the csv file	ByteArrayInput Stream	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status returned by updation	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/domain/0/filereputation/customfingerprints

Payload:

```
NSM-SDK-API: OEZDNzAwNUQ3OTM2MjUzM0I3QTBBREQ4MENFMzExMTM6MQ== Accept: application/vnd.nsm.v1.0+json Content-
Type: multipart/form-data; boundary=Boundary_1_21363001_1362483936674 MIME-Version: 1.0 User-Agent: Java/
1.6.0_25 Host: localhost:8888 Connection: keep-alive Content-Length: 348 --Boundary_1_21363001_1362483936674
Content-Type: application/json {"Action":"REPLACE"} --Boundary_1_21363001_1362483936674 Content-Type:
application/octet-stream collectmail_notwo0a.pdf,1,MD5,075c8160789eb0829488a4fc9b59ed6c,description
putty_v0.60.exe,1,MD5,acdac6399f73539f6c01b7670045eec7,desc --Boundary_1_21363001_1362483936674--
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1101	Internal server error
2	404	1105	Invalid domain

Delete Custom Fingerprints

This URL deletes the custom fingerprints imported in the Manager.

Resource URL

DELETE /domain/<domain_id>/filereputation/customfingerprints

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status returned by deletion	Number

Example

Request

DELETE https://%3CNSM_IP%3E/sdkapi/domain/0/filereputation/customfingerprints

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1105	Invalid domain
2	400	2801	No custom finger prints to delete

Manage Custom File Types

This URL provides the supported file types/formats to be scanned.

Resource URL

PUT /domain/<domain_id>/filereputation/filetypes

Request Parameters:

URL parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Payload parameters:

Field Name	Description	Data Type	Mandatory
`fileStatus`	List of file formats and their status	ObjectList	Yes

Details of fileStatus:

Field Name	Description	Data Type	Mandatory
`fileType`	List of file formats and their status	Object	No

Details of fileType:

Field Name	Description	Data Type	Mandatory
`fileFormat`	File format	String	Yes
`enabled`	File format status, default is true	Boolean	No

Response Parameters

Field Name	Description	Data Type
`status`	Status returned by updation	Number

Example

Request

PUThttps://%3CNSM_IP%3E/sdkapi/domain/0/filereputation/filetypes

Payload:

```
{ "fileStatus": [ { "fileFormat": "apk", "enabled": true }, { "fileFormat": "cpl", "enabled": true },
{ "fileFormat": "doc", "enabled": false }, { "fileFormat": "docx", "enabled": false }, { "fileFormat": "drv",
"enabled": false }, { "fileFormat": "exe", "enabled": false }, { "fileFormat": "ocx", "enabled": false },
{ "fileFormat": "pdf", "enabled": false }, { "fileFormat": "ppt", "enabled": false }, { "fileFormat": "pptx",
"enabled": false }, { "fileFormat": "scr", "enabled": false }, { "fileFormat": "sys", "enabled": false },
{ "fileFormat": "xls", "enabled": false }, { "fileFormat": "xlsx", "enabled": false } ] }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1101	Internal error
2	404	1105	Invalid domain
3	404	1105	Invalid domain: This operation is only allowed for root domain
4	400	7001	File format is not valid

Number of Fingerprints in Use

This URLs provides the count of custom and allowed fingerprints in use.

Resource URL

GET /domain/<domain_id>/filereputation/fingerprintscount

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
AllowedFingerprintsCount	Number of allowed fingerprints in use	Number
CustomFingerprintsCount	Number of custom fingerprints in use	Number

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/domain/0/filereputation/fingerprintscount

Response

```
{ " AllowedFingerprintsCount ": 0, " CustomFingerprintsCount ": 10 }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1105	Invalid domain

Get Custom File Types

This URLs provides the custom file types.

Resource URL

GET /domain/<domain_id>/filereputation/filetypes

Request Parameters:

URL parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
fileStatus	List of file formats and their status	ObjectList

Details of fileStatus:

Field Name	Description	Data Type
`fileType`	List of file formats and their status	Object

Details of fileType:

Field Name	Description	Data Type
`fileFormat`	File format	String
`enabled`	File format status, default is true	boolean

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/domain/0/filereputation/filetypes

Payload:

```
{ "fileStatus": [ { "fileFormat": "apk", "enabled": true }, { "fileFormat": "cpl", "enabled": true },
{ "fileFormat": "doc", "enabled": false }, { "fileFormat": "docx", "enabled": false }, { "fileFormat": "drv",
"enabled": false }, { "fileFormat": "exe", "enabled": false }, { "fileFormat": "ocx", "enabled": false },
{ "fileFormat": "pdf", "enabled": false }, { "fileFormat": "ppt", "enabled": false }, { "fileFormat": "pptx",
"enabled": false }, { "fileFormat": "scr", "enabled": false }, { "fileFormat": "sys", "enabled": false },
{ "fileFormat": "xls", "enabled": false }, { "fileFormat": "xlsx", "enabled": false } ] }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1105	Invalid domain
2	404	1105	Invalid domain: This operation is only allowed for root domain

Get GTI File Types

This URLs provides the GTI file types.

Resource URL

GET /domain/<domain_id>/filereputation/gti/filetypes

Request Parameters:

URL parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
fileFormat	File format	StringList

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/filereputation/gti/filetypes

Response

```
{ "fileFormat": [ "apk", "cpl", "drv", "exe", "ocx", "pdf", "scr", "sys" ] }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1105	Invalid domain

Get Severity for GTI

This URLs provides the severity for GTI.

Resource URL

GET /domain/<domain_id>/filereputation/gti

Request Parameters:

URL parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
Sensitivity	Sensitivity for GTI	String
inheritSettings	Inherit settings from parent domain	Boolean

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/filereputation/gti

Response

```
{ "inheritSettings": false, "Sensitivity": "VERY_LOW" }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1105	Invalid domain

Update Alert Relevance

This URL enables or disables alert relevance on the Manager.

Resource URL

PUT /alertrelevance

Request Parameters

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`isEnabled`	Is alert relevance enabled or not	Boolean	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status returned on updation	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/alertrelevance

Payload:

```
{ "isEnabled":true }
```

Response

```
{ "status":1 }
```

Get Alert Relevance

This URL gets the current status of alert relevance on the Manager.

Resource URL

GET /alertrelevance

Request Parameters

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`isEnabled`	Is alert relevance enabled	Boolean

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/alertrelevance

Response

```
{ "isEnabled":true }
```

Automatic Botnet File Download to Manager

This URL automatically downloads the latest botnet file from Update Server to the Manager.

Resource URL

PUT /botnetdetectors/import/automatic

Request Parameters

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status returned by updation	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/botnetdetectors/import/automatic

Response

```
{ "status":1 }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1001	internal error

Manual Botnet File Import to Manager

This URL imports the botnet file manually to the Manager.

Resource URL

PUT /botnetdetectors/import/manual

Request Parameters

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`MultiPart`	Holds the body part objects	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
`BodyPart[0]`	Holds the file format object	Application/json object	Yes

Details of file format:

Field Name	Description	Data Type	Mandatory
`fileName`	Name of the file	String	Yes
`type`	File type should be "ZIP"	String	Yes

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
`BodyPart[1]`	Holds the file as input stream	Application/octet-stream	Yes

Details of .zip file:

Field Name	Description	Data Type	Mandatory
`File`	botnet file input stream	ByteArrayInput Stream	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Status returned by the update	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/botnetdetectors/import/manual

Payload:

```
NSM-SDK-API: QkI2Q0Y4NjgxNzUzNkY0RTc5Qjc5NUJCRUFCRUZEOUM6MQ== Accept: application/vnd.nsm.v1.0+json Content-
Type: multipart/form-data; boundary=Boundary_1_13198090_1360147081930 MIME-Version: 1.0 User-Agent: Java/
1.6.0_25 Host: 127.0.0.1:8888 Connection: keep-alive Content-Length: 307803 --Boundary_1_13198090_1360147081930
Content-Type: application/json {"fileName":"botnet_sdkapi","type":"ZIP"} --Boundary_1_13198090_1360147081930
Content-Type: application/octet-stream 3WA«^JY header.json{"sha1": "d37a91be6f92f2620bf0bf0bdba985a2eecced94",
"file-length": 229869, "iv": "D+grgU2y12NHI/OFt8LaRVzP0an/1Fwin8TWhuGIS4aQYfjBhZEQLTzmUGxYjePyPC+v6fQoDfEp
\nT5qHAaZX4xn5b1gdeR9iQgIx9mui2hkHEd2zxaLwzzS/1mWOYbvoKO4DPxYpT3UdDFxhe5nd8PPI
\nCGkDMExlmo2OwHjxiuUIwOOZfGEeA1SVHf8DiGKsmv25WVjF7LsTndRpeksyWyQX1/WESlnC+VkE
\nOaJK6l4DBCfzror7GuFADOKIPcGeZzgUCn/EMYfG/QhFw2vfu+OVub4f6qJZB6fDBn1li8KL+DQ5\niDCI/Gq6zCIGksHPFJ9W
+RN1RdlKVIkATdkkQQ==\n", "version": 31.0, "key": "sFXb40h4vS6dWlaynBPdojhuXJDv9WoN1Jh0ts5+G9x9siDy/
tMwGo9U8pxoLveHJKu7mspI5nL5\nxFI8rR8EMzHjdeO9c9qMs/x6djhKpDn8LQDQT03zdIW5QXwt5uA2tByLAOoKK5LKsveApJzqJMGw\nu/
20sgvouKBLESGVE1WTZ1rlRWC6JPQ5l6ZzkW4kkjtcqGbqSnATipJmyKD2a5sAztXpp7vpNOrK\nGUHH8jViWzgwnzlgW/
8IcypQdCwFiYWnU2lDBzkBx24ROd/D7CavlBHBDUU6vvoeX6mtJLm0UcBN\nHZX/rLmVlqS4hWn79e6F+lkB9/+LntizVRb57g==\n", "date":
1350968439, "file-type": 1} --Boundary_1_13198090_1360147081930
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1001	internal error
2	400	3001	Botnet supports only .zip file format

Manual Signature Set Import to Manager

This URL imports the signature set file manually to the Manager.

Resource URL

PUT /signatureset/import/manual

Request Parameters

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`MultiPart`	Holds the body part objects	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
`BodyPart[0]`	Holds the file format object	Application/json object	Yes

Details of file format:

Field Name	Description	Data Type	Mandatory
`fileName`	Name of the file	String	Yes
`type`	File type can be "JAR"\"IVU"	String	Yes

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
`BodyPart1]`	Holds the file as input stream	Application/octet-stream	Yes

Details of . jar/.ivu file:

Field Name	Description	Data Type	Mandatory
`File`	Signature set file input stream	ByteArrayInput Stream	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Status returned by updation	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/signatureset/import/manual

Payload:

```
NSM-SDK-API: QjUzNDQzMjNCNUQ2NkEzQjc4Mzc5REMxRjMxMDg0OTE6MQ== Accept: application/vnd.nsm.v1.0+json Content-
Type: multipart/form-data; boundary=Boundary_1_17241377_1362484380857 MIME-Version: 1.0 User-Agent: Java/
1.6.0_25 Host: localhost:8888 Connection: keep-alive Content-Length: 15956464 --
Boundary_1_17241377_1362484380857 Content-Type: application/json
{"fileName":"siganturesets_sdkapi","type":"JAR"} --Boundary_1_17241377_1362484380857 Content-Type: application/
octet-stream ÒrÝ?ü0¥ÿ<^}c,¢eXœ^:4 JhÍ2µ□rDYñÇÚd¶/Â¿í□F~ ÆIc§¼ēá©ÿ_8Öø«¯C6Ô654îÞg‘J6?x,*T2¡qhã4ÎÅVµ¬Gƒo9ŸCÒª„í¹Ì
—Áë&1¹ì,Ú‹yì^î‘Vö5U.kÝ$±Ñ g§zï0□wÌ [:…œ`Žíì’DŒ¾¸xŒ7è□L“t"á}ñÕùA‡B6W¦P!;Ð?j*;G¾=X¦Š1s(□ì_œ8•¯Ð"®ƒMîQ,®UÉÔ`7»©2xN
£o†¾$h;ÕeÆÄŸ0ÀÑÄ¦ûNü,1”1Sõ±œ'n¨$èŒ`I¤@ã¥?$^hé_gÙÎ□4L[gàÏ©:•ŒÔ òH‰KÃïÃÒ"ÑÆ*¼²žØ|r-Þ„”¶K¥*¾¬□k}ddZ¡□ßÔ
¥dK9¥Ð¾ýÎk“{Oj□- ¾€ýb3ÔÏ&«PƒTF âê¡,4Â{0ä!ÈÝ]ðā[”¿1•!;d³_ --Boundary_1_17241377_1362484380857--
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1001	internal error
2	400	3002	Signature set supports .ivu and .jar file formats
3	400	3004	Specified signature set version is not supported or EMS already has this update version
4	400	3005	Invalid signature set file

Manual Device Software Import to Manager

This URL imports the device software file manually to Manager.

Resource URL

PUT /devicesoftware/import/manual

Request Parameters

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`MultiPart`	Holds the body part objects	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
`BodyPart[0]`	Holds the file format object	Application/json object	Yes

Details of file format:

Field Name	Description	Data Type	Mandatory
`fileName`	Name of the file	String	Yes

Field Name	Description	Data Type	Mandatory
`type`	File type should be "JAR"	String	Yes

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
`BodyPart1]`	Holds the file as input stream	Application/octet-stream	Yes

Details of .jar file:

Field Name	Description	Data Type	Mandatory
`File`	Device software input stream	ByteArrayInput Stream	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status returned by updation	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/devicesoftware/import/manual

Payload:

```
NSM-SDK-API: QjUzNDQzMjNCNUQ2NkEzQjc4Mzc5REMxRjMxMDg0OTE6MQ== Accept: application/vnd.nsm.v1.0+json Content-
Type: multipart/form-data; boundary=Boundary_1_17241377_1362484380857 MIME-Version: 1.0 User-Agent: Java/
1.6.0_25 Host: localhost:8888 Connection: keep-alive Content-Length: 15956464 --
Boundary_1_17241377_1362484380857 Content-Type: application/json {"fileName":"software_sdkapi","type":"JAR"} --
Boundary_1_17241377_1362484380857 Content-Type: application/octet-stream ÒrÝ?ü0¥ÿ<ˆ}c,¢eXœ^:4 JhÍ2µ□rDYñÇÚd¶/
Â¿í□F~ ÆIc§¼éá©ÿ_8Öø« C6Ô654îÞg‛J6?x,*T2¡qhã4ÎÅVµ¬Gƒo9ŸCÒª„í¹Ì —Áë&1¹ì,Ú‹yì^î‛Vö5U.kÝ$±Ñ g§zï0□wÌ [:…
œ`Žíì’DŒ¾¸xŒ7è□L‶t"á}ñÕùA‡B6W¦P!;Ð?j*;G¾=X¦Š1s(□ì_œ8•¯Ð"®ƒMîQ,®UÉÔ`7»©2xN£o†¾$h;ÕeÆÄŸ0ÀÑÄ¦ûNü,1”1Sõ±œ'n¨$èŒ`I¤@ã
¥?$ˆhé_gÙÎ□4L[gàÏ©:•ŒÔ òH‰KÃïÃÒ"ÑÆ*¼²žØ|r-Þ„”¶K¥*¾¬□k}ddZ¡□ßÔ ¥dK9¥Ð¾ýÎk‟{Oj□- ¾€ýb3ÔÏ&«PƒTF âê¡,4Â{0ä!ÈÝ]ðä[”
¿1•!;d³_ --Boundary_1_17241377_1362484380857--
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1001	internal error
2	400	3003	Device software supports only .jar file format

Get the Device Software's Available in the Server

This URL gets the device software's available in the server.

Resource URL

GET /devicesoftware/versions

Request Parameters

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`downloadedVersions`	Device software's present in the Manager	Array
`availableVersions`	Device software's available in the server for download	Array

Details of objects under downloadedVersions:

Field Name	Description	Data Type
`model`	Sensor model	String
`versions`	List of downloaded versions	Array

Details of objects under availableVersions:

Field Name	Description	Data Type
`model`	Sensor model	String
`versions`	List of downloaded versions	Array

Details of objects under versions of availableVersions:

Field Name	Description	Data Type
`version`	Version number	String
`releaseDate`	Release date	String
`fileSize`	Size of the file	String
`isFIPSCompliant`	Is the image FIPS compliant	Boolean

Example

Request

GET https://<NSM_IP>/sdkapi/devicesoftware/versions

Response

```
{ "downloadedVersions": [ { "model": "IPS-NS5100", "versions": [ "10.1.5.75" ] }, { "model": "IPS-NS9200",
"versions": [ "10.1.5.75" ] } ], "availableVersions": [ { "model": "M-8000", "versions": [ { “version”:
“9.1.3.18”, “releaseDate”: “10-Oct-2020”, “fileSize”: “59.79 MB”, “isFIPSCompliant”: false }… ] },…. }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1001	internal error

Manual Gateway Anti-Malware File Import to Manager

This URL imports the Gateway Anti-Malware file manually to Manager.

Resource URL

PUT /gam/import/manual

Request Parameters

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`MultiPart`	Holds the body part objects	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
`BodyPart[0]`	Holds the file format object	Application/json object	Yes

Details of file format:

Field Name	Description	Data Type	Mandatory
`fileName`	Name of the file	String	Yes
`type`	File type should be "UPD"	String	Yes

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
`BodyPart1]`	Holds the file as input stream	Application/octet-stream	Yes

Details of .upd file:

Field Name	Description	Data Type	Mandatory
`File`	Gateway Anti-Malware engine data input stream	ByteArrayInput Stream	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Status returned by updation	number

Example

Request

PUT https://<NSM_IP>/sdkapi/gam/import/manual

Payload:

```
NSM-SDK-API: QjUzNDQzMjNCNUQ2NkEzQjc4Mzc5REMxRjMxMDg0OTE6MQ== Accept: application/vnd.nsm.v1.0+json Content-
Type: multipart/form-data; boundary=Boundary_1_17241377_1362484380857 MIME-Version: 1.0 User-Agent: Java/
1.6.0_25 Host: localhost:8888 Connection: keep-alive Content-Length: 15956464 --
Boundary_1_17241377_1362484380857 Content-Type: application/json {"fileName":"software_sdkapi","type":"JAR"} --
Boundary_1_17241377_1362484380857 Content-Type: application/octet-stream //file data input stream --
Boundary_1_17241377_1362484380857--
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1001	internal error
2	400	3007	Gateway Anti-Malware update supports only UPD file format

Download the Device Software from the Server

This URL downloads the device software from the server.

Resource URL

PUT /devicesoftware/import/automatic

Request Parameters

Payload request parameters:

Field Name	Description	Data Type	Mandatory
`model`	Device model for which the download is done	String	Yes
`version`	Software version to download	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status returned by download	Number

Example

PUT https://<NSM_IP>/sdkapi/ devicesoftware/import/automatic

Request

```
Payload: { ‘model’ : ‘M-3050’, ‘version’ : ‘9.1.5.9’ }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1001	Internal error
2	400	3008	Device model and software to update is mandatory
3	400	3009	Device model provided does not exist : <model>
4	400	3010	Software version provided does not exist for the Sensor : (<model>. <version>)
5	400	3011	Software version provided is already present in the Manager.

Get All the Device Software Available in the Server

This URL gets all the device software available in the server.

Resource URL

GET /devicesoftware/versions

Request Parameters

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`downloadedVersions`	All device software present in the Manager	Array
`availableVersions`	All device software available in the server for download	Array

Details of objects under downloadedVersions:

Field Name	Description	Data Type
`model`	Sensor model	String
`versions`	List of downloaded versions	Array

Details of objects under availableVersions:

Field Name	Description	Data Type
`model`	Sensor model	String

Field Name	Description	Data Type
`versions`	List of downloaded versions	Array

Details of objects under versions of availableVersions:

Field Name	Description	Data Type
`version`	Version number	String
`releaseDate`	Release date	String
`fileSize`	Size of the file	String
`isFIPSCompliant`	Is the image FIPS compliant	Boolean

Example

PUT https://<NSM_IP>/sdkapi/devicesoftware/versions

Response

```
{ "downloadedVersions": [ { "model": "IPS-NS5100", "versions": [ "10.1.5.75" ] }, { "model": "IPS-NS9200",
"versions": [ "10.1.5.75" ] } ], "availableVersions": [ { "model": "M-8000", "versions": [ { “version”:
“9.1.3.18”, “releaseDate”: “10-Oct-2020”, “fileSize”: “59.79 MB”, “isFIPSCompliant”: false }… ] },…. }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1001	Internal error

Allow Malware Archive File

This URL adds the file hash to the allow list.

Resource URL

PUT /malwarearchive/action

Request Parameters

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`fileHash`	Holds the hash value of the filename	String	Yes
`action`	Action to be taken "ALLOW"	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status returned by updation	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/malwarearchive/action

Payload:

```
{ "fileHash":" 0bea3f79a36b1f67b2ce0f595524c77c", "action":"ALLOW" }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1001	internal error
2	400	3401	Invalid file hash value

Download Malware File

This URL downloads the malware file as Base64 encoded ByteStream.

Resource URL

GET /malwarearchive/download/<filehash>

Request Parameters

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`filehash`	Hash value of the filename	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`byteStream`	Base64 encoded byte stream of the malware file	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/malwarearchive/download/0bea3f79a36b1f67b2ce0f595524c77c

Response

```
{ "byteStream": "TVqOAQEAAAAEAAAA//
8AALgAAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIHJlcXVpcm
VzIE1pY3Jvc29mdCBXaW5kb3dzLg0KJAAAAAAAAAAABORQU8JgEtAAAAAAABgwMAABQAALIWAgAAAAAAAwADAE8AQABYAOwADQETAdMBAAAHAAQAAA
ACCCQAdhYAAAoDJgBiyVAdYsnoDNtQUB3bUAISKElxDShJBAAFgAQAAAAAAJoWCAAwHGWAAAAAAAKIWGg” }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1001	internal error
2	400	3401	Invalid file hash value

Get List of Archived Malware Files

This URL gets the list of malware files currently archived on the Manager.

Resource URL

GET /malwarearchive/list

Request Parameters

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`ArchiveFileList`	List of archive files available in the Manager	Array

Details of ArchiveFileList:

Field Name	Description	Data Type
`fileHashValue`	Hash value of the file	String
`fileSize`	File size	Number
`fileType`	File type	String
`creationTime`	File creation time	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/malwarearchive/list

Response

```
{ "archiveFileDetails": [ { "fileHashValue": "0bea3f79a36b1f67b2ce0f595524c77c", "fileSize": 94784, "fileType":
"Executables", "creationTime": "Tue Dec 18 21:35:13 IST 2012" }, { "fileHashValue":
"4498f4c53d122c463861bbd3e8b903f7", "fileSize": 91648, "fileType": "Office Files", "creationTime": "Tue Dec 18
21:40:12 IST 2012" }, { "fileHashValue": "d64c92b4a49d7ff50d8e61ee4ea42ee2", "fileSize": 318976, "fileType":
"Office Files", "creationTime": "Tue Dec 18 21:45:12 IST 2012" }, { "fileHashValue":
"0d6054cbbe0ae053fde006f25a0ead61", "fileSize": 1561, "fileType": "Compressed Files", "creationTime": "Tue Dec
18 21:45:12 IST 2012" } ] }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1001	internal error

Delete Malware Archive File

This URL deletes the malware archived files.

Resource URL

PUT /malwarearchive?fileHash=

Query Parameter: ?fileHash=

- Hash value of the file name

Note: If "fileHash" is not defined, all the archived files will be deleted

Request Parameters

Field Name	Description	Data Type	Mandatory
`fileHash`	Hash value of the file name	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status returned by deletion	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/malwarearchive?filehash=0bea3f79a36b1f67b2ce0f595524c77c

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1001	internal error
2	400	3401	Invalid file hash value
3	400	3402	No file to delete

Get Passive Device Profiling Setting at the Domain Level

This URL gets passive device profiling setting at the domain level.

Resource URL

GET /domain/<domain_id>/passivedeviceprofiling

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`inheritSettingsfromParentNode`	Inherit settings from parent node	Boolean
`passiveDeviceProfilingSetting`	Passive device profiling setting	Object

Details of fields in passiveDeviceProfilingSetting:

Field Name	Description	Data Type
`profilingTechniques`	Profiling technique to use for device profiling	Object
`profileExpiration`	Profile expiration duration for re-profiling of a device	Object
`hostInactivityTimerInHrs`	Specifies the duration after which information for a device is considered invalid	Number

Details of fields in profilingTechniques:

Field Name	Description	Data Type
`DHCPEnableStatus`	Enable DHCP for device profiling	Boolean
`TCPEnableStatus`	Enable TCP for device profiling	Boolean
`HTTPEnableStatus`	Enable HTTP for device profiling	Boolean

Details of fields in profileExpiration:

Field Name	Description	Data Type
`duration`	Profile expiration duration	Number

Field Name	Description	Data Type
unit	Profile expiration duration unit, can be "MINUTES" / "HOURS"	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/domain/0/passivedeviceprofiling

Response

```
{ "inheritSettingsfromIPSSettingsNode": false, "passiveDeviceProfilingSetting": { "profilingTechniques":
{ "DHCPEnableStatus": true, "TCPEnableStatus": true, "HTTPEnableStatus": false }, "profileExpiration":
{ "duration": 30, "unit": "MINUTES" }, "hostInactivityTimerInHrs": 2 } }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Update Passive Device Profiling Setting at Domain Level

This URL updates passive device profiling setting at the domain level.

Resource URL

PUT /domain/<domain_id>/passivedeviceprofiling

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
inheritSettingsfromParentNode	Inherit settings from parent node	Boolean	Yes
passiveDeviceProfilingSetting	Passive device profiling setting	Object	Yes

Details of fields in passiveDeviceProfilingSetting:

Field Name	Description	Data Type	Mandatory
profilingTechniques	Profiling technique to use for device profiling	Object	Yes
profileExpiration	Profile expiration duration for re-profiling of a device	Object	Yes

Field Name	Description	Data Type	Mandatory
hostInactivityTimerInHrs	Specifies the duration after which information for a device is considered invalid	Number	Yes

Details of fields in profilingTechniques:

Field Name	Description	Data Type	Mandatory
DHCPEnableStatus	Enable DHCP for device profiling	boolean	Yes
TCPEnableStatus	Enable TCP for device profiling	boolean	Yes
HTTPEnableStatus	Enable HTTP for device profiling	boolean	Yes

Details of fields in profileExpiration:

Field Name	Description	Data Type	Mandatory
duration	Profile expiration duration	Number	Yes
unit	Profile expiration duration unit, can be "MINUTES" / "HOURS"	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Status returned by update	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/domain/0/passivedeviceprofiling

Payload

```
{ "inheritSettingsfromIPSSettingsNode": true, "passiveDeviceProfilingSetting": { "profilingTechniques":
{ "DHCPEnableStatus": true, "TCPEnableStatus": true, "HTTPEnableStatus": false }, "profileExpiration":
{ "duration": 30, "unit": "MINUTES" }, "hostInactivityTimerInHrs": 2 } }
```

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid domain
2	400	3301	Profile expiration value must be between 5 and 59 minutes
3	400	3302	Profile expiration value must be between 1 and 12 hours

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
4	400	3303	Profile expiration value cannot be greater than host inactivity timer
5	400	3304	Please enable at least one profiling technique

Get Passive Device Profiling Setting at Sensor Level

This URL gets passive device profiling setting at the Sensor level.

Resource URL

GET /sensor/<sensor_id>/passivedeviceprofiling

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensor_id	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
inheritSettingsfromParentNode	Inherit settings from parent node	Boolean
passiveDeviceProfilingSetting	Object that contains passive device profiling setting	Object
bindIPForCopiedDHCPTraffic	Bind monitoring port of a Sensor to receive a DHCP traffic with a relay agent	Boolean
bindIPAddressDetails	Object that contains monitoring port details for receiving DHCP traffic	Object
PassiveDeviceProfilingStateForSensor	Passive device profiling state on Sensor	String
interfaceStatusList	List of interfaces with enable status of passive device profiling setting in inbound/outbound direction	Object

Details of fields in passiveDeviceProfilingSetting:

Field Name	Description	Data Type
profilingTechniques	Profiling technique to use for device profiling	Object
profileExpiration	Profile expiration duration for re-profiling of a device	Object

Field Name	Description	Data Type
`hostInactivityTimerInHrs`	Specifies the duration after which information for a device is considered invalid	Number

Details of fields in profilingTechniques:

Field Name	Description	Data Type
`DHCPEnableStatus`	Enable DHCP for device profiling	Boolean
`TCPEnableStatus`	Enable TCP for device profiling	Boolean
`HTTPEnableStatus`	Enable HTTP for device profiling	Boolean

Details of fields in profileExpiration:

Field Name	Description	Data Type
`duration`	Profile expiration duration	Number
`unit`	Profile expiration duration unit, can be "MINUTES" / "HOURS"	String

Details of fields in bindIPAddressDetails:

Field Name	Description	Data Type
`designatedPort`	Monitoring port of a Sensor to receive a DHCP traffic with a relay agent	String
`portIPAddress`	IP address of the monitoring port	String
`networkMask`	Network mask	String
`defaultGateway`	Default gateway	String
`vlanID`	VLAN id	String

Details of object in interfaceStatusList:

Field Name	Description	Data Type
`interfaceId`	Interface id	Number
`interfaceName`	Interface name	String
`enableInbound`	Enable status in inbound direction	Boolean
`enableOutbound`	Enable status in outbound direction	Boolean
`subinterfaceStatusList`	List of sub-interfaces in a particular interface with enable status of passive device profiling in inbound/outbound direction	Object

Details of fields in subinterfaceStatusList:

Field Name	Description	Data Type
`interfaceId`	Interface id	Number
`interfaceName`	Interface name	String
`enableInbound`	Enable status in inbound direction	Boolean
`enableOutbound`	Enable status in outbound direction	Boolean

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/sensor/1001/passivedeviceprofiling

Response

```
{ "inheritSettingsfromIPSSettingsNode": true, "passiveDeviceProfilingSetting": { "profilingTechniques":
{ "DHCPEnableStatus": false, "TCPEnableStatus": false, "HTTPEnableStatus": true }, "profileExpiration":
{ "duration": 10, "unit": "HOURS" }, "hostInactivityTimerInHrs": 11 }, "bindIPForCopiedDHCPTraffic": true,
"bindIPAddressDetails": { "designatedPort": "4A", "portIPAddress": "100.100.100.10", "networkMask":
"255.255.0.0", "defaultGateway": "100.100.100.1", "vlanID": "10" }, "PassiveDeviceProfilingStateForSensor":
"ENABLE_DEVICEPROFILING_FOR_ENTIRE_DEVICE", "interfaceStatusList": [ { "interfaceId": 117, "interfaceName":
"3B", "enableInbound": true, "enableOutbound": true }, { "interfaceId": 105, "interfaceName": "1A-1B",
"enableInbound": true, "enableOutbound": true, "subinterfaceStatusList": [ { "subInterfaceId": 118,
"subInterfaceName": "TestVLAN1", "enableInbound": true, "enableOutbound": true } ] }, { "interfaceId": 104,
"interfaceName": "2A-2B", "enableInbound": true, "enableOutbound": true }, { "interfaceId": 103,
"interfaceName": "3A", "enableInbound": true, "enableOutbound": true }, { "interfaceId": 102, "interfaceName":
"4A-4B", "enableInbound": true, "enableOutbound": true } ] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor

Update Passive Device Profiling Setting at Sensor Level

This URL updates passive device profiling setting at the Sensor level.

Resource URL

PUT /sensor/<sensor_id>/passivedeviceprofiling

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Domain id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`inheritSettingsfromParentNode`	Inherit settings from parent node	Boolean	Yes

Field Name	Description	Data Type	Mandatory
`passiveDeviceProfilingSetting`	Object that contains passive device profiling setting	Object	Yes
`bindIPForCopiedDHCPTraffic`	Bind monitoring port of a Sensor to receive a DHCP traffic with a relay agent	Boolean	Yes
`bindIPAddressDetails`	Object that contains monitoring port details for receiving DHCP traffic	Object	Yes
`PassiveDeviceProfilingStateForSensor`	Passive device profiling state on Sensor	String	Yes
`interfaceStatusList`	List of interfaces with enable status of passive device profiling setting in inbound/ outbound direction	Object	Yes

Details of fields in passiveDeviceProfilingSetting:

Field Name	Description	Data Type	Mandatory
`profilingTechniques`	Profiling technique to use for device profiling	Object	Yes
`profileExpiration`	Profile expiration duration for re-profiling of a device	Object	Yes
`hostInactivityTimerInHrs`	Specifies the duration after which information for a device is considered invalid	Number	Yes

Details of fields in profilingTechniques:

Field Name	Description	Data Type	Mandatory
`DHCPEnableStatus`	Enable DHCP for device profiling	Boolean	Yes
`TCPEnableStatus`	Enable TCP for device profiling	Boolean	Yes
`HTTPEnableStatus`	Enable HTTP for device profiling	Boolean	Yes

Details of fields in profileExpiration:

Field Name	Description	Data Type	Mandatory
`duration`	Profile expiration duration	Number	Yes
`unit`	Profile expiration duration unit, can be "MINUTES" / "HOURS"	String	Yes

Details of fields in bindIPAddressDetails:

Field Name	Description	Data Type	Mandatory
designatedPort	Monitoring port of a Sensor to receive a DHCP traffic with a relay agent	String	Yes
portIPAddress	IP address of the monitoring port	String	Yes
networkMask	Network mask	String	Yes
defaultGateway	Default gateway	String	Yes
vlanID	VLAN id	String	Yes

Details of object in interfaceStatusList:

Field Name	Description	Data Type	Mandatory
interfaceId	Interface id	Number	Yes
interfaceName	Interface name	String	Yes
enableInbound	Enable status in inbound direction	Boolean	Yes
enableOutbound	Enable status in outbound direction	Boolean	Yes
subinterfaceStatusList	List of sub-interfaces in a particular interface with enable status of passive device profiling in inbound/ outbound direction	Object	Yes

Details of fields in subinterfaceStatusList:

Field Name	Description	Data Type	Mandatory
interfaceId	Interface id	Number	Yes
interfaceName	Interface name	String	Yes
enableInbound	Enable status in inbound direction	Boolean	Yes
enableOutbound	Enable status in outbound direction	Boolean	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Status returned by update	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/sensor/1001/passivedeviceprofiling

Payload

```
{ "inheritSettingsfromIPSSettingsNode": true, "passiveDeviceProfilingSetting": { "profilingTechniques":
{ "DHCPEnableStatus": false, "TCPEnableStatus": false, "HTTPEnableStatus": true }, "profileExpiration":
{ "duration": 10, "unit": "HOURS" }, "hostInactivityTimerInHrs": 11 }, "bindIPForCopiedDHCPTraffic": true,
"bindIPAddressDetails": { "designatedPort": "4A", "portIPAddress": "100.100.100.10", "networkMask":
"255.255.0.0", "defaultGateway": "100.100.100.1", "vlanID": "10" }, "PassiveDeviceProfilingStateForSensor":
"ENABLE_DEVICEPROFILING_FOR_ENTIRE_DEVICE", "interfaceStatusList": [ { "interfaceId": 117, "interfaceName":
"3B", "enableInbound": true, "enableOutbound": true }, { "interfaceId": 105, "interfaceName": "1A-1B",
"enableInbound": true, "enableOutbound": true, "subinterfaceStatusList": [ { "subInterfaceId": 118,
"subInterfaceName": "TestVLAN1", "enableInbound": true, "enableOutbound": true } ] }, { "interfaceId": 104,
"interfaceName": "2A-2B", "enableInbound": true, "enableOutbound": true }, { "interfaceId": 103,
"interfaceName": "3A", "enableInbound": true, "enableOutbound": true }, { "interfaceId": 102, "interfaceName":
"4A-4B", "enableInbound": true, "enableOutbound": true } ] }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	3301	Profile expiration value must be between 5 and 59 minutes
3	400	3302	Profile expiration value must be between 1 and 12 hours
4	400	3303	Profile expiration value cannot be greater than host inactivity timer
5	400	3304	Please enable at least one profiling technique
6	400	3305	Inter connecting port cannot be specified as monitoring port
7	400	3306	Invalid monitoring port
8	400	3307	Invalid port IP address
9	400	3308	Invalid network mask
10	400	3309	Invalid default gateway
11	400	3310	VLAN id should be between 0 and 65535

Add Alert Exception

This URL adds a new alert exception.

Resource URL

POST /alertexception

Request Parameters

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`attackId`	Unique hexadecimal attack id	String	yes
`sourceIp`	IPV4/IPV6 address/"ANY"	String	Yes
`destinationIp`	IPV4/IPV6 address/"ANY"	String	Yes
`expiration`	Expiration can be "ONE_DAY" / "TWO_DAYS" / "THREE_DAYS" / "ONE_WEEK" / "ONE_MONTH"/" ONE_YEAR"	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique id of the created alert exception	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/alertexception

```
{ "attackId" : "0x42C03A00", "sourceIp" : "2.2.2.2", "destinationIp" : "Any", "expiration" : "ONE_DAY" }
```

Response

```
{ "createdResourceId":120 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	404	1105	Invalid domain
3	400	1402	Invalid attack id
4	400	1406	Invalid IP format

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
5	400	4001	Source and destination can contain either IPV4/IPV6, but not both simultaneously
6	400	4003	Similar alert exception already exist
7	400	4004	Source and destination IP cannot be same
8	400	4005	Alert exception limit exceeded
9	400	4006	Attack id, source and destination IP, all the three can't be any

Get Alert Exception

This URL gets the alert exception details.

Resource URL

GET /alertexception /<alert_exception_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`alert_exception_id`	Alert exception id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`alertId`	Unique alert id	Number
`attackId`	Unique hexadecimal attack id	String
`sourceIp`	IPV4/IPV6 address/"ANY"	String
`destinationIp`	IPV4/IPV6 address/"ANY"	String
`expiration`	Expiration of the exception	String
`lastModified`	Last modified time of the alert exception	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/alerexception/106

Response

```
{ "alertId" : 106, "attackId" : "0x40500100", "sourceIp" : "192.168.215.57", "destinationIp" : "172.16.233.11",
"expiration" : "2013-03-06 14:03:44.0", "lastModified" : "2013-03-05 14:03:44.0" }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	4002	Invalid alert exception id

Get All Alert Exception

This URL gets all the alert exception details available in the Manager.

Resource URL

GET /alertexception /list

Request Parameters

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`alertExceptionDescriptorList`	List of alert exception in the Manager	Array

Details of alertExceptionDescriptorList:

Field Name	Description	Data Type
`alertId`	Unique alert id	Number
`attackId`	Unique hexadecimal attack id	String
`sourceIp`	IPV4/IPV6 address/"ANY"	String
`destinationIp`	IPV4/IPV6 address/"ANY"	String
`expiration`	Expiration of the exception	String
`lastModified`	Last modified time of the alert exception	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/alerexception/list

Response

```
{ "alertExceptionDescriptor" : [{ "alertId" : 102, "attackId" : "0x42c01800", "sourceIp" : "116.232.112.112",
"destinationIp" : "95.124.86.145", "expiration" : "2013-02-27 13:51:49.0", "lastModified" : "2013-02-26
13:51:49.0" }, { "alertId" : 103, "attackId" : "0x42c03a00", "sourceIp" : "4.41.149.92", "destinationIp" :
"1.134.102.228", "expiration" : "2013-02-27 14:06:18.0", "lastModified" : "2013-02-26 14:43:08.0" },
{ "alertId" : 104, "attackId" : "0x42c03a00", "sourceIp" : "4.41.149.92", "destinationIp" : "1.134.102.228",
"expiration" : "2013-02-27 14:51:56.0", "lastModified" : "2013-02-26 20:43:06.0" }, { "alertId" : 105,
"attackId" : "0x40300200", "sourceIp" : "121.251.148.6", "destinationIp" : "64.54.175.34", "expiration" :
"2013-02-27 20:47:52.0", "lastModified" : "2013-02-27 14:16:49.0" }, { "alertId" : 106, "attackId" :
"0x40500100", "sourceIp" : "192.168.215.57", "destinationIp" : "172.16.233.11", "expiration" : "2013-03-06
14:03:44.0", "lastModified" : "2013-03-05 14:03:44.0" } ] }
```

Error Information

Delete Alert Exception

This URL deletes the specified alert exception.

Resource URL

GET /alertexception /<alert_exception_id>

Request Parameters

Field Name	Description	Data Type	Mandatory
`alert_exception_id`	Alert exception id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status returned by deletion	Number

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/alerexception/106

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	4002	Invalid alert exception id

Configure Global Auto Ack Setting

This URL is used to configure global auto ack setting.

Resource URL

PUT /globalautoack

Request Parameters

URL Parameters:

N/A

Payload Parameters:

Field Name	Description	Data Type
`GlobalAutoAckElem`	Object that contains the details of the field to be sent	Object

Details of fields in GlobalAutoAckElem:

Field Name	Description	Data Type	Mandatory
`enableAutoAlertAck`	Enable automatic alert acknowledgment	Boolean	Yes
`applicableTo`	Applicable alert types NON_RFSB_ALERTS_ONLY/ ALL_ALERTS	String	Yes
`severity`	Can be INFORMATIONAL_0/ LOW_1/ LOW_2/ LOW_3/ MEDIUM_4/ MEDIUM_5/ MEDIUM_6/ HIGH_7/ HIGH_8/ HIGH_9	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/globalautoack

Payload

```
{ "enableAutoAlertAck": true, “applicableTo": “ALL_ALERTS”, "severity": "LOW_3" }
```

Response

```
{ "status": 1 }
```

Error Information

N/A

Get Global Auto Ack Setting

This URL is used to retrieved global auto ack setting.

Resource URL

GET /globalautoack

Request Parameters

URL Parameters:

N/A

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`GlobalAutoAckElem`	Object that contains the details of the field to be sent	Object

Details of fields in GlobalAutoAckElem:

Field Name	Description	Data Type
`enableAutoAlertAck`	Enable automatic alert acknowledgment	boolean
`applicableTo`	applicable alert types NON_RFSB_ALERTS_ONLY/ALL_ALERTS	string
`severity`	Can be INFORMATIONAL_0/ LOW_1/ LOW_2/ LOW_3/ MEDIUM_4/ MEDIUM_5/ MEDIUM_6/ HIGH_7/ HIGH_8/ HIGH_9	string

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/globalautoack

Response

```
{ "enableAutoAlertAck": true, "applicableTo": "ALL_ALERTS", "severity": "LOW_3" }
```

Error Information

N/A

Get Attacks for Rules Configuration

This URL is used to retrieve attack lists.

Resource URL

GET /globalautoack/attack/<search_string>

Request Parameters

URL Parameters:

N/A

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
attackId	Attack id	String
attackName	Attack name	String

Example

Request

GET https://<NSM_IP>/sdkapi/globalautoack/attacks/malware

Response

```
{ [ “attackId”:”0x23323223” “attackName”:“malwareBlocklist” ] }
```

Error Information

N/A

Get Global Auto Ack Rules

This URL is used to retrieve auto ack rules.

Resource URL

POST /globalautoack/rules

Request Parameters

N/A

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type	Mandatory
attackId	Attack id	String	Yes
attackName	Attack name	String	Yes
ruleId	Rule id	Number	Yes
targetEndpoint	Target endpoint	String	Yes
attackerEndpoint	Attacker endpoint	String	Yes
expiration	Expiration	String	Yes
comment	Comment	String	Yes

Example

Request

POST https://<NSM_IP>/sdkapi/globalautoack/rules

Response

```
{ "autoAckRules": [ { "attackId":"0x45d29400", "ruleId":"154", "attackName":"Aasync: Aasync LIST Command
Response Filename Handling Overflow", "targetEndpoint":"1.12.4.4", "attackerEndpoint":"1.1.1.1",
"expiration":"2016-01-08 00:00:00.0", "lastModifiedBy":"admin", "lastModifiedDate":"2016-01-07 14:20:03.0",
"comment":"adssfsd" } ] }
```

Error Information

N/A

Get Global Auto Ack Rule

This URL is used to retrieve a single auto ack rule.

Resource URL

POST /globalautoack/rules/<rule_id>

Request Parameters

Field Name	Description	Data Type	Mandatory
`Rule_id`	Rule id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type	Mandatory
`attackId`	Attack id	String	Yes
`attackName`	Attack name	String	Yes
`ruleId`	Rule id	Number	Yes
`targetEndpoint`	Target endpoint	String	Yes
`attackerEndpoint`	Attacker endpoint	String	Yes
`expiration`	Expiration	String	Yes
`comment`	Comment	String	Yes

Example

Request

POST https://<NSM_IP>/sdkapi/globalautoack/rules/154

Response

```
{ "autoAckRules": [ { "attackId":"0x45d29400", "ruleId":"154", "attackName":"Aasync: Aasync LIST Command
Response Filename Handling Overflow", "targetEndpoint":"1.12.4.4", "attackerEndpoint":"1.1.1.1",
"expiration":"2016-01-08 00:00:00.0", "lastModifiedBy":"admin", "lastModifiedDate":"2016-01-07 14:20:03.0",
"comment":"adssfsd" } ] }
```

Error Information

N/A

Create Global Auto Ack Rules

This URLis used to create auto ack rules.

Resource URL

POST /globalautoack/rules

Request Parameters

URL Parameters:

N/A

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`attackId`	Attack id	String	Yes
`targetEndpoint`	Target endpoint	String	Yes
`attackerEndpoint`	Attacker endpoint	String	Yes
`expiration`	Expiration	String	Yes
`comment`	Comment	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

POST https://<NSM_IP>/sdkapi/globalautoack/rules

Payload

```
{ "attackId":"0x45d29400", "targetEndpoint":"1.12.4.4", "attackerEndpoint":"1.1.1.1", "expiration":"2016-01-08
00:00:00.0", "comment":"adssfsd" }
```

Response

```
{ "status": 1 }
```

Error Information

N/A

Update Global Auto Ack Rules

This URL is used to create auto ack rules.

Resource URL

POST /globalautoack/rules/<rule_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`Rule_id`	Rule id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`attackId`	Attack id	String	Yes
`targetEndpoint`	Target endpoint	String	Yes
`attackerEndpoint`	Attacker endpoint	String	Yes
`expiration`	Expiration	String	Yes
`comment`	Comment	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/globalautoack/rules/154

Payload

```
{ "attackId":"0x45d29400", "targetEndpoint":"1.12.4.4", "attackerEndpoint":"1.1.1.1", "expiration":"2016-01-08
00:00:00.0", "comment":"adssfsd" }
```

Response

```
{ "status": 1 }
```

Error Information

N/A

Update Name Resolution Settings at Domain Level

This URL updates name resolution setting at domain level.

Resource URL

PUT /domain/<domain_id>/nameresolution

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type
`DNSDetailsElement`	Object that contains the details of the field to be sent	Object

Details of fields in DNSDetailsElement:

Field Name	Description	Data Type	Mandatory
`inheritFromIPSSetting`	Inherit setting from parent domain	Boolean	Yes
`enableNameResolution`	Enable name resolution setting	Boolean	Yes
`dnsSuffixList`	List of DNS suffix	Array	No
`primaryDNSServer`	Primary DNS server IP, mandatory when name resolution is enabled	String	No
`secondaryDNSServer`	Secondary DNS server IP	String	No
`refreshIntervalInHours`	Refresh interval in hours, applicable only for NTBA device	Number	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/domain/0/nameresolution

Payload

```
{ "inheritFromIPSSetting": false, "enableNameResolution": true, "dnsSuffixList": [ "mcafee.com", "google.com" ],
"primaryDNSServer": "172.16.230.211", "secondaryDNSServer": "172.16.232.72", "refreshIntervalInHours": 120 }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	3101	Cannot inherit setting for root domain
3	400	4701	Duplicate suffix found:
4	400	4702	Primary DNS Server is required
5	400	4703	Invalid domain name
6	400	4704	Invalid primary DNS server
7	400	4705	Invalid secondary DNS server
8	400	4706	Refresh interval must be between 24 and 9999 hours

Get Name Resolution Configuration at Domain level

This URL gets name resolution configuration at domain level.

Resource URL

GET /domain/<domain_id>/nameresolution

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`DNSDetailsElement`	Object that contains the details of the fields	Object

Details of fields in DNSDetailsElement:

Field Name	Description	Data Type
`inheritFromIPSSetting`	Inherit setting from parent domain	Boolean
`enableNameResolution`	Enable name resolution setting	Boolean
`dnsSuffixList`	List of DNS suffix	Array
`primaryDNSServer`	Primary DNS server IP, mandatory when name resolution is enabled	String
`secondaryDNSServer`	Secondary DNS server IP	String
`refreshIntervalInHours`	Refresh interval in hours, applicable only for NTBA device	Number

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/domain/0/nameresolution

Response

```
{ "inheritFromIPSSetting": false, "enableNameResolution": true, "dnsSuffixList": [ "mcafee.com", "google.com" ],
"primaryDNSServer": "172.16.230.211", "secondaryDNSServer": "172.16.232.72", "refreshIntervalInHours": 120 }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Update Name Resolution Settings at Sensor Level

This URL updates name resolution setting at Sensor level.

Resource URL

PUT /sensor/<sensor_id>/nameresolution

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type
`DNSDetailsElement`	Object that contains the details of the field to be sent	Object

Details of fields in DNSDetailsElement:

Field Name	Description	Data Type	Mandatory
`inheritFromIPSSetting`	Inherit setting from parent domain	Boolean	Yes
`enableNameResolution`	Enable name resolution setting	Boolean	Yes
`dnsSuffixList`	List of DNS suffix	Array	No
`primaryDNSServer`	Primary DNS server IP, mandatory when name resolution is enabled	String	No
`secondaryDNSServer`	Secondary DNS server IP	String	No
`refreshIntervalInHours`	Refresh interval in hours, applicable only for NTBA device	Number	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/sensor/1001/nameresolution

Payload

```
{ "inheritFromIPSSetting": false, "enableNameResolution": true, "dnsSuffixList": [ "mcafee.com", "google.com" ],
"primaryDNSServer": "172.16.230.211", "secondaryDNSServer": "172.16.232.72", "refreshIntervalInHours": 120 }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	3101	Cannot inherit setting for root domain

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
3	400	4701	Duplicate suffix found:
4	400	4702	Primary DNS server is required
5	400	4703	Invalid domain name
6	400	4704	Invalid primary DNS server
7	400	4705	Invalid secondary DNS server
8	400	4706	Refresh interval must be between 24 and 9999 hours

Get Name Resolution Configuration at Sensor Level

This URL gets name resolution configuration at Sensor level.

Resource URL

GET /sensor/<sensor_id>/nameresolution

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`DNSDetailsElement`	Object that contains the details of the fields	Object

Details of fields in DNSDetailsElement:

Field Name	Description	Data Type
`inheritFromIPSSetting`	Inherit setting from parent domain	Boolean
`enableNameResolution`	Enable name resolution setting	Boolean
`dnsSuffixList`	List of DNS suffix	Array
`primaryDNSServer`	Primary DNS server IP, mandatory when name resolution is enabled	String
`secondaryDNSServer`	Secondary DNS server IP	String
`refreshIntervalInHours`	Refresh interval in hours, applicable only for NTBA device	Number

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/sensor/1001/nameresolution

Response

```
{ "inheritFromIPSSetting": false, "enableNameResolution": true, "dnsSuffixList": [ "mcafee.com", "google.com" ],
"primaryDNSServer": "172.16.230.211", "secondaryDNSServer": "172.16.232.72", "refreshIntervalInHours": 0 }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor

Add Device

This URL adds a new device in the specified domain.

Resource URL

POST /domain/<domain_id>/device

Request Parameters

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`deviceId`	Unique device id, not required for POST	String	Yes
`deviceName`	Device name	String	Yes
`deviceType`	Device type can be IPSNACSensor/ virtualHIPSensor/ NTBAAppliance/ loadBalancer	Object	Yes
`contactInformation`	Contact information for the device	String	No
`location`	Device location	String	No
`lastModifiedTime`	Last modified time of the device	String	No

Details of IPSNACSensor:

Field Name	Description	Data Type	Mandatory
`sharedSecret`	Device shared secret key	String	Yes
`confirmSharedSecret`	Device confirmed shared secret key	String	Yes
`updatingMode`	Update mode can be ONLINE/ OFFLINE/ UNKNOWN	String	Yes

Details of virtualHIPSensor:

Field Name	Description	Data Type	Mandatory
`sharedSecret`	Device shared secret key	String	Yes
`confirmSharedSecret`	Device confirmed shared secret key	String	Yes

Details of NTBAAppliance:

Field Name	Description	Data Type	Mandatory
`sharedSecret`	Device shared secret key	String	Yes
`confirmSharedSecret`	Device confirmed shared secret key	String	Yes

Details of loadBalancer:

Field Name	Description	Data Type	Mandatory
`ipAddress`	IP address	String	Yes
`SNMPv3User`	SNMP user name. Required for XC-240	String	No
`authenticationPassword`	Authentication password. required for XC-240	String	No
`privacyPassword`	Privacy password. Required for XC-240	String	No
`model`	Load balancer model. Values can be XC-240 or XC-640	String	Yes
`user`	Device username. Required for XC-640	String	No
`password`	Device password. Required for XC-640	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique id of the created device	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/domain/0/device

```
{ "deviceName": "Load_BALANCER", "deviceType": { "virtualHIPSensor": null, "loadBalancer": { "ipAddress":
"1.1.1.1", "SNMPv3User": "SNMP", "authenticationPassword": "admin123", "privacyPassword": "admin123" "model":
"XC-240" } }, "contactInformation": "Contact_Infor", "location": "Location", "LastModifiedTime": "Mon Jul 22
20:05:00 IST 2013" }
```

Response

```
{ "createdResourceId":1006 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	4601	Device name is required

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
3	400	4602	Device name should not be greater than 25 chars
4	400	4603	Shared secret is required
5	400	4604	Confirm shared secret is required
6	400	4605	Shared secret does not match
7	400	4609	SNMPv3 username is required
8	400	4610	Authentication password is required
9	400	4611	Privacy password is required
10	400	4612	Password should not be less than 8 chars
11	400	4613	Name must contain only letters, numerical, dot, hyphens or underscore
12	400	4614	Device name already exists
13	400	4615	IP address already exists
14	400	4616	Device profile provided is not up to date
15	400	4617	Location should not be greater than 25 chars
16	400	4618	Location must contain only letters, numerical, dot, hyphens or underscore
17	400	4619	Contact should not be greater than 25 chars
18	400	4620	Location must contain only letters, numerical, dot, hyphens or underscore
19	400	4621	Shared secret should not be greater than 25 chars

Get Device

This URL gets the device details.

Resource URL

GET /domain/<domain_id>/device/<device_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`device_id`	Device id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`deviceId`	Unique device id, not required for POST	String
`deviceName`	Device name	String
`deviceType`	Device type can be IPSNACSensor/ virtualHIPSensor/ NTBAAppliance/ loadBalancer	Object
`contactInformation`	Contact information for the device	String
`location`	Device location	String
`lastModifiedTime`	Last modified time of the device	String

Details of IPSNACSensor:

Field Name	Description	Data Type
`sharedSecret`	Device shared secret key	String
`confirmSharedSecret`	Device confirmed shared secret key	String
`updatingMode`	Update mode can be ONLINE/ OFFLINE/ UNKNOWN	String

Details of virtualHIPSensor:

Field Name	Description	Data Type
`sharedSecret`	Device shared secret key	String
`confirmSharedSecret`	Device confirmed shared secret key	String

Details of NTBAAppliance:

Field Name	Description	Data Type
`sharedSecret`	Device shared secret key	String
`confirmSharedSecret`	Device confirmed shared secret key	String

Details of loadBalancer:

Field Name	Description	Data Type
`ipAddress`	IP address	String
`SNMPv3User`	SNMP user name	String
`authenticationPassword`	Authentication password	String
`privacyPassword`	Privacy password	String
`model`	LB model	String
`user`	Device user name	String
`password`	Device user password	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/device/1005

Response

```
{ "deviceId": 1005, "deviceName": "NTBA_APPLIANCEs", "deviceType": { "virtualHIPSensor": null, "NTBAAppliance":
{ "sharedSecret": "admin123", "confirmSharedSecret": "admin123" }, "loadBalancer": null }, "contactInformation":
"Contact_Infor", "location": "Locaiton", "LastModifiedTime": "2013-07-22 20:04:17.0" }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	404	4608	Invalid device id /device not visible in this domain

Update Device

This URL adds a new device in the specified domain.

Resource URL

PUT /domain/<domain_id>/device/<device_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`device_id`	Device Id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`deviceId`	Unique device id, not required for POST	String	Yes
`deviceName`	Device name	String	Yes
`deviceType`	Device type can be IPSNACSensor/ virtualHIPSensor/ NTBAAppliance/ loadBalancer	Object	Yes
`contactInformation`	Contact information for the device	String	No
`location`	Device location	String	No
`lastModifiedTime`	Last modified time of the device	String	No

Details of IPSNACSensor:

Field Name	Description	Data Type	Mandatory
`sharedSecret`	Device shared secret key	String	Yes
`confirmSharedSecret`	Device confirmed shared secret key	String	Yes
`updatingMode`	Update mode can be ONLINE/ OFFLINE/ UNKNOWN	String	Yes

Details of virtualHIPSensor:

Field Name	Description	Data Type	Mandatory
`sharedSecret`	Device shared secret key	String	Yes
`confirmSharedSecret`	Device confirmed shared secret key	String	Yes

Details of NTBAAppliance:

Field Name	Description	Data Type	Mandatory
`sharedSecret`	Device shared secret key	String	Yes
`confirmSharedSecret`	Device confirmed shared secret key	String	Yes

Details of loadBalancer:

Field Name	Description	Data Type	Mandatory
`ipAddress`	IP address	String	Yes

Field Name	Description	Data Type	Mandatory
`SNMPv3User`	SNMP user name	String	Yes
`authenticationPassword`	Authentication password	String	Yes
`privacyPassword`	Privacy password	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique id of the created device	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/domain/0/device/1006

```
{ "deviceId": 1006, "deviceName": "Load_BALANCER", "deviceType": { "virtualHIPSensor": null, "loadBalancer":
{ "ipAddress": "1.1.1.1", "SNMPv3User": "SNMP", "authenticationPassword": "admin123", "privacyPassword":
"admin123" } }, "contactInformation": "ContactInform", "location": "Location", "LastModifiedTime": "Mon Jul 22
20:05:00 IST 2013" }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	4601	Device name is required
3	400	4602	Device name should not be greater than 25 chars
4	400	4603	Shared secret is required
5	400	4604	Confirm shared secret is required
6	400	4605	Shared secret does not match
7	400	4606	Device name cannot be modified
8	400	4607	Update mode is required
9	404	4608	Invalid device id /device not visible in this domain
10	400	4609	SNMPv3 username is required
11	400	4610	Authentication password is required
12	400	4611	Privacy password is required

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
13	400	4612	Password should not be less than 8 chars
14	400	4613	Name must contain only letters, numerical, dot, hyphens or underscore
15	400	4614	Device name already exists
16	400	4615	IP address already exists
17	400	4616	Device profile provided is not up to date
18	400	4617	Location should not be greater than 25 chars
19	400	4618	Location must contain only letters, numerical, dot, hyphens or underscore
20	400	4619	Contact should not be greater than 25 chars
21	400	4620	Location must contain only letters, numerical, dot, hyphens or underscore
22	400	4621	Shared secret should not be greater than 25 chars

Delete Device

This URL deletes the specified device.

Resource URL

GET /domain/<domain_id>/device/<device_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
device_id	Device id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
Status	Status returned by deletion	Number

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/domain/0/device/120

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	4002	Invalid alert exception id

Get All Device

This URL gets all the alert exception details available in the Manager.

Resource URL

GET /domain/<domainId>/device

Request Parameters

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`DeviceResponseList`	List of edvices in the domain	Array

Details of alertExceptionDescriptorList:

Field Name	Description	Data Type
`deviceId`	Unique device id	Number
`deviceName`	Device name	String
`deviceType`	Device type can be LOAD_BALANCER / NTBA_APPLIANCE / VIRTUAL_HIP_SENSOR / IPS_SENSOR	String
`updatingMode`	Update mode can ONLINE/ OFFLINE/ UNKNOWN	String
`contactInformation`	Contact information	String
`location`	Device location	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/domain/0/device

Response

```
{ "DeviceResponseList": [ { "deviceId": 1010, "deviceName": "LB", "deviceType": "LOAD_BALANCER", "updatingMode":
"UNKNOWN" }, { "deviceId": 1002, "deviceName": "M-2850", "deviceType": "IPS_SENSOR", "updatingMode": "ONLINE",
"contactInformation": "", "location": "" }, { "deviceId": 1001, "deviceName": "M-2950", "deviceType":
"IPS_SENSOR", "updatingMode": "ONLINE" }, { "deviceId": 1003, "deviceName": "M-3050", "deviceType":
"IPS_SENSOR", "updatingMode": "ONLINE" }, { "deviceId": 1009, "deviceName": "M-8000-P", "deviceType":
"IPS_SENSOR", "updatingMode": "ONLINE" }, { "deviceId": 1008, "deviceName": "M8000-34", "deviceType":
"IPS_SENSOR", "updatingMode": "ONLINE" }, { "deviceId": 1004, "deviceName": "NTBA-Regression", "deviceType":
"NTBA_APPLIANCE", "updatingMode": "UNKNOWN" } ] }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Get NTBA Monitors

This URL gets the available NTBA monitors.

Resource URL

GET /ntbamonitors

Request Parameters

N/A

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`ntbaMonitors`	List of NTBA's	Array

Details of NTBA:

Field Name	Description	Data Type
`nbaId`	Id	String
`name`	Name	String
`serialNumber`	Serial number	String
`softwareVersion`	Software version	String
`ipAddress`	IP address	String
`LastSignatureUpdateTime`	Threat description	String
`lastRebootTime`	Reboot time	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors

Response

```
{ "ntbaMonitors":[{ "nbaId":1003,"name":"T-100VM",
"serialNumber":"T0020121211165440","softwareVersion":"8.0.4.5",
"ipAddress":"172.16.232.162","LastSignatureUpdateTime":"2013-08-14 19:14:37.0", "lastRebootTime":"2013-08-14
19:14:37.0"}] }
```

Error Information

Get Hosts Threat Factor

This URL gets the list of hosts threat factor.

Resource URL

GET /ntbamonitors/{ntbaId}/hoststhreatfactor? TopN=<TopN>
&timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`TopN`	Number of top rows, default 50.	Number	No
`timePeriod`	Duration: can be • LAST_MINUTE • LAST_10_MINUTES • LAST_HOUR • LAST_24_HOURS • CUSTOM Custom incase start and end time is provided	String	No
`startTime`	Start time in the format: yyyy-MM-dd HH:mm	String	No
`endTime`	End time in the format: yyyy-MM-dd HH:mm	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`hostsThreatFactor`	List of hosts threat factors in the NTBA	Array

Details of NTBA:

Field Name	Description	Data Type
`hostIP`	Host IP	String
`hostId`	Host id	Number
`userName`	User name	String
`zone`	Zone details	String
`threatFactor`	Threat factor	String
`threats`	Threat description	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/hoststhreatfactor?timePeriod=CUSTOM&startTime=2012-APR-20%2012:15&endTime=2012-APR-20%2012:11

Response

```
{ "hostsThreatFactor" : [{ "hostIP" : "10.100.16.125", "zone" : "Default Inside Zone", "threatFactor" : "10.0",
"threats" : "Illegal Reputation, BOT: Potential Bot Detected - High Confidence Heuristics Correlation, HTTP:
Executable File in PDF File Detected, BOT: Potential Bot Detected - Medium Confidence Heuristics Correlation
" }, { "hostIP" : "18.16.24.22", "zone" : "Default Inside Zone", "threatFactor" : "10.0", "threats" : "Illegal
Reputation " }, { "hostIP" : "80.198.199.175", "zone" : "Default Inside Zone", "threatFactor" : "10.0",
"threats" : "Illegal Reputation " } ] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id

Get Top URLs

This URL gets the list of top urls.

Resource URL

GET /ntbamonitors/{ntbaId}/topurls? TopN=<TopN> &timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`TopN`	Number of top rows, default 50.	Number	No
`timePeriod`	Duration: can be • LAST_MINUTE • LAST_10_MINUTES • LAST_HOUR • LAST_24_HOURS • CUSTOM Custom incase start and end time is provided	String	No
`startTime`	Start time in the format: yyyy-MM-dd HH:mm	String	No
`endTime`	End time in the format: yyyy-MM-dd HH:mm	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`topURLsOnNetwork`	List of urls	Array

Details of topURLsOnNetwork:

Field Name	Description	Data Type
`reputation`	Reputation	String
`url`	URL	Number
`urlId`	URL id	String
`category`	Category	String
`categoryId`	Category id	Number
`country`	Country	String
`count`	Count	Number

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/%20topurls?timePeriod=CUSTOM&startTime=2012-APR-20%2012:15&endTime=2012-APR-20%2012:11

Response

{"topURLsOnNetwork": [{ "reputation":"Minimal Risk", "url":"twitter.com", "urlId":"8390917", "category":"Blogs/Wiki", "categoryId":898, "country":"United States", "count":6 }] }

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id

Get Top Zone URLs

This URL gets the list of top zone urls.

Resource URL

GET /ntbamonitors/{ntbaId}/topzoneurls/<zoneid>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`zoneid`	Zone id.	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`topURLsOnNetwork`	List of urls	Array

Details of topURLsOnNetwork:

Field Name	Description	Data Type
`reputation`	Reputation	String
`url`	url	Number
`urlId`	URL id	String
`category`	Category	String
`categoryId`	Category id	Number
`country`	Country	String
`count`	Count	Number

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/%20topzoneurls/9898

Response

```
{"topURLsOnNetwork": [ { "reputation":"Minimal Risk", "url":"twitter.com", "urlId":"8390917", "category":"Blogs/
Wiki", "categoryId":898, "country":"United States", "count":6 } ] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
7	400	4312	Invalid zone id or no data

Get Top Host URLs

This URL gets the list of top host urls.

Resource URL

GET /ntbamonitors/{ntbaId}/tophosturls/<hostId >

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`hostid`	Host id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`topURLsOnNetwork`	List of urls	Array

Details of topURLsOnNetwork:

Field Name	Description	Data Type
`reputation`	Reputation	String
`url`	URL	Number
`urlId`	URL id	String
`category`	Category	String
`categoryId`	Category id	Number
`country`	Country	String
`count`	Count	Number

Example

Request

GEThttps://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/%20tophosturls/9

Response

```
{"topURLsOnNetwork": [ { "reputation":"Minimal Risk", "url":"twitter.com", "urlId":"8390917", "category":"Blogs/
Wiki", "categoryId":898, "country":"United States", "count":6 } ] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id
7	400	4310	Invalid host id or no data

Get Top URLs by Reputations

This URL gets the list of top urls by reputations.

Resource URL

GET /ntbamonitors/{ntbaId}/topurlsbyreputation? TopN=<TopN>
&timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`TopN`	Number of top rows, default 50	Number	No
`timePeriod`	Duration: can be • LAST_MINUTE • LAST_10_MINUTES • LAST_HOUR • LAST_24_HOURS • CUSTOM Custom incase start and end time is provided	String	No
`startTime`	Start time in the format: yyyy-MM-dd HH:mm	String	No
`endTime`	End time in the format: yyyy-MM-dd HH:mm	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`topURLsOnNetwork`	List of urls	Array

Details of topURLsOnNetwork:

Field Name	Description	Data Type
`reputation`	Reputation	String
`url`	URL	Number
`urlId`	URL id	String
`country`	Country	String
`count`	Count	Number

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/topurlsbyreputation?timePeriod=CUSTOM&startTime=2012-APR-20

Response

```
{ "topURLsOnNetwork": [{ "reputation":"Minimal Risk", "url":"twitter.com","urlId":"8390917", "category":"Blogs/
Wiki","country":"United States","count":6 }] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id

Get URL Activity

This URL gets the list of activities for given url id.

Resource URL

GET /ntbamonitors/{ntbaId}/showurlactivity/{urlid}? TopN=<TopN>
&timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`TopN`	Number of top rows, default 50	Number	No
`timePeriod`	Duration: can be • LAST_MINUTE • LAST_10_MINUTES • LAST_HOUR • LAST_24_HOURS • CUSTOM Custom incase start and end time is provided	String	No
`startTime`	Start time in the format: yyyy-MM-dd HH:mm	String	No
`endTime`	End time in the format: yyyy-MM-dd HH:mm	String	No
`urlId`	URL id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`urlActivities`	List of urls	Array

Details of urlActivities:

Field Name	Description	Data Type
`srcEndpoint`	Endpoint	String
`srcReputation`	Reputation	Number
`srcZone`	Source zone	String
`srcCountry`	Source country	String
`destEndpoint`	Dest endpoint	String
`destReputation`	Dest reputation	String
`destZone`	Dest zone	String
`destCountry`	Dest country	String
`action`	Action	String
`lastAccessed`	Last accessed	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/showurlactivity%20/8390917?timePeriod=CUSTOM&startTime=2012-APR-20

Response

```
{"urlActivities": [{ "srcEndpoint":"16843018", "srcReputation":"Not Queried", "srcZone":"Default Inside Zone",
"srcCountry":"---", "destEndpoint":"16843017", "destReputation":"Minimal Risk", "destZone":"Default Outside
Zone", "destCountry":"Malaysia", "action":"URL Accessed", "lastAccessed":"2013-08-20 06:15:18"} ] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id
7	400	4307	Invalid url id or no activities

Get URLS by Category

This URL gets the list of urls by category.

Resource URL

GET /ntbamonitors/{ntbaId}/ topurlsbycategory? TopN=<TopN>
&timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`TopN`	Number of top rows, default 50	Number	No
`timePeriod`	Duration: can be • LAST_MINUTE • LAST_10_MINUTES • LAST_HOUR • LAST_24_HOURS • CUSTOM Custom incase start and end time is provided	String	No

Field Name	Description	Data Type	Mandatory
`startTime`	Start time in the format: yyyy-MM-dd HH:mm	String	No
`endTime`	End time in the format: yyyy-MM-dd HH:mm	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`topURLsOnNetwork`	List of urls	Array

Details of topURLsOnNetwork:

Field Name	Description	Data Type
`category`	Category	String
`categoryId`	Category id	Number
`count`	Count	Number

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/topurlsbycategory?timePeriod=CUSTOM&startTime=2012-APR-20

Response

```
{ "topURLsOnNetwork": [{ "category":"Blogs/Wiki","categoryId":"188","count":15 }] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id

Get URLs for Category

This URL gets the list of urls for category.

Resource URL

GET /ntbamonitors/{ntbaId}/ topurlsbycategory/<category_id>? TopN=<TopN>
&timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`TopN`	Number of top rows, default 50.	Number	No
`timePeriod`	Duration: can be • LAST_MINUTE • LAST_10_MINUTES • LAST_HOUR • LAST_24_HOURS • CUSTOM Custom incase start and end time is provided	String	No
`startTime`	Start time in the format: yyyy-MM-dd HH:mm	String	No
`endTime`	End time in the format: yyyy-MM-dd HH:mm	String	No
`Category_id`	Category id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`topURLsOnNetwork`	List of URLs	Array

Details of topURLsOnNetwork:

Field Name	Description	Data Type
`reputation`	Reputation	String
`url`	URL	Number
`urlId`	URL id	String
`country`	Country	String
`count`	Count	Number

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/topurlsbycategory/188?timePeriod=CUSTOM&startTime=2012-APR-20

Response

```
{ "topURLsOnNetwork":[{ "reputation":"Minimal Risk","url":"twitter.com","urlId":"8390917","category":"Blogs/
Wiki","country":"United States","count":6},{"reputation":"Minimal
Risk","url":"wikipedia.org","urlId":"10536655","category":"Education/Reference","country":"United
States","count":7}] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id
7	400	4308	Invalid category id

Get Top Files

This URL gets the list of top files.

Resource URL

GET /ntbamonitors/{ntbaId}/topfiles? TopN=<TopN> &timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`TopN`	Number of top rows, default 50	Number	No
`timePeriod`	Duration: can be • LAST_MINUTE • LAST_10_MINUTES • LAST_HOUR • LAST_24_HOURS • CUSTOM Custom incase start and end time is provided	String	No
`startTime`	Start time in the format: yyyy-MM-dd HH:mm	String	No
`endTime`	End time in the format: yyyy-MM-dd HH:mm	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`topFilesOnNetwork`	List of files	Array

Details of topFilesOnNetwork:

Field Name	Description	Data Type
`File`	File	String
`fileId`	File id	Number
`Count`	Count	Number

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/topfiles?timePeriod=CUSTOM&startTime=2012-APR-20

Response

```
{ "topFilesOnNetwork":[{ "file":"test.txt", "fileId":8389181, "count":2}] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id

Get Top Zone Files

This URL gets the list of top files.

Resource URL

GET /ntbamonitors/{ntbaId}/topzonefiles/<zone_id

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes

Field Name	Description	Data Type	Mandatory
`Zone_id`	Zone id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`topFilesOnNetwork`	List of files	Array

Details of topFilesOnNetwork:

Field Name	Description	Data Type
`File`	File	String
`fileId`	File id	Number
`Count`	Count	Number

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/topzonefiles/9

Response

```
{ "topFilesOnNetwork":[{ "file":"test.txt", "fileId":8389181, "count":2}] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id
7	400	4312	Invalid zone id

Get Top Host Files

This URL gets the list of top files for given host id.

Get File Activity

This URL gets the activities for the given file id.

Resource URL

GET /ntbamonitors/{ntbaId}/ fileactivity/{fileid}? TopN=<TopN>
&timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>

Request Parameters

Field Name	Description	Data Type	Mandatory
ntbaId	NTBA monitor id	Number	Yes
TopN	Number of top rows, default 50.	Number	No
timePeriod	Duration: can be • LAST_MINUTE • LAST_10_MINUTES • LAST_HOUR • LAST_24_HOURS • CUSTOM Custom incase start and end time is provided	String	No
startTime	Start time in the format: yyyy-MM-dd HH:mm	String	No
endTime	End time in the format: yyyy-MM-dd HH:mm	String	No
fileId	File Id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
fileActivities	List of activities	Array

Details of fileActivities:

Field Name	Description	Data Type
srcEndpoint	Source endpoint	String
srcUser	Source User	String
srcZone	Source zone	String
destEndpoint	Dest endpoint	String
destUser	Dest user	String
destZone	Dest zone	String

Field Name	Description	Data Type
action	Action	String
lastAccessed	Last accessed	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/fileactivity/8389181?timePeriod=CUSTOM&startTime=2012-APR-20%2012:15&endTime=2012-APR-20%2012:11

Response

```
{“fileActivities”:[{ “srcEndpoint”:”16843018”, “srcUser”:”—“, “srcZone”:”Default Inside Zone”,
“destEndpoint”:”16843017”, “destUser”:”—“, “destZone”:”Default Outside Zone”, “action”:”file upload”,
“lastAccessed”:”2013-08-20 06:15:18”} ] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id
7	400	4309	Invalid file id or no data.

Get External Hosts by Reputation

This URL gets the list of external hosts by reputation.

Resource URL

GET /ntbamonitors/{ntbaId}/topexthostsbyreputation? TopN=<TopN>
&timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>

Request Parameters

Field Name	Description	Data Type	Mandatory
ntbaId	NTBA monitor id	Number	Yes
TopN	Number of top rows, default 50.	Number	No
timePeriod	Duration: can be • LAST_MINUTE • LAST_10_MINUTES • LAST_HOUR	String	No

Field Name	Description	Data Type	Mandatory
	• LAST_24_HOURS • CUSTOM Custom incase start and end time is provided		
`startTime`	Start time in the format: yyyy-MM-dd HH:mm	String	No
`endTime`	End time in the format: yyyy-MM-dd HH:mm	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`topHostsOnNetwork`	List of hosts	Array

Details of topHostsOnNetwork:

Field Name	Description	Data Type
`reputation`	Reputation	String
`hostId`	Host id	Number
`hostIp`	Host ip	String
`zone`	Zone details	String
`country`	Country	String
`Time`	Time	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/%20topexthostsbyreputation?timePeriod=CUSTOM&startTime=2012-APR-20%2012:15&endTime=2012-APR-20%2012:11

Response

```
{ "topHostsOnNetwork":[{ "reputation":"Unverified","hostIp":"11.11.10.60", "hostId":4480240188,"zone":"Default
Outside Zone", "country":"United States","time":"2013-08-27 16:30:24"}] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id

Get New Hosts

This URL gets the list of new hosts.

Resource URL

GET /ntbamonitors/{ntbaId}/newhosts? TopN=<TopN>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`TopN`	Number of top rows, default 50.	Number	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`newHostsOnNetwork`	List of hosts	Array

Details of newHostsOnNetwork:

Field Name	Description	Data Type
`endpointIp`	Host IP	String
`hostId`	Host id	Number
`lastseen`	Last seen	String
`zone`	Zone details	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/newhosts

Response

```
{ "newHostsOnNetwork":[{" endpointIp":"10.10.10.60","hostId":62,"zone":"Default Inside
Zone","lastSeen":"2013-08-27 16:32:48"}] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id

Get Active Hosts

This URL gets the list of active hosts.

Resource URL

GET /ntbamonitors/{ntbaId}/activehosts? TopN=<TopN>
&timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`TopN`	Number of top rows, default 50.	Number	No
`timePeriod`	Duration: can be • LAST_MINUTE • LAST_10_MINUTES • LAST_HOUR • LAST_24_HOURS • CUSTOM Custom incase start and end time is provided	String	No
`startTime`	Start time in the format: yyyy-MM-dd HH:mm	String	No
`endTime`	End time in the format: yyyy-MM-dd HH:mm	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`activeHosts`	List of active hosts.	Array

Details of active hosts:

Field Name	Description	Data Type
endpointIp	Host IP	String
hostId	Host id	Number
lastseen	Last seen	String
zone	Zone details	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/activehosts?timePeriod=CUSTOM&startTime=2012-APR-20%2012:15&endTime=2012-APR-20%2012:11

Response

```
{ "activeHosts":[{ "hostId":11,"endpointIp":"1.1.1.10", "zone":"Default Inside Zone","lastSeen":"2013-08-27
16:26:14"}] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id

Get Top Hosts Traffic

This URL gets the list of hosts traffic.

Resource URL

GET /ntbamonitors/{ntbaId}/tophoststraffic? TopN=<TopN>
&startTime=<startTime>&endTime=<endTime>&direction=<direction>

Request Parameters

Field Name	Description	Data Type	Mandatory
ntbaId	NTBA monitor id	Number	Yes
TopN	Number of top rows, default 50.	Number	No

Field Name	Description	Data Type	Mandatory
`startTime`	Start time in the format: yyyy-MM-dd HH:mm	String	No
`endTime`	End time in the format: yyyy-MM-dd HH:mm	String	No
`direction`	Direction: Bidirectional Inbound Outbound	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`hostsTraffic`	Hosts traffic	Array

Details of hosts traffic:

Field Name	Description	Data Type
`endpointIp`	Host IP	String
`hostId`	Host id	Number
`zone`	Zone details	String
`traffic`	Traffic volume	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/tophoststraffic?startTime=2012-APR-20%2012:15&endTime=2012-APR-20%2012:11

Response

```
{"hostsTraffic":[{" endpointIp":"1.1.1.10", "hostId":11, "zone":"Default Inside Zone", "traffic":"22M"}] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id

Get Application Traffic

This URL gets the list of application traffic.

Resource URL

GET /ntbamonitors/{ntbaId}/applicationtraffic? TopN=<TopN>
&startTime=<startTime>&endTime=<endTime>&direction=<direction>&frequency=<frequency>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`TopN`	Number of top rows, default 50.	Number	No
`startTime`	Start time in the format: yyyy-MM-dd HH:mm	String	No
`endTime`	End time in the format: yyyy-MM-dd HH:mm	String	No
`direction`	Direction: Bidirectional Inbound Outbound	String	No
`frequency`	Frequency: 1min 10mins Hourly Daily	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`applicationsTraffic`	Application traffic	Array

Details of applicationsTraffic:

Field Name	Description	Data Type
`application`	Application name	String
`applicationId`	Application id	Number
`inbound`	Inbound traffic	String
`outbound`	Outbound traffic	String
`total`	Total	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/applicationtraffic?startTime=2012-APR-20%2012:15&endTime=2012-APR-20%2012:11

Response

```
{"applicationsTraffic":[ {"application":"FTP","applicationId":1191186432, "inbound":"7M", "outbound":"7M",
"total":"15M" }] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id

Get Application Profile

This URL gets the application profile for given application id.

Resource URL

GET /ntbamonitors/{ntbaId}/ applicationtraffic/profile/{appId}? startTime=<startTime>&endTime=<endTime>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`startTime`	Start time in the format: yyyy-MM-dd HH:mm	String	No
`endTime`	End time in the format: yyyy-MM-dd HH:mm	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`serversProfile`	Servers profile data	Array
`clientsProfile`	Clients profile data	Array

Details of serverProfile/clientsProfile:

Field Name	Description	Data Type
endpointIp	Host IP	String
hostName	Host name	String
zone	Zone name	String
inboundTraffic	Inbound traffic	String
outboundTraffic	outbound traffic	String
totalTraffic	Total traffic	String
noOfConnections	Number of connection	Number

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/applicationprofile/profile/131231?startTime=2012-APR-20%2012:15&endTime=2012-APR-20%2012:11

Response

```
{"serversProfile":[{ "endpointIp":"1.1.1.1", "hostName":"--", "zone":"Default Inside Zone", "vlanId":"---",
"inboundTraffic":"1M", "outboundTraffic":"1M", "totalTraffic":"2M", "noOfConnections":2, }] "clientsProfile":
[{ "endpointIp":"1.1.1.1", "hostName":"--", "zone":"Default Inside Zone", "vlanId":"---", "inboundTraffic":"1M",
"outboundTraffic":"1M", "totalTraffic":"2M", "noOfConnections":2, }] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id
7	400	4311	Invalid application id or no data

Get Throughput Traffic

This URL gets details of enterprise throughput.

Resource URL

GET /ntbamonitors/{ntbaId}/throughputtraffic? TopN=<TopN>
&startTime=<startTime>&endTime=<endTime&frequency=<frequency>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`TopN`	Number of top rows, default 50.	Number	No
`startTime`	Start time in the format: yyyy-MM-dd HH:mm	String	No
`endTime`	End time in the format: yyyy-MM-dd HH:mm	String	No
`frequency`	Frequency: 1min 10mins Hourly Daily	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`throughputTrafficList`	Traffic list	Array

Details of throughputTrafficList:

Field Name	Description	Data Type
`inbound`	Inbound traffic	String
`outbound`	Outbound traffic	String
`time`	Time	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/throughputtraffic?startTime=2012-APR-20%2012:15&endTime=2012-APR-20%2012:11

Response

```
{ "throughputTrafficList":[ {"inbound":"0M", "outbound":"0M", "time":"2013-08-27 16:47:00"}] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
3	400	4303	Start time is greater than ned time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id
7	400	4311	Invalid application id or no data

Get Bandwidth Utilization

This URL gets the details of bandwidth utilization.

Resource URL

GET /ntbamonitors/{ntbaId}/bandwidthutilization? TopN=<TopN>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`TopN`	Number of top rows, default 50.	Number	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`bandwidthUtilizationList`	Bandwidth utilization list	Array

Details of bandwidthUtilizationList:

Field Name	Description	Data Type
`exporter`	Exporter	String
`exporterId`	Exported id	Number
`interface`	Interface name	String
`interfaceId`	Interface id	Number
`linkSpeed`	Link speed	String
`inbound`	Inbound traffic percentage	String
`outbound`	Outbound traffic percentage	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/bandwidthutilization

Response

```
{ "bandwidthUtilizationList":[{ "exporter":"M-1450", "exporterId":3, "interface":"1A", "interfaceId":0,
"linkSpeed":"1.0G", "inbound":"0%", "outbound":"0%"}] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id

Get Zone Traffic

This URL gets the list of zone traffic.

Resource URL

GET /ntbamonitors/{ntbaId}/zonetraffic? TopN=<TopN> &direction=<direction>&frequency=<frequency>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`TopN`	Number of top rows, default 50.	Number	No
`direction`	Direction: Bidirectional inbound outbound	String	No
`frequency`	Frequency: 1min 10mins hourly daily	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`zoneTrafficList`	Zone traffic	Array

Details of zoneTrafficList:

Field Name	Description	Data Type
`zone`	Zone name	String
`zoned`	Zone id	Number
`inbound`	Inbound traffic	String
`outbound`	Outbound traffic	String
`lastseen`	Last seen	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/zonetraffic

Response

```
{ “ zoneTrafficList ”:[{ “zone”:”Inside Zone”, “zoneId”:1191186432, “inbound”:”7M”, “outbound”:”7M”, “lastseen”:
2013-08-27 16:47:00”}] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id

Get Active Services

This URL gets the list of active services.

Resource URL

GET /ntbamonitors/{ntbaId}/activeservices? TopN=<TopN>
&timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`TopN`	Number of top rows, default 50.	Number	No

Field Name	Description	Data Type	Mandatory
`timePeriod`	Duration: can be • LAST_MINUTE • LAST_10_MINUTES • LAST_HOUR • LAST_24_HOURS • CUSTOM Custom incase start and end time is provided	String	No
`startTime`	Start time in the format: yyyy-MM-dd HH:mm	String	No
`endTime`	End time in the format: yyyy-MM-dd HH:mm	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`services`	List of services	Array

Details of services:

Field Name	Description	Data Type
`service`	Service name	String
`serviceId`	Service id	Number
`protocol`	Protocol	String
`lastSeen`	Last seen	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/activeservices?timePeriod=CUSTOM&startTime=2012-APR-20%2012:15&endTime=2012-APR-20%2012:11

Response

```
{ “services”:[{ “service”:”Unprofiled”, “serviceId”:0, “protocol”:”ipv4”, “lastSeen”:”2013-08-27 16:44:06” }] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id

Get Host Active Services

This URL gets the list of host active services.

Resource URL

GET /ntbamonitors/{ntbaId}/tophostactiveservices/<host_id>? TopN=<TopN>
&timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`TopN`	Number of top rows, default 50.	Number	No
`timePeriod`	Duration: can be • LAST_MINUTE • LAST_10_MINUTES • LAST_HOUR • LAST_24_HOURS • CUSTOM Custom incase start and end time is provided	String	No
`startTime`	Start time in the format: yyyy-MM-dd HH:mm	String	No
`endTime`	End time in the format: yyyy-MM-dd HH:mm	String	No
`Host_id`	Host id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`services`	List of services	Array

Details of services:

Field Name	Description	Data Type
`service`	Service name	String
`serviceId`	Service id	Number

Field Name	Description	Data Type
`protocol`	Protocol	String
`lastSeen`	Last seen	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/tophostactiveservices/9?timePeriod=CUSTOM&startTime=2012-APR-20%2012:15&endTime=2012-APR-20%2012:11

Response

```
{ "services":[{ "service":"Unprofiled", "serviceId":0, "protocol":"ipv4", "lastSeen":"2013-08-27 16:44:06" }] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id
7	400	4310	Invalid host id or no data

Get New Services

This URL gets the list of new services.

Resource URL

GET /ntbamonitors/{ntbaId}/newservices? TopN=<TopN>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`TopN`	Number of top rows, default 50.	Number	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
services	List of services	Array

Details of services:

Field Name	Description	Data Type
service	Service name	String
serviceId	Service id	Number
protocol	Protocol	String
lastSeen	Last seen	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/newservices

Response

```
{ "services":[{ "service":"Unprofiled", "serviceId":0, "protocol":"ipv4", "lastSeen":"2013-08-27 16:44:06" }] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id

Get Active Applications

This URL gets the list of active applications.

Resource URL

GET /ntbamonitors/{ntbaId}/activeapplications? TopN=<TopN>
&timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>

Request Parameters

Field Name	Description	Data Type	Mandatory
ntbaId	NTBA monitor id	Number	Yes

Field Name	Description	Data Type	Mandatory
`TopN`	Number of top rows, default 50.	Number	No
`timePeriod`	Duration: can be • LAST_MINUTE • LAST_10_MINUTES • LAST_HOUR • LAST_24_HOURS • CUSTOM Custom incase start and end time is provided	String	No
`startTime`	Start time in the format: yyyy-MM-dd HH:mm	String	No
`endTime`	End time in the format: yyyy-MM-dd HH:mm	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`applications`	List of applications	Array

Details of applications:

Field Name	Description	Data Type
`applicationName`	Application name	String
`applicationId`	Application id	Number
`starttime`	Start time	String
`lastSeen`	Last seen	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/activeapplications?timePeriod=CUSTOM&startTime=2012-APR-20%2012:15&endTime=2012-APR-20%2012:11

Response

```
{ "applications":[{ "applicationName":"FTP", "applicationId":1191186432, "starttime":"2013-08-27 16:44:06",
"lastseen":"2013-08-27 16:44:06"} }] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id

Get New Applications

This URL gets the list of new applications.

Resource URL

GET /ntbamonitors/{ntbaId}/newapplications? TopN=<TopN>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`TopN`	Number of top rows, default 50.	Number	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`applications`	List of applications	Array

Details of applications:

Field Name	Description	Data Type
`applicationName`	Application name	String
`applicationId`	Application id	Number
`starttime`	Start time	String
`lastSeen`	Last seen	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/newapplications

Response

```
{ "applications":[{ "applicationName":"FTP", "applicationId":1191186432, "starttime":"2013-08-27 16:44:06",
"lastseen":"2013-08-27 16:44:06"} }] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id

Get Host Active Applications

This URL gets the list of host active applications.

Resource URL

GET /ntbamonitors/{ntbaId}/tophostactiveapplications/<host_id>? TopN=<TopN>
&timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>

Request Parameters

Field Name	Description	Data Type	Mandatory
`ntbaId`	NTBA monitor id	Number	Yes
`TopN`	Number of top rows, default 50.	Number	No
`timePeriod`	Duration: can be • LAST_MINUTE • LAST_10_MINUTES • LAST_HOUR • LAST_24_HOURS • CUSTOM Custom incase start and end time is provided	String	No
`startTime`	Start time in the format: yyyy-MM-dd HH:mm	String	No
`endTime`	End time in the format: yyyy-MM-dd HH:mm	String	No
`Host_id`	Host id	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`applications`	List of applications	Array

Details of applications :

Field Name	Description	Data Type
`applicationName`	Application name	String
`applicationId`	Application id	Number
`starttime`	Start time	String
`lastSeen`	Last seen	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/tophostactiveapplications/9?timePeriod=CUSTOM&startTime=2012-APR-20%2012:15&endTime=2012-APR-20%2012:11

Response

```
{ "applications":[{ "applicationName":"FTP", "applicationId":1191186432, "starttime":"2013-08-27 16:44:06",
"lastseen":"2013-08-27 16:44:06"} }] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id
7	400	4310	Invalid host id or no data

Get Host Ports

This URL gets the list of host ports.

Resource URL

GET /ntbamonitors/{ntbaId}/tophostports/<host_id>? TopN=<TopN>
&timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>

Request Parameters

Field Name	Description	Data Type	Mandatory
ntbaId	NTBA monitor id	Number	Yes
TopN	Number of top rows, default 50.	Number	No
timePeriod	Duration: can be • LAST_MINUTE • LAST_10_MINUTES • LAST_HOUR • LAST_24_HOURS • CUSTOM Custom incase start and end time is provided	String	No
startTime	Start time in the format: yyyy-MM-dd HH:mm	String	No
endTime	End time in the format: yyyy-MM-dd HH:mm	String	No
Host_id	Host_id	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
hostports	List of ports	Array

Details of applications:

Field Name	Description	Data Type
port	Port	String
protocol	Protocol	Number
starttime	Start time	String
lastSeen	Last seen	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/ntbamonitors/1006/tophostports/9?timePeriod=CUSTOM&startTime=2012-APR-20%2012:15&endTime=2012-APR-20%2012:11

Response

```
{ "hostports":[{ "port":8888, "protocol":”ftp”, "starttime":"2013-08-27 16:44:06", "lastseen":"2013-08-27
16:44:06"} }] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	4303	Start time is greater than end time
4	400	4304	Invalid date format
5	400	4305	Start/End date is not provided
6	400	4306	Invalid NTBA id
7	400	4310	Invalid host id or no data

Get Endpoint Intelligence

This URL gets the list of executables running on your internal endpoints.

Resource URL

GET /<nbaid>/endpointintelligence?
search=<search_string>&&confidencetype=<confidencetype>&&classificationtype=<classificationtype>&&duration=<duration>

Request Parameters

Field Name	Description	Data Type	Mandatory
nbaId	NTBA monitors id	String	Yes
Search	Search string	String	No
confidencetype	Confidence type • any • block • allow • unclassified Default: any	String	No
classificationtype	Classification type • high • any Default: any	String	No
duration	Duration • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST-12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
EndpointExecutableList	List of endpoint executables	Array

Details of EndpointExecutableList:

Field Name	Description	Data Type
executableHash	Executable hash	String

Field Name	Description	Data Type
`executableName`	Executable name	String
`executableVersions`	Executable versions	String
`classification`	Classification	String
`fileSize`	File size	String
`firstseen`	First seen	String
`lastseen`	Last seen	String
`endpointsCount`	Endpoints count	Int
`connectionsCount`	Connections count	Int
`eventsCount`	Events count	Int
`comment`	Comment	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/1001/endpointintelligence/%20endpointintelligence?duration=LAST_14_DAYS&&confidencetype=any&&classificationtype=any

Response

```
{ "endpointExecutableList":[ {"executableHash":"1aaaaaaaaaaaaaaaaaaaaaaaaaaaaaa23", "executableName":"abc.exe",
"executableVersions":"file_version", "malwareConfidence":"Medium", "classification":"unclassified", "fileSize":
2566795, "firstSeen":"2013-09-10 00:00:00", "lastSeen":"2013-09-10 12:45:00", "endpointsCount":1,
"connectionsCount":4, "eventsCount":12}] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	3601	Invalid duration
3	400	3603	Invalid confidence type
4	400	3604	Invalid classification type
4	400	4904	Failed to retrieve data

Get Executable Information

This URL gets the executable information for given hash value.

Resource URL

GET /<nbaid>/endpointintelligence/<hash>/executableinformation? duration=<duration>

Request Parameters

Field Name	Description	Data Type	Mandatory
`duration`	Duration	String	No

Field Name	Description	Data Type	Mandatory
	• LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST-12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS		
hash	Hash	String	Yes
nbaId	NTBA monitors id	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
EndpointExecutableList	List of endpoint executables	Array

Details of EndpointExecutableList:

Field Name	Description	Data Type
properties	Executable properties	Object
heuristics	Heuristics data	Object
libraryProcesses	Process using this library	Object
parentProcesses	Parent process	Object
suspiciousLibraries	Suspicious libraries	Object

Details of properties:

Field Name	Description	Data Type
hash	Executable hash	String
binaryType	Binary type	String
binaryName	Binary name	String
productName	Product name	String
productVersion	Product version	String
overallMalwareConfidence	Overall malware confidence	String
eiaAgentMalwareConfidence	EIA agent malware confidence	String
classification	Classification	String
classifier	Classifier	String
classified	Classified	String

Field Name	Description	Data Type
`filesize`	File size	Long

Details of heuristics:

Field Name	Description	Data Type
`digitallySigned`	Digitally signed	String
`certificateStatus`	Certificate status	String
`packed`	Packed	String
`resourceSection`	Resource section	String
`smallerThan500KB`	Smaller than 500 KB	String
`embeddedUI`	Embedded UI	String
`obfuscatedFileExtention`	Obfuscated file extension	String
`recentlyModified`	Recently modified	String
`gtiReputation`	GTI reputation	String

Details of parentProcesses:

Field Name	Description	Data Type
`hash`	Hash value	String
`name`	Name	String

Details of suspiciousLibraries and libraryProcesses:

Field Name	Description	Data Type
`hash`	Hash value	String
`name`	Name	String
`malwareConfidence`	Malware confidence	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/1001/endpointintelligence/aaaaaaa16/%20executableinformation?duration=LAST_14_DAYS

Response

```
{ "properties": {"hash":"1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa23", "binaryType":"Process", "binaryName":"abc.exe",
"productName":"", "productVersion":"file_version", "overallMalwareConfidence":"Medium",
"eiaAgentMalwareConfidence":"Medium", "classification":"unclassified", "classifier":"---","filesize":2566795},
"heuristics":{}, "suspiciousLibraries":[{ "hash":"1aaaaaaaaaaaaaaaaaaaaaaaaaaaaab1", "name":"abc_dll.dll",
"malwareConfidence":"High"}] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	3601	Invalid duration
2	400	4901	Invalid hash/failed retrieve

Get Endpoints

This URL gets the endpoints information.

Resource URL

GET /<nbaid>/endpointintelligence/<hash>/endpoints? duration=<duration>

Request Parameters

Field Name	Description	Data Type	Mandatory
`duration`	Duration • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST-12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	No
`hash`	Hash	String	Yes
`nbaId`	NTBA monitors id	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`EndpointList`	List of endpoints	Array

Details of EndpointList:

Field Name	Description	Data Type
`ipAddress`	Executable hash	String
`hostName`	Executable name	String
`os`	Executable versions	String
`user`	Classification	String
`connectionsCount`	Connections count	Int
`eventsCount`	Events count	Int

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/1001/endpointintelligence/aaaaaaaa16/endpoints?duration=LAST_14_DAYS

Response

```
{ "endpointList": [{"ipAddress":"2.1.1.1","hostName":"","os":"","user":"poori.com\
\admin@test.com","connectionsCount":3,"eventsCount":0}] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	3601	Invalid duration
2	400	4901	Invalid hash/failed retrieve

Get Applications

This URL gets the applications information.

Resource URL

GET /<nbaid>/endpointintelligence/<hash>/applications? duration=<duration>

Request Parameters

Field Name	Description	Data Type	Mandatory
`duration`	Duration • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST-12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	No
`hash`	Hash	String	Yes
`nbaId`	NTBA monitors id	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`ApplicationList`	List of applications	Array

Details of ApplicationList:

Field Name	Description	Data Type
`applicationName`	Application name	String

Field Name	Description	Data Type
`connectionsCount`	Connections count	Int
`eventsCount`	Events count	Int

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/1001/endpointintelligence/aaaaaaa16/applications?duration=LAST_14_DAYS

Response

```
{ {" applicationList ":[{" applicationName ":"abc.exe","connectionscount":1,"eventsCount":0}] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	3601	Invalid duration
2	400	4901	Invalid hash/failed retrieve

Get Events

This URL gets the events information.

Resource URL

GET /<nbaid>/endpointintelligence/<hash>/events? duration=<duration>

Request Parameters

Field Name	Description	Data Type	Mandatory
`duration`	Duration • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST-12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	No
`hash`	Hash	String	Yes
`nbaId`	NTBA monitors id	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`eventList`	List of events	Array

Details of eventList:

Field Name	Description	Data Type
`time`	Attack time	String
`attack`	Attack	String
`result`	Result	String
`direction`	Direction	String
`attackerIpAddress`	Attacker ip address	String
`attackerCountry`	Attacker country	String
`victimIpAddress`	Victim ip address	String
`victimPort`	Victim port	Int
`victimCountry`	Victim country	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/1001/endpointintelligence/aaaaaaaa16/events?duration=LAST_14_DAYS

Response

```
{ {"eventList":[{"time":"Tue Sep 10 17:16:26 IST 2013","attack":"MALWARE: High-confidence malware executable
detected by Endpoint Intelligence Agent
engine","result":"Inconclusive","direction":"Unknown","attackerCountry":"---","victimIpAddress":"0.1.138.146","v
ictimPort":0,"victimCountry}] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	3601	Invalid duration
2	400	4901	Invalid hash/failed retrieve

Action on Hash

This URL to perform the action on hash to make it allow/block/unclassified.

Resource URL

PUT /<nbaid>/endpointintelligence/<hash>/takeaction/<action>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`hash`	Hash	String	Yes
`Action`	Action	String	Yes

Field Name	Description	Data Type	Mandatory
	• Allow • Block • Unclassified		
`nbaId`	NTBA monitors id	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Status	Int

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/1001/endpointintelligence/aaaaaaaa16/takeaction/Allow

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	3601	Invalid duration
2	400	4901	Invalid hash
3	400	4903	Invalid action

Get NMS IPs at Domain

This URL gets the NMS IP's present at the domain and the parent domains.

Resource URL

GET /domain/<domain_id> /nmsips

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domainId	Domain id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
NMSIPList	Contains the list of NMS IP's	ObjectList

Details of fields in NMSIPList:

Field Name	Description	Data Type
NMSIPDetails	NMS IP details	Object

Details of fields in NMSIPDetails:

Field Name	Description	Data Type
IPAddress	NMS IP	String
IPId	Id of the NMS IP	Number
createdAt	Resource where the NMS IP was created	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/101/nmsips

Response

```
{ "nmsIPDetails": [ { "IPAddress": "1.1.1.1", "IPId": 49, "createdAt": "/My Company" }, { "IPAddress":
"2.2.2.2", "IPId": 50, "createdAt": "/My Company/Test Child Domain 1" } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Create NMS IP at Domain

This URL creates the NMS IP at domain.

Resource URL

POST /domain/<domain_id> /nmsip

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`NMSIPAddress`	Contains the NMS IP	Object	Yes

Details of fields in NMSIPAddress:

Field Name	Description	Data Type	Mandatory
`IPAddress`	NMS IP	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique id of the created domain	Number

Example

Request

POST https://<NSM_IP>/sdkapi/domain/0/nmsip

Payload

```
{ "IPAddress": "1.1.1.1" }
```

Response

```
{ "createdResourceId": 49 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	5601	IP address cannot be empty

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
3	400	5602	Same IP already exists in Sensor
4	400	5603	Same IP already exists in domain
5	400	5604	Maximum IP addresses allowed exceeded
6	400	5605	Maximum IPv6 addresses allowed exceeded
7	400	5606	Maximum IPv4 addresses allowed exceeded
8	400	5607	IP address not present in this domain
9	400	1406	Invalid IP format

Delete the NMS IP at Domain

This URL deletes the NMS IP at domain.

Resource URL

DELETE / domain/<domain_id> /nmsip/<ipId>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes
`IPId`	NMS IP id	Number	Yes

Payload Parameters:

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/domain/0/nmsip/49

Payload

None

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	5601	IP address cannot be empty
3	400	5607	IP address not present in this domain
4	400	1406	Invalid IP format

Get NMS IPs at Sensor

This URL gets the NMS IPs allocated and created at the Sensor.

Resource URL

GET /sensor/<sensor_id> /nmsips

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`NMSIPList`	Contains the list of NMS IP's	ObjectList

Details of fields in NMSIPList:

Field Name	Description	Data Type
`NMSIPDetails`	NMS IP details	Object

Details of fields in NMSIPDetails:

Field Name	Description	Data Type
`IPAddress`	NMS IP	String
`IPId`	Id of the NMS IP	Number
`createdAt`	Resource where the NMS IP was created	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/nmsips

Response

```
{ "nmsIPDetails": [ { "IPAddress": "1.1.1.1", "IPId": 49, "createdAt": "/My Company" }, { "IPAddress":
"2.2.2.2", "IPId": 50, "createdAt": "Sensor" } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1124	The Sensor is inactive
3	400	5401	FIPS enabled on Sensor

Get available NMS IPs at Sensor

This URL gets the NMS IPs available at domain to allocate to the Sensor.

Resource URL

GET /sensor/<sensor_id> /nmsips/available

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensorId	Sensor id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
NMSIPList	Contains the list of NMS IP's	ObjectList

Details of fields in NMSIPList:

Field Name	Description	Data Type
NMSIPDetails	NMS IP details	Object

Details of fields in NMSIPDetails:

Field Name	Description	Data Type
IPAddress	NMS IP	String
IPId	Id of the NMS IP	Number

Field Name	Description	Data Type
`createdAt`	Resource where the NMS IP was created	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/nmsips/available

Response

```
{ "nmsIPDetails": [ { "IPAddress": "1.1.1.1", "IPId": 49, "createdAt": "/My Company" } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1124	The Sensor is inactive
3	400	5401	FIPS enabled on Sensor

Create NMS IP at Sensor

This URL creates the NMS user at the Sensor.

Error Information

POST /sensor/<sensor_id> /nmsip

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`NMSIPAddress`	Contains the NMS IP	Object	Yes

Details of fields in NMSIPAddress:

Field Name	Description	Data Type	Mandatory
`IPAddress`	NMS IP	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique id of the created domain	Number

Example

Request

POST https://<NSM_IP>/sdkapi/sensor/1001/nmsip

Payload

```
{ "IPAddress": "1.1.1.1" }
```

Response

```
{ "createdResourceId": 25 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1124	The Sensor is inactive
3	400	5401	FIPS enabled on Sensor
4	400	5601	IP address cannot be empty
5	400	5602	Same IP already exists in Sensor
6	400	5603	Same IP already exists in domain
7	400	5604	Maximum IP addresses allowed exceeded
8	400	5605	Maximum IPv6 addresses allowed exceeded
9	400	5606	Maximum IPv4 addresses allowed exceeded
10	400	5607	IP address not present in this domain
11	400	1406	Invalid IP format

Allocate NMS IP to Sensor

This URL allocates the NMS IP to Sensor.

Resource URL

POST /sensor/<sensor_id> /nmsip/allocate/<ipId>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes
`IPId`	NMS IP id	Number	Yes

Payload Parameters:

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique id of the created domain	Number

Example

Request

POST https://<NSM_IP>/sdkapi/sensor/1001/nmsip/allocate/49

Payload

None

Response

```
{ "createdResourceId": 50 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1124	The Sensor is inactive
3	400	5401	FIPS enabled on Sensor
4	400	5601	IP address cannot be empty
5	400	5602	Same IP already exists in Sensor
6	400	5603	Same IP already exists in domain
7	400	5604	Maximum IP addresses allowed exceeded
8	400	5605	Maximum IPv6 addresses allowed exceeded
9	400	5606	Maximum IPv4 addresses allowed exceeded

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
10	400	5607	IP address not present in this domain
11	400	1406	Invalid IP format
12	400	5608	Invalid IP id given for allocation: ID

Delete the NMS IP at Sensor

This URL deletes the NMS IP at the Sensor.

Resource URL

DELETE / sensor/<sensor_id> /nmsip

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes
`IPId`	NMS IP id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`NMSIPAddress`	Contains the NMS IP	Object	Yes

Details of fields in NMSIPAddress:

Field Name	Description	Data Type	Mandatory
`IPAddress`	NMS IP	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/sensor/1001/nmsip

Payload

```
{ "IPAddress": "1.1.1.1" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1124	The Sensor is inactive
3	400	5401	FIPS enabled on Sensor
4	400	5601	IP address cannot be empty
5	400	5602	Same IP already exists in Sensor
6	400	5603	Same IP already exists in domain
7	400	5604	Maximum IP addresses allowed exceeded
8	400	5605	Maximum IPv6 addresses allowed exceeded
9	400	5606	Maximum IPv4 addresses allowed exceeded
10	400	5607	IP address not present in this domain
11	400	1406	Invalid IP format

Get NMS Users at Domain

This URL gets the NMS users present at the domain and the parent domains.

Resource URL

GET /domain/<domain_id> /nmsusers

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`NMSUserList`	Contains the list of NMS users	ObjectList

Details of fields in NMSUserList:

Field Name	Description	Data Type
`NMSUserDetails`	NMS user details	Object

Details of fields in NMSUserDetails:

Field Name	Description	Data Type
`userName`	Name of the NMS user	String
`userId`	ID of the NMS user	Number
`createdAt`	Resource where the NMS user was created	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/101/nmsusers

Response

```
{ "nmsUserDetails": [ { "userName": "user1", "userId": 14, "createdAt": "/My Company" }, { "userName":
"admin123", "userId": 9, "createdAt": "/My Company/Test Child Domain 1" }, { "userName": "user1234", "userId":
10, "createdAt": "/My Company/Test Child Domain 1" } ] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Create NMS User at Domain

This URL creates the NMS user at domain.

Resource URL

POST /domain/<domain_id> /nmsuser

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`NMSUser`	Contains the details of the NMS user	Object	Yes

Details of fields in NMSUser:

Field Name	Description	Data Type	Mandatory
`userName`	Name of the NMS user	String	Yes
`authenticationKey`	Authentication key for the NMS user	String	Yes
`privateKey`	Private key for the NMS user	String	Yes

Response Parameter

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique ID of the created domain	Number

Example

Request

POST https://<NSM_IP>/sdkapi/domain/0/nmsuser

Payload

```
{ "userName": "user2", "authenticationKey": "admin1235", "privateKey": "admin1235" }
```

Response

```
{ "createdResourceId": 14 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	5601	User name, private key and authorization key are mandatory
3	400	5602	User name, private key and authorization key should be alphanumeric
4	400	5603	User name's length should be between 8 and 31
5	400	5604	Length of private key and authorization key should be between 8 and 15
6	400	5605	User name exists in Sensor
7	400	5606	User name exists in same or parent domain
8	400	5607	Maximum users that can be handled by Sensor crossed
9	400	5608	This feature not supported on Sensor
10	400	5609	User name cannot be changed
11	400	5610	This object has been created in some other domain: Cannot be deleted/edited

Update NMS User at Domain

This URL updates the NMS user at domain.

Resource URL

PUT /domain/<domain_id> /nmsuser/<nmsuser_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Field Name	Description	Data Type	Mandatory
`nmsUserId`	Id of the NMS user	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`NMSUser`	Contains the details of the NMS user	Object	Yes

Details of fields in NMSUser:

Field Name	Description	Data Type	Mandatory
`userName`	Name of the NMS user	String	Yes
`authenticationKey`	Authentication key for the NMS user	String	Yes
`privateKey`	Private key for the NMS user	String	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

POST https://<NSM_IP>/sdkapi/domain/0/nmsuser/14

Payload

```
{ "userName": "user2", "authenticationKey": "admin123", "privateKey": "admin123" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	5601	User name, private key and authorization key are mandatory
3	400	5602	User name, private key and authorization key should be alphanumeric
4	400	5603	User name's length should be between 8 and 31

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
5	400	5604	Length of private key and authorization key should be between 8 and 15
6	400	5605	User name exists in Sensor
7	400	5606	User name exists in same or parent domain
8	400	5607	Maximum users that can be handled by Sensor crossed
9	400	5608	This feature not supported on Sensor
10	400	5609	User name cannot be changed
11	400	5610	This object has been created in some other domain: Cannot be deleted/edited
12	500	3514	Invalid user id message from backend: Array index out of range: 0

Get the NMS User Details at Domain

This URL gets the NMS user details.

Resource URL

GET / domain/<domain_id> /nmsuser/<nmsuser_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes
`nmsUserId`	Id of the NMS user	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type	Mandatory
`NMSUser`	Contains the details of NMS users	ObjectList	Yes

Details of fields in NMSUser:

Field Name	Description	Data Type	Mandatory
`userName`	Name of the NMS user	String	Yes
`authenticationKey`	Authentication key for the NMS user	String	Yes
`privateKey`	Private key for the NMS user	String	Yes

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/nmsuser/14

Payload

None

Response

```
{ "userName": "user2", "authenticationKey": "admin123", "privateKey": "admin123" }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	500	3514	Invalid user id message from backend: Array index out of range: 0

Delete the NMS User at Domain

This URL deletes the NMS user.

Resource URL

DELETE / domain/<domain_id> /nmsuser/<nmsuser_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes
`nmsUserId`	Id of the NMS user	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/domain/0/nmsuser/14

Payload

None

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	500	3514	Invalid user id Message from backend: Array index out of range: 0

Get NMS Users at Sensor

This URL gets the NMS users allocated and created at the Sensor.

Resource URL

GET /sensor/<sensor_id> /nmsusers

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`NMSUserList`	Contains the list of NMS users	ObjectList

Details of fields in NMSUserList:

Field Name	Description	Data Type
`NMSUserDetails`	NMS user details	Object

Details of fields in NMSUserDetails:

Field Name	Description	Data Type
`userName`	Name of the NMS user	String

Field Name	Description	Data Type
`userId`	Id of the NMS user	Number
`createdAt`	Resource where the NMS user was created	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/nmsusers

Response

```
{ "nmsUserDetails": [ { "userName": "user1", "userId": 14, "createdAt": "/My Company" }, { "userName":
"admin123", "userId": 9, "createdAt": "Sensor" } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1124	The Sensor is inactive
3	400	5401	FIPS enabled on Sensor

Get Available NMS Users at Sensor

This URL gets the NMS users available at domain to allocate to the Sensor.

Resource URL

GET /sensor/<sensor_id> /nmsusers/available

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`NMSUserList`	Contains the list of NMS users	ObjectList

Details of fields in NMSUserList:

Field Name	Description	Data Type
`NMSUserDetails`	NMS user details	Object

Details of fields in NMSUserDetails:

Field Name	Description	Data Type
`userName`	Name of the NMS user	String
`userId`	Id of the NMS user	Number
`createdAt`	Resource where the NMS user was created	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/nmsusers/available

Response

```
{ "nmsUserDetails": [ { "userName": "user1", "userId": 14, "createdAt": "/My Company" }, { "userName":
"admin123", "userId": 9, "createdAt": "/My Company " }, { "userName": "user1234", "userId": 10, "createdAt":
"/My Company" } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1124	The Sensor is inactive
3	400	5401	FIPS enabled on Sensor

Create NMS User at Sensor

This URL creates the NMS user at Sensor.

Resource URL

POST /sensor/<sensor_id> /nmsuser

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`NMSUser`	Contains the details of the NMS user	Object	Yes

Details of fields in NMSUser:

Field Name	Description	Data Type	Mandatory
`userName`	Name of the NMS user	String	Yes
`authenticationKey`	Authentication key for the NMS user	String	Yes
`privateKey`	Private key for the NMS user	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique id of the created domain	Number

Example

Request

POST https://<NSM_IP>/sdkapi/sensor/1001/nmsuser

Payload

```
{ "userName": "user2", "authenticationKey": "admin1235", "privateKey": "admin1235" }
```

Response

```
{ "createdResourceId": 20 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	5601	User name, private key and authorization key are mandatory
3	400	5602	User name, private key and authorization key should be alphanumeric
4	400	5603	User name's length should be between 8 and 31
5	400	5604	Length of private key and authorization key should be between 8 and 15
6	400	5605	User name exists in Sensor
7	400	5606	User name exists in same or parent domain
8	400	5607	Maximum users that can be handled by Sensor crossed

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
9	400	5608	This feature not supported on Sensor
10	400	5609	User name cannot be changed
11	400	5610	This object has been created in some other domain: Cannot be deleted/edited
12	400	1124	The Sensor is inactive
13	400	5401	FIPS enabled on Sensor

Allocate NMS User to Sensor

This URL allocates the NMS user to Sensor.

Resource URL

POST /sensor/<sensor_id> /nmsuser/<nmsuser_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensorId	Sensor id	Number	Yes
nmsUserId	Id of the NMS user	Number	Yes

Payload Parameters:

None

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
createdResourceId	Unique id of the created domain	Number

Example

Request

POST https://<NSM_IP>/sdkapi/sensor/1001/nmsuser/14

Payload

None

Response

```
{ "createdResourceId": 25 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	5601	User name, private key and authorization key are mandatory
3	400	5602	User name, private key and authorization key should be alphanumeric
4	400	5603	User name's length should be between 8 and 31
5	400	5604	Length of private key and authorization key should be between 8 and 15
6	400	5605	User name exists in Sensor
7	400	5606	User name exists in same or parent domain
8	400	5607	Maximum users that can be handled by Sensor crossed
9	400	5608	This feature not supported on Sensor
10	400	5609	User name cannot be changed
11	400	5610	This object has been created in some other domain: Cannot be deleted/edited
12	400	1124	The Sensor is inactive
13	400	5401	FIPS enabled on Sensor
14	400	5110	Invalid user id

Update NMS User at Sensor

This URL updates the NMS user at Sensor.

Resource URL

PUT /sensor/<sensor_id> /nmsuser/<nmsuser_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes
`nmsUserId`	Id of the NMS user	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`NMSUser`	Contains the details of the NMS user	Object	Yes

Details of fields in NMSUser:

Field Name	Description	Data Type	Mandatory
`userName`	Name of the NMS user	String	Yes
`authenticationKey`	Authentication key for the NMS user	String	Yes
`privateKey`	Private key for the NMS user	String	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

POST https://<NSM_IP>/sdkapi/sensor/1001/nmsuser/20

Payload

```
{ "userName": "user2", "authenticationKey": "admin123", "privateKey": "admin123" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	5601	User name, private key and authorization key are mandatory

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
3	400	5602	User name, private key and authorization key should be alphanumeric
4	400	5603	User name's length should be between 8 and 31
5	400	5604	Length of private key and authorization key should be between 8 and 15
6	400	5605	User name exists in Sensor
7	400	5606	User name exists in same or parent domain
8	400	5607	Maximum users that can be handled by Sensor crossed
9	400	5608	This feature not supported on Sensor
10	400	5609	User name cannot be changed
11	400	5610	This object has been created in some other domain: Cannot be deleted/edited
12	400	1124	The Sensor is inactive
13	400	5401	FIPS enabled on Sensor
14	400	5110	Invalid user id

Get the NMS User Details at Sensor

This URL gets the NMS user details.

Resource URL

GET / sensor/<sensor_id> /nmsuser/<nmsuser_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes
`nmsUserId`	Id of the NMS user	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type	Mandatory
NMSUser	Contains the details of the NMS user	Object	Yes

Details of fields in NMSUser:

Field Name	Description	Data Type	Mandatory
userName	Name of the NMS user	String	Yes
authenticationKey	Authentication key for the NMS user	String	Yes
privateKey	Private key for the NMS user	String	Yes

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/nmsuser/20

Payload

None

Response

```
{ "userName": "user2", "authenticationKey": "admin123", "privateKey": "admin123" }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1124	The Sensor is inactive
3	400	5401	FIPS enabled on Sensor
4	400	5110	Invalid user id

Delete the NMS User at Sensor

This URL deletes the NMS user at Sensor.

Resource URL

DELETE / sensor/<sensor_id> /nmsuser/<nmsuser_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensorId	Sensor id	Number	Yes
nmsUserId	Id of the NMS user	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/sensor/1001/nmsuser/20

Payload

None

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1124	The Sensor is inactive
3	400	5401	FIPS enabled on Sensor
4	400	5110	Invalid user id

Get the List of Importable IPS and Reconnaissance Policies

This URL gets the list of importable IPS and reconnaissance policies.

Resource URL

PUT /domain/<domain_id>/ipsreconpolicy/import

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`MultiPart`	Holds the body part objects	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
`BodyPart[0]`	Holds the import file element object	Application/json object	Yes

Details of ImportFileElement:

Field Name	Description	Data Type	Mandatory
`fileName`	Name of the file	String	Yes
`fileType`	File type should be "XML"	String	Yes
`selectedPolicyNameList`	List of the names of the policy to be imported	StringList	No

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
`BodyPart[1]`	Holds the file as input stream	Application/octet-stream	Yes

Details of .xml file:

Field Name	Description	Data Type	Mandatory
`File`	Policy(file input stream)	ByteArrayInput stream	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`PolicyDiffElementList`	Contains the list of the policy status when the policy present on XML is compared by the policy present on the Manager	ObjectList

Details of fields in PolicyDiffElementList:

Field Name	Description	Data Type
`PolicyDiffElement`	Difference between the policy present on the Manager and the XML file	Object

Details of fields in PolicyDiffElement:

Field Name	Description	Data Type
`policyId`	ID of the policy (-1 if not present on the Manager)	String
`policyName`	Name of the policy	String
`status`	Status of the policy when the policy on XML and Manager are compared	String
`outboundPolicyId`	Outbound ID of the policy (-1 if not present on the Manager)	String
`isOutbound`	If the policy is outbound	Boolean
`type`	If the policy is IPS (1) or reconnaissance (3)	Number
`import`	If the policy is importable (DISABLED if it is not importable)	String

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/ipsreconpolicy/import

Payload

Response

```
{ "policyDiffElement": [ { "status": "Exists and Not Identical", "policyName": "NSAT_AIWA_Blocking",
"outboundPolicyId": "312", "isOutbound": false, "policyId": "312", "import": "UNCHECKED", "type": 1 },
{ "status": "Exists and Identical", "policyName": "NSAT 7.1 Reconnaissance Policy", "isOutbound": false,
"policyId": "301", "import": "DISABLED", "type": 3 }, { "status": "Exists and Not Identical", "policyName":
"NSAT_AIWA_AlertNotf", "outboundPolicyId": "308", "isOutbound": false, "policyId": "309", "import": "UNCHECKED",
"type": 1 }, { "status": "Exists and Not Identical", "policyName": "NSAT_AIWA_SB", "outboundPolicyId": "315",
"isOutbound": false, "policyId": "316", "import": "UNCHECKED", "type": 1 }, { "status": "Exists and Not
Identical", "policyName": "NSAT All-Inclusive With Audit", "outboundPolicyId": "313", "isOutbound": false,
"policyId": "314", "import": "UNCHECKED", "type": 1 }, { "status": "Exists and Not Identical", "policyName":
"NSAT AIWA Filtered", "outboundPolicyId": "310", "isOutbound": false, "policyId": "311", "import": "UNCHECKED",
"type": 1 } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	5301	Invalid file type given for import
3	500	5302	Policy version not supported
4	500	5303	Unable to read file
5	500	5304	Unable to transfer file
6	400	5305	The policy given to import is not present in the file
7	400	5306	The policy given to import is not importable
8	500	5307	Policy import failed.. Please look into the logs..
9	500	2202	Input stream read error

Import the IPS and Reconnaissance Policies

This URL imports the IPS and reconnaissance policies.

Resource URL

POST /domain/<domain_id>/ipsreconpolicy/import

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`MultiPart`	Holds the body part objects	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
`BodyPart[0]`	Holds the import file element object	Application/json object	Yes

Details of ImportFileElement:

Field Name	Description	Data Type	Mandatory
`fileName`	Name of the file	String	Yes
`fileType`	File type should be "XML"	String	Yes
`selectedPolicyNameList`	List of the names of the policy to be imported	StringList	No

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
`BodyPart[1]`	Holds the file as input stream	Application/octet-stream	Yes

Details of .xml file:

Field Name	Description	Data Type	Mandatory
`File`	Policy(file input stream)	ByteArrayInput stream	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

POST https://<NSM_IP>/sdkapi/domain/0/ipsreconpolicy/import

Payload

```
----Boundary_1_12424925_1353496814940 Content-Type: application/json { "fileType": "xml",
"selectedPolicyNameList": ["NSAT_AIWA_Blocking"], "fileName": "IPS_ReconnaissancePolicy_latest_NSAT" } ----
Boundary_1_12424925_1353496814940 Content-Type: application/octet-stream <userinput><?xml version='1.0'
encoding='ISO-8859-1'?></userinput> <userinput><PolicyExport version="5.0"></userinput> <userinput><Recon
hash="ce408928d2292651da7acd44f32c4b7"></userinput> <userinput><ReconPolicy name="NSAT 7.1 Reconnaissance
Policy" visibleToChild="yes"></userinput> //….. ….. …..// <userinput><attack id="0xe000da00"
isActive="INHERIT"/></userinput> <userinput></customizedAttacks></userinput> <userinput></policy></userinput>
<userinput></IDSPolicy></userinput> <userinput></PolicyExport></userinput> ----
Boundary_1_12424925_1353496814940--
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	5301	Invalid file type given for import

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
3	500	5302	Policy version not supported
4	500	5303	Unable to read file
5	500	5304	Unable to transfer file
6	400	5305	The policy given to import is not present in the file
7	400	5306	The policy given to import is not importable
8	500	5307	Policy import failed.. Please look into the logs..
9	500	2202	Input stream read error

Import the Malware Policies

This URL imports the malware policies.

Resource URL

POST /domain/<domain_id>/malwarepolicy/import

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`MultiPart`	Holds the body part objects	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
`BodyPart[0]`	Holds the import file element object	Application/json object	Yes

Details of ImportFileElement:

Field Name	Description	Data Type	Mandatory
`fileName`	Name of the file	String	Yes
`fileType`	File type should be "XML"	String	Yes

Field Name	Description	Data Type	Mandatory
`skipDuplicate`	Whether the duplicate policies should be skipped(default is true)	Boolean	No

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
`BodyPart[1]`	Holds the file as input stream	Application/octet-stream	Yes

Details of .xml file:

Field Name	Description	Data Type	Mandatory
`File`	Policy(file input stream)	ByteArrayInput stream	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number
`message`	Message returned from the backend	String

Example

Request

POST https://<NSM_IP>/sdkapi/domain/0/malwarepolicy/import

Payload

```
----Boundary_1_12424925_1353496814940 Content-Type: application/json { "fileType": "xml", "skipDuplicate":
false, "fileName": "MalwarePolicies0" } ----Boundary_1_12424925_1353496814940 Content-Type: application/octet-
stream <?xml version='1.0' encoding='ISO-8859-1'?> <MalwarePolicyConfig> <MalwarePolicyExport
EMSVersion="8.0.5.9.108"> <MalwarePolicy> <MalwarePolicyVO name="TestMalwarePolicy_1" owner="0"
visibleToChild="yes" isEditable="yes" desc="VisibletoChildDomain"/> </MalwarePolicy> <MalwarePolicy>
<MalwarePolicyVO name="TestMalwarePolicy_2" owner="0" visibleToChild="no" isEditable="yes" desc="NotVisible
tochildDomain"/> </MalwarePolicy> <MalwarePolicy> <MalwarePolicyVO name="malware archive" owner="0"
visibleToChild="yes" isEditable="yes" desc=""> <MalwarePolicyProtocol idnum="16" enabled="yes"/>
<MalwarePolicyProtocol idnum="12" enabled="yes"/> </MalwarePolicyVO> <MalwarePolicyFileActions groupId="1"
engineStatus="19" alertingConfidence="5" blockingConfidence="5" sendTcpConfidence="5" quaratineConfidence="0"
saveFileConfidence="1" blacklistConfidence="0" fileSize="0"/> <MalwarePolicyFileActions groupId="2"
engineStatus="18" alertingConfidence="5" blockingConfidence="5" sendTcpConfidence="5" quaratineConfidence="0"
saveFileConfidence="1" blacklistConfidence="0" fileSize="0"/> <MalwarePolicyFileActions groupId="3"
engineStatus="27" alertingConfidence="5" blockingConfidence="5" sendTcpConfidence="5" quaratineConfidence="0"
saveFileConfidence="1" blacklistConfidence="0" fileSize="0"/> <MalwarePolicyFileActions groupId="4"
engineStatus="18" alertingConfidence="5" blockingConfidence="5" sendTcpConfidence="5" quaratineConfidence="0"
saveFileConfidence="1" blacklistConfidence="0" fileSize="0"/> <MalwarePolicyFileActions groupId="5"
engineStatus="3" alertingConfidence="5" blockingConfidence="5" sendTcpConfidence="5" quaratineConfidence="0"
saveFileConfidence="1" blacklistConfidence="0" fileSize="0"/> <MalwarePolicyFileActions groupId="6"
engineStatus="18" alertingConfidence="5" blockingConfidence="5" sendTcpConfidence="5" quaratineConfidence="0"
saveFileConfidence="1" blacklistConfidence="0" fileSize="0"/> </MalwarePolicy> </MalwarePolicyExport> </
MalwarePolicyConfig> ----Boundary_1_12424925_1353496814940--
```

Response

```
{ "status": 1, "message": ",,Importing Malware Policy: malware archive,Importing Malware Policy:
TestMalwarePolicy_2,Importing Malware Policy: TestMalwarePolicy_1, " }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	5301	Invalid file type given for import
3	500	5307	Policy import failed.. Please look into the logs..
4	500	2202	Input stream read error

Import the Firewall Policies

This URL imports the firewall policies.

Resource URL

POST /domain/<domain_id>/ firewallpolicy/import

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`MultiPart`	Holds the body part objects	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
`BodyPart[0]`	Holds the import file element object	Application/json object	Yes

Details of ImportFileElement:

Field Name	Description	Data Type	Mandatory
`fileName`	Name of the file	String	Yes
`fileType`	File type should be "XML"	String	Yes
`skipDuplicate`	Whether the duplicate policies should be skipped(default is true)	Boolean	No

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
`BodyPart[1]`	Holds the file as input stream	Application/octet-stream	Yes

Details of .xml file:

Field Name	Description	Data Type	Mandatory
`File`	Policy(file input stream)	ByteArrayInput stream	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number
message	Message returned from the backend	String

Example

Request

POST https://<NSM_IP>/sdkapi/domain/0/firewallpolicy/import

Payload

```
----Boundary_1_12424925_1353496814940 Content-Type: application/json { "fileType": "xml", "skipDuplicate":
false, "fileName": "FirewallPolicies0" } ----Boundary_1_12424925_1353496814940 Content-Type: application/octet-
stream <FWConfig> <NetworkObjects/> <FWPolicies> <FWPolicy owner_ad="My Company" policyName="FirewallPolicy4"
policyType="1" visibleToChild="false" policyDescription="Firewall Policy for Port"> <FWPolicyRules owner_ad="My
Company" uuid="108" Rulename="" direction="3" action="0" enablelog="N" description="" ordernum="0" type="1"
state="1" mandate_auth="N"> <SourceObjectMember> <NetworkObjectMember noid="-1" noname="" notype="1"
noconfig="1"/> </SourceObjectMember> <DestinationObjectMember> <NetworkObjectMember noid="-1" noname=""
notype="1" noconfig="1"/> </DestinationObjectMember> <ServiceObjectMember> <NetworkObjectMember noid="-1"
noname="" notype="8" noconfig="1"/> </ServiceObjectMember> //……// DestinationObjectMember> <NetworkObjectMember
noid="-1" noname="" notype="1" noconfig="1"/> </DestinationObjectMember> <ServiceObjectMember>
<NetworkObjectMember noid="-1" noname="" notype="8" noconfig="1"/> </ServiceObjectMember> <TimeObjectMember>
<NetworkObjectMember noid="-1" noname="" notype="9" noconfig="1"/> </TimeObjectMember> <UserObjectMember>
<NetworkObjectMember noid="-1" noname="" notype="32" noconfig="1"/> </UserObjectMember> </FWPolicyRules> </
FWPolicy> </FWPolicies> </FWConfig> ----Boundary_1_12424925_1353496814940--
```

Response

```
{ "status": 1, "message": "Added new Firewall Policy in the current Admin Domain : FirewallPolicy4 Added new
Firewall Policy in the current Admin Domain : FirewallPolicy3 Added new Firewall Policy in the current Admin
Domain : FirewallPolicy2 Added new Firewall Policy in the current Admin Domain : FirewallPolicy1" }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	5301	Invalid file type given for import
3	500	5307	Policy import failed.. Please look into the logs..
4	500	2202	Input stream read error

Import the Exceptions

This URL imports the firewall policies.

Resource URL

POST /domain/<domain_id>/ exceptions/import

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
MultiPart	Holds the body part objects	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the import file element object	Application/json object	Yes

Details of ImportFileElement:

Field Name	Description	Data Type	Mandatory
fileName	Name of the file	String	Yes
fileType	File type should be "XML"	String	Yes
skipDuplicate	Whether the duplicate policies should be skipped(default is true)	Boolean	No

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
BodyPart[1]	Holds the file as Input stream	Application/octet-stream	Yes

Details of .xml file:

Field Name	Description	Data Type	Mandatory
File	Policy(file input stream)	ByteArrayInput stream	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number
message	Message returned from the backend	String

Example

Request

POST https://<NSM_IP>/sdkapi/domain/0/exceptions/import

Payload

```
----Boundary_1_12424925_1353496814940 Content-Type: application/json {"fileType": "xml", "skipDuplicate": false,
"fileName": "IDSAlertFilter"} ----Boundary_1_12424925_1353496814940 Content-Type: application/octet-stream <?xml
version='1.0' encoding='ISO-8859-1'?> <AFConfig> <AlertFilterExport EMSVersion="8.1.3.1.22"> <AlertFilter
name="test1" visibleToChild="yes" addressType="0"> <AlertExclusion srcMode="2" dstMode="3" srcAddr="null"
srcMask="null" destAddr="null" destMask="null" srcPortType="0" srcPort="null" destPortType="0" destPort="null"/>
<AlertExclusion srcMode="1" dstMode="1" srcAddr="null" srcMask="null" destAddr="null" destMask="null"
srcPortType="0" srcPort="null" destPortType="0" destPort="null"/> </AlertFilter> <AlertFilter name="test2"
visibleToChild="yes" addressType="0"> <AlertExclusion srcMode="1" dstMode="1" srcAddr="null" srcMask="null"
destAddr="null" destMask="null" srcPortType="0" srcPort="null" destPortType="0" destPort="null"/> </AlertFilter>
<AlertFilter name="test3" visibleToChild="yes" addressType="0"> <AlertExclusion srcMode="1" dstMode="1"
srcAddr="null" srcMask="null" destAddr="null" destMask="null" srcPortType="0" srcPort="null" destPortType="0"
destPort="null"/> </AlertFilter> </AlertFilterExport> </AFConfig> ----Boundary_1_12424925_1353496814940--
```

Response

```
{ "status": 1, "message": ",,Importing Alert Filter: test3,Importing Alert Filter: test2,Importing Alert Filter:
test1" }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	5301	Invalid file type given for import
3	500	5307	Policy import failed.. Please look into the logs..
4	500	2202	Input stream read error

Gets the Exportable IPS Reconnaissance Policies from the Manager

This URL gets the exportable IPS reconnaissance policies from the Manager.

Resource URL

GET /domain/<domain_id>/ipsreconpolicy/export

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`exportablePolicyList`	List of exportable IPS & reconnaissance policies	Object

Details of exportablePolicyList:

Field Name	Description	Data Type
`exportablePolicyDetail`	List of exportable IPS & reconnaissance policy detail	ObjectList

Details of exportablePolicyDetail:

Field Name	Description	Data Type
`policyName`	Name of the policy	String
`policyType`	Type of the policy, one of the two: • IPS_POLICY • RECON_POLICY	String
`policyId`	ID of the policy	Integer

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/ipsreconpolicy/export

Response

```
{ 'exportablePolicyDetail': [{ 'policyName': 'DefaultIPSAttackSettings', 'policyType': 'IPS_POLICY', 'policyId':
-1 }, { 'policyName': 'DefaultIDS', 'policyType': 'IPS_POLICY', 'policyId': 0 }, { 'policyName': 'Null',
'policyType': 'IPS_POLICY', 'policyId': 18 }, { 'policyName': 'DefaultInlineIPS', 'policyType': 'IPS_POLICY',
'policyId': 19 }, { 'policyName': 'DefaultReconnaissancePolicy', 'policyType': 'RECON_POLICY', 'policyId':
300 }] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Export the IPS Reconnaissance Policies

This URL exports IPS reconnaissance policies from the Manager.

Resource URL

GET /domain/<domain_id>/ipsreconpolicy/export

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`selectedPolicyList`	List of the policies to export	Object	Yes

Details of selectedPolicyList:

Field Name	Description	Data Type	Mandatory
`selectedPolicyNameList`	List of name of IPS & reconnaissance policy to export. By default all the policies are exported.	StringList	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`byteStream`	Byte stream of the exported file	String

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/ipsreconpolicy/export

Payload

```
{ “selectedPolicyNameList”:[“DefaultInlineIPS”,“NSAT 7.1 Reconnaissance Policy”] }
```

Response

```
{ "byteSream": "<?xml version='1.0' encoding='ISO-8859-1'?> <PolicyExport version="5.0"> <Recon
hash="ce408928d2292651da7acd44f32c4b7"> <ReconPolicy name="NSAT 7.1 Reconnaissance Policy"
visibleToChild="yes"> //….. ….. …..// <attack id="0xe000da00" isActive="INHERIT"/> </customizedAttacks> </
policy> </IDSPolicy> </PolicyExport>" }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	5305	The policy given is not present: <policyname>

Gets the Exportable Malware Policies from the Manager

This URL gets the exportable malware policies from the Manager.

Resource URL

GET /domain/<domain_id>/malwarepolicy/export

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`exportablePolicyList`	List of exportable malware policies	Object

Details of exportablePolicyList:

Field Name	Description	Data Type
`exportablePolicyDetail`	List of exportable malware policy detail	ObjectList

Details of exportablePolicyDetail:

Field Name	Description	Data Type
`policyName`	Name of the policy	String
`policyType`	Type of the policy: • MALWARE_POLICY	String
`policyId`	ID of the policy	Integer

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/malwarepolicy/export

Response

```
{ 'exportablePolicyDetail': [{ 'policyName': 'DefaultMalwarePolicy', 'policyType': 'MALWARE_POLICY', 'policyId':
1 }, { 'policyName': 'TestMalwarePolicy_1', 'policyType': 'MALWARE_POLICY', 'policyId': 301 }, { 'policyName':
'TestMalwarePolicy_2', 'policyType': 'MALWARE_POLICY', 'policyId': 302 }, { 'policyName': 'malwarearchive',
'policyType': 'MALWARE_POLICY', 'policyId': 305 }] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Export the Malware Policies

This URL exports malware policies from the Manager.

Resource URL

PUT /domain/<domain_id>/malwarepolicy/export

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
selectedPolicyList	List of the policies to export	Object	Yes

Details of selectedPolicyList:

Field Name	Description	Data Type	Mandatory
selectedPolicyNameList	List of name of malware policy to export. By default all the policies are exported.	StringList	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
byteStream	Byte stream of the exported file	string

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/malwarepolicy/export

Payload

```
{ “selectedPolicyNameList”:[“ TestMalwarePolicy_1”,“ TestMalwarePolicy_2” ,“malware archive”] }
```

Response

```
{ "byteSream": " <?xml version='1.0' encoding='ISO-8859-1'?> <MalwarePolicyConfig> <MalwarePolicyExport
EMSVersion="8.0.5.9.108"> <MalwarePolicy> <MalwarePolicyVO name="TestMalwarePolicy_1" owner="0"
visibleToChild="yes" isEditable="yes" desc="VisibletoChildDomain"/> </MalwarePolicy> <MalwarePolicy>
<MalwarePolicyVO name="TestMalwarePolicy_2" owner="0" visibleToChild="no" isEditable="yes" desc="NotVisible
tochildDomain"/> </MalwarePolicy> <MalwarePolicy> <MalwarePolicyVO name="malware archive" owner="0"
visibleToChild="yes" isEditable="yes" desc=""> <MalwarePolicyProtocol idnum="16" enabled="yes"/>
<MalwarePolicyProtocol idnum="12" enabled="yes"/> </MalwarePolicyVO> <MalwarePolicyFileActions groupId="1"
engineStatus="19" alertingConfidence="5" blockingConfidence="5" sendTcpConfidence="5" quaratineConfidence="0"
saveFileConfidence="1" blacklistConfidence="0" fileSize="0"/> <MalwarePolicyFileActions groupId="2"
engineStatus="18" alertingConfidence="5" blockingConfidence="5" sendTcpConfidence="5" quaratineConfidence="0"
saveFileConfidence="1" blacklistConfidence="0" fileSize="0"/> <MalwarePolicyFileActions groupId="3"
engineStatus="27" alertingConfidence="5" blockingConfidence="5" sendTcpConfidence="5" quaratineConfidence="0"
saveFileConfidence="1" blacklistConfidence="0" fileSize="0"/> <MalwarePolicyFileActions groupId="4"
engineStatus="18" alertingConfidence="5" blockingConfidence="5" sendTcpConfidence="5" quaratineConfidence="0"
saveFileConfidence="1" blacklistConfidence="0" fileSize="0"/> <MalwarePolicyFileActions groupId="5"
engineStatus="3" alertingConfidence="5" blockingConfidence="5" sendTcpConfidence="5" quaratineConfidence="0"
saveFileConfidence="1" blacklistConfidence="0" fileSize="0"/> <MalwarePolicyFileActions groupId="6"
engineStatus="18" alertingConfidence="5" blockingConfidence="5" sendTcpConfidence="5" quaratineConfidence="0"
saveFileConfidence="1" blacklistConfidence="0" fileSize="0"/> </MalwarePolicy> </MalwarePolicyExport> </
MalwarePolicyConfig> " }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	5305	The policy given is not present: <policyname>

Gets the Exportable Firewall Policies from the Manager

This URL gets the exportable firewall policies from the Manager.

Resource URL

GET /domain/<domain_id>/firewallpolicy/export

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`exportablePolicyList`	List of exportable firewall policies	Object

Details of exportablePolicyList:

Field Name	Description	Data Type
`exportablePolicyDetail`	List of exportable firewall policy detail	ObjectList

Details of exportablePolicyDetail:

Field Name	Description	Data Type
`policyName`	Name of the policy	String
`policyType`	Type of the policy: • FIREWALL_POLICY	String
`policyId`	ID of the policy	Integer

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/firewallpolicy/export

Response

```
{ 'exportablePolicyDetail': [{ 'policyName': 'FirewallPolicy4', 'policyType': 'FIREWALL_POLICY', 'policyId':
107 }, { 'policyName': 'FirewallPolicy3', 'policyType': 'FIREWALL_POLICY', 'policyId': 105 }, { 'policyName':
'FirewallPolicy2', 'policyType': 'FIREWALL_POLICY', 'policyId': 103 }, { 'policyName': 'FirewallPolicy1',
'policyType': 'FIREWALL_POLICY', 'policyId': 101 }] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Export the firewall policies

This URL exports firewall policies from the Manager.

Resource URL

PUT /domain/<domain_id>/firewallpolicy/export

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
selectedPolicyList	List of the policies to export	Object	Yes

Details of selectedPolicyList:

Field Name	Description	Data Type	Mandatory
selectedPolicyNameList	List of name of firewall policy to export. By default all the policies are exported.	StringList	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
byteStream	Byte stream of the exported file	String

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/firewallpolicy/export

Payload

```
{ "selectedPolicyNameList":["FirewallPolicy4","FirewallPolicy3"] }
```

Response

```
{ "byteSream": “<FWConfig> <NetworkObjects/> <FWPolicies> <FWPolicy owner_ad="My Company"
policyName="FirewallPolicy4" policyType="1" visibleToChild="false" policyDescription="Firewall Policy for Port">
<FWPolicyRules owner_ad="My Company" uuid="108" Rulename="" direction="3" action="0" enablelog="N"
description="" ordernum="0" type="1" state="1" mandate_auth="N"> <SourceObjectMember> <NetworkObjectMember
noid="-1" noname="" notype="1" noconfig="1"/> </SourceObjectMember> <DestinationObjectMember>
<NetworkObjectMember noid="-1" noname="" notype="1" noconfig="1"/> </DestinationObjectMember>
<ServiceObjectMember> <NetworkObjectMember noid="-1" noname="" notype="8" noconfig="1"/> </
ServiceObjectMember> //……// DestinationObjectMember> <NetworkObjectMember noid="-1" noname="" notype="1"
noconfig="1"/> </DestinationObjectMember> <ServiceObjectMember> <NetworkObjectMember noid="-1" noname=""
notype="8" noconfig="1"/> </ServiceObjectMember> <TimeObjectMember> <NetworkObjectMember noid="-1" noname=""
notype="9" noconfig="1"/> </TimeObjectMember> <UserObjectMember> <NetworkObjectMember noid="-1" noname=""
notype="32" noconfig="1"/> </UserObjectMember> </FWPolicyRules> </FWPolicy> </FWPolicies> </FWConfig>” }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	5305	The policy given is not present: <policyname>

Gets the Exportable Exceptions from the Manager

This URL gets the exportable exceptions from the Manager.

Resource URL

GET /domain/<domain_id>/exceptions/export

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
exportablePolicyList	List of exportable exceptions	Object

Details of exportablePolicyList:

Field Name	Description	Data Type
exportablePolicyDetail	List of exportable exception detail	ObjectList

Details of exportablePolicyDetail:

Field Name	Description	Data Type
policyName	Name of the policy	String

Field Name	Description	Data Type
`policyType`	Type of the policy: • EXCEPTIONS	String
`policyId`	ID of the policy	Integer

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/exceptions/export

Response

```
{ 'exportablePolicyDetail': [{ 'policyName': 'test1', 'policyType': 'EXCEPTIONS', 'policyId': 301 },
{ 'policyName': 'test2', 'policyType': 'EXCEPTIONS', 'policyId': 302 }] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Export the Exceptions

This URL exports exceptions from the Manager.

Resource URL

PUT /domain/<domain_id>/exceptions/export

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`selectedPolicyList`	List of the policies to export	Object	Yes

Details of selectedPolicyList:

Field Name	Description	Data Type	Mandatory
`selectedPolicyNameList`	List of name of exceptions to export. By default all the exceptions are exported.	StringList	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
byteStream	Byte stream of the exported file	String

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/exceptions/export

Payload

```
{ “selectedPolicyNameList”:[“test1”,“test2”, “test3”] }
```

Response

```
{ "byteSream": “<?xml version='1.0' encoding='ISO-8859-1'?> <AFConfig> <AlertFilterExport
EMSVersion="8.1.3.1.22"> <AlertFilter name="test1" visibleToChild="yes" addressType="0"> <AlertExclusion
srcMode="2" dstMode="3" srcAddr="null" srcMask="null" destAddr="null" destMask="null" srcPortType="0"
srcPort="null" destPortType="0" destPort="null"/> <AlertExclusion srcMode="1" dstMode="1" srcAddr="null"
srcMask="null" destAddr="null" destMask="null" srcPortType="0" srcPort="null" destPortType="0" destPort="null"/>
</AlertFilter> <AlertFilter name="test2" visibleToChild="yes" addressType="0"> <AlertExclusion srcMode="1"
dstMode="1" srcAddr="null" srcMask="null" destAddr="null" destMask="null" srcPortType="0" srcPort="null"
destPortType="0" destPort="null"/> </AlertFilter> <AlertFilter name="test3" visibleToChild="yes"
addressType="0"> <AlertExclusion srcMode="1" dstMode="1" srcAddr="null" srcMask="null" destAddr="null"
destMask="null" srcPortType="0" srcPort="null" destPortType="0" destPort="null"/> </AlertFilter> </
AlertFilterExport> </AFConfig>” }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	5305	The policy given is not present: <policyname>

Get TCP Settings Configuration at Sensor Level

This URL gets the TCP settings on the Sensor.

Resource URL

GET /sensor/<sensor_id>/tcpsettings

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`TCPSettings`	The TCP settings on the Sensor	Object

Details of fields in TCPSettings:

Field Name	Description	Data Type
`tcpParameter`	The parameters of TCP settings	Object

Details of fields in tcpParameter:

Field Name	Description	Data Type
`supportedUDPFlows`	The supported UDP flows	Number
`tcbInactivityTimesInMinutes`	The TCP inactivity timer (minutes)	Number
`tcpSegmentTimerInSeconds`	The TCP segment timer (seconds)	Number
`tcp2MSLTimerInSeconds`	The TCP 2MSL timer (seconds)	Number
`coldStartTimeInMinutes`	The cold start time (minutes)	Number
`coldStartAckScanAlertDiscardIntervalInMinutes`	The cold start ack scan alert discard interval(minutes)	Number
`coldStartDropAction`	The cold start drop action. The value can be: • DROP_FLOWS • FORWARD_FLOWS	String
`tcpFlowViolation`	The TCP flow violation. The value can be: • PERMIT • DENY	String

Field Name	Description	Data Type
	• PERMIT_OUT_OF_ORDER • DENY_NO_TCB • STATELESS_INSPECTION	
`unsolicitedUDPPacketTimeOutInSeconds`	The unsolicited UDP packets timeout (seconds)	Number
`Normalization`	The normalization. The value can be: • ON • OFF	String
`tcpOverlapOption`	The TCP overlap option. The value can be: • OLD_DATA • NEW_DATA	String
`synCookie`	The SYN cookie data	Object
`resetUnfinished3WayHandshakeConnection`	The reset unfinished 3 way handshake connection. The value can be: • DISABLED • SET_FOR_ALL_TRAFFIC • SET_FOR_DOS_ATTACK_TRAFFIC_ONLY	String
`dnsSinkholingTimeToLive`	DNS sinkholing time to live	Number
`dnsSinkholingIPAddress`	DNS sinkholing IP address	String

Details of fields in synCookie:

Field Name	Description	Data Type
`synCookieOption`	The SYN cookie option. The value can be: • DISABLED • INBOUND_ONLY • OUTBOUND_ONLY • BOTH_INBOUND_AND_OUTBOUND	String
`inboundThresholdValue`	The inbound threshold value	Number
`outboundThresholdValue`	The outbound threshold value	Number

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1002/tcpsettings

Response

```
{ "tcpParameter": { "supportedUDPFlows": 100, "tcbInactivityTimesInMinutes": 10, "tcpSegmentTimerInSeconds": 10,
"tcp2MSLTimerInSeconds": 10, "coldStartTimeInMinutes": 0, "coldStartAckScanAlertDiscardIntervalInMinutes": 0,
"coldStartDropAction": "FORWARD_FLOWS", "tcpFlowViolation": "PERMIT_OUT_OF_ORDER",
"unsolicitedUDPPacketTimeOutInSeconds": 10, "normalization": "OFF", "tcpOverlapOption": "NEW_DATA", "synCookie":
{ "synCookieOption": "INBOUND_ONLY", "inboundThresholdValue": 14112, "outboundThresholdValue": 10000 },
"dnsSinkholingTimeToLive": 720, "dnsSinkholingIPAddress": "1.1.1.1" "resetUnfinished3WayHandshakeConnection":
"SET_FOR_DOS_ATTACK_TRAFFIC_ONLY" } }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor

Update the TCP Settings on Sensor

This URL updates the TCP settings on the Sensor.

Resource URL

PUT /sensor/<sensor_id>/tcpsettings

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`TCPSettings`	The TCP settings on the Sensor	Object	Yes

Details of fields in TCPSettings:

Field Name	Description	Data Type	Mandatory
`tcpParameter`	The parameters of TCP settings	Object	No

Details of fields in tcpParameter:

Field Name	Description	Data Type	Mandatory
`supportedUDPFlows`	The supported UDP flows	Number	No
`tcbInactivityTimesInMinutes`	The TCP inactivity timer(minutes)	Number	No
`tcpSegmentTimerInSeconds`	The TCP segment timer(seconds)	Number	No
`tcp2MSLTimerInSeconds`	The TCP 2MSL timer (seconds)	Number	No
`coldStartTimeInMinutes`	The cold start time (minutes)	Number	No
`coldStartAckScanAlertDiscardIntervalInMinutes`	The cold start ack scan alert discard Interval (minutes)	Number	No
`coldStartDropAction`	The cold start drop action. The value can be:	String	No

Field Name	Description	Data Type	Mandatory
	• DROP_FLOWS • FORWARD_FLOWS		
tcpFlowViolation	The TCP flow violation. The value can be: • PERMIT • DENY • PERMIT_OUT_OF_ORDER • DENY_NO_TCB • STATELESS_INSPECTION	String	No
unsolicitedUDPPacketTimeOutInSeconds	The unsolicited UDP packets timeout (seconds)	Number	No
Normalization	The normalization. The value can be: • ON • OFF	String	No
tcpOverlapOption	The TCP overlap option. The value can be: • OLD_DATA • NEW_DATA	String	No
synCookie	The SYN cookie data	Object	No
resetUnfinished3WayHandshakeConnection	The reset unfinished 3 way handshake connection. The value can be: • DISABLED • SET_FOR_ALL_TRAFFIC • SET_FOR_DOS_ATTACK_TRAFFIC_ONLY	String	No
dnsSinkholingTimeToLive	DNS sinkholing time to live	Number	No
dnsSinkholingIPAddress	DNS sinkholing IP address	String	No

Details of fields in synCookie:

Field Name	Description	Data Type	Mandatory
synCookieOption	The SYN cookie option. The value can be: • DISABLED • INBOUND_ONLY • OUTBOUND_ONLY • BOTH_INBOUND_AND_OUTBOUND	String	Yes
inboundThresholdValue	The inbound threshold value	Number	No
outboundThresholdValue	The outbound threshold value	Number	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1002/tcpsettings

Payload

```
{ "tcpParameter": { "supportedUDPFlows": 100, "tcbInactivityTimesInMinutes": 10, "tcpSegmentTimerInSeconds": 10,
"tcp2MSLTimerInSeconds": 10, "coldStartTimeInMinutes": 0, "coldStartAckScanAlertDiscardIntervalInMinutes": 0,
"coldStartDropAction": "FORWARD_FLOWS", "tcpFlowViolation": "PERMIT_OUT_OF_ORDER",
"unsolicitedUDPPacketTimeOutInSeconds": 10, "normalization": "OFF", "tcpOverlapOption": "NEW_DATA", "synCookie":
{ "synCookieOption": "INBOUND_ONLY", "inboundThresholdValue": 14112, "outboundThresholdValue": 10000 },
"dnsSinkholingTimeToLive": 720, "dnsSinkholingIPAddress": "1.1.1.1" "resetUnfinished3WayHandshakeConnection":
"SET_FOR_DOS_ATTACK_TRAFFIC_ONLY" } }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1124	The Sensor is inactive
3	400	5501	Supported UDP flows should be between <value>
4	400	5502	TCB inactivity time should be between 10 and 1200
5	400	5503	TCP segment timer should be between 10 and 120
6	400	5504	TCP 2MSL should be between 3 and 120 and the value should be 3 sec more than the correlation time for signatures. Correlation time is <value>
7	400	5505	Cold start time should be between 0 and 10080
8	400	5506	Cold start ack scan alert discard interval should be between 0 and 1440
9	400	5507	Unsolicited UDP packet timeout should be between 10 and 3600

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
10	400	5508	Disable SYN cookie first before setting TCP flow violation to stateless inspection
11	400	5509	SYN cookie must be set to DISABLED when TCP flow violation is stateless inspection
12	400	5510	Cannot update SYN cookie when TCP flow violation is set to stateless inspection
13	400	5515	Syncookie threshold value should be between 0 and <value>
14	400	5516	Syncookie threshold value is mandatory

Update IP Settings Configuration at Sensor Level

This URL updates IP settings configuration at Sensor level.

Resource URL

PUT /sensor/<sensor_id>/ipsettings

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`IPSettings`	The IP settings on the Sensor	Object	Yes

Details of fields in IPSettings:

Field Name	Description	Data Type	Mandatory
`ipv4Parameter`	The ipv4 parameter settings for IP settings	Object	No
`ipv6Parameter`	The ipv6 parameter settings for IP settings	Object	No
`jumboFrameParsing`	The jumbo frame parsing settings for IP settings. The value can be: • ENABLED • DISABLED	String	No

Details of fields in ipv4Parameter:

Field Name	Description	Data Type	Mandatory
`fragmentTimer`	The fragment timer (seconds)	Number	No
`overlapOption`	The overlap option. The value can be: • OLD_DATA • NEW_DATA	String	No
`smallestFragmentSize`	The smallest fragment size	Number	No
`smallFragmentThreshold`	The small fragment threshold	Number	No

Field Name	Description	Data Type	Mandatory
`fragmentReassembly`	The fragment reassembly. The value can be: • ENABLED • DISABLED	String	No

Details of fields in ipv6Parameter:

Field Name	Description	Data Type	Mandatory
`ipv6Scanning`	The IPv6 scanning data. The value can be: • SCAN_IPV_6_TRAFFIC_FOR_ATTACKS • DROP_ALL_IPV_6_TARFFIC_INLINE_ONLY • PASS_IPV_6_TRAFFIC_WITHOUT_SCANNING	String	No
`overlapOption`	The overlap option. The value can be: • OLD_DATA • NEW_DATA • DROP	String	No
`smallestFragmentSize`	The smallest fragment size	Number	No
`smallFragmentThreshold`	The small fragment threshold	Number	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1002/ipsettings

Payload

```
{ "ipv4Parameter": { "fragmentTimer": 180, "overlapOption": "OLD_DATA", "smallestFragmentSize": 1480,
"smallFragmentThreshold": 100000, "fragmentReassembly": "DISABLED" }, "ipv6Parameter": { "ipv6Scanning":
"SCAN_IPV_6_TRAFFIC_FOR_ATTACKS", "overlapOption": "OLD_DATA", "smallestFragmentSize": 1280,
"smallFragmentThreshold": 100000 }, "jumboFrameParsing": null }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
2	400	5511	Fragment timer should be between 30 and 180
3	400	5512	Smallest fragment size for IPV4 should be between 8 and 1480 and should be a multiple of 8
4	400	5513	Small fragment threshold should be between 100 and 100000
5	400	5514	Smallest fragment size for IPV6 should be between 40 and 1280 and a multiple of 8
6	500	1001	NE disconnected

Get IP Settings Configuration at Sensor Level

This URL gets IP settings configuration at Sensor level.

Resource URL

GET /sensor/<sensor_id>/ipsettings

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensor_id	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
IPSettings	Object that contains the details of the fields	Object

Details of fields in IPSettings:

Field Name	Description	Data Type
ipv4Parameter	The ipv4 parameter settings for IP settings	Object
ipv6Parameter	The ipv6 parameter settings for IP settings	Object
jumboFrameParsing	The jumbo frame parsing settings for IP settings. The value can be:	String

Field Name	Description	Data Type
	• ENABLED • DISABLED	

Details of fields in ipv4Parameter:

Field Name	Description	Data Type
`fragmentTimer`	The fragment timer (seconds)	Number
`overlapOption`	The overlap option. The value can be: • OLD_DATA • NEW_DATA	String
`smallestFragmentSize`	The smallest fragment size	Number
`smallFragmentThreshold`	The small fragment threshold	Number
`fragmentReassembly`	The fragment reassembly. The value can be: • ENABLED • DISABLED	String

Details of fields in ipv6Parameter:

Field Name	Description	Data Type
`ipv6Scanning`	The IPv6 scanning data. The value can be: • SCAN_IPV_6_TRAFFIC_FOR_ATTACKS • DROP_ALL_IPV_6_TARFFIC_INLINE_ONLY • PASS_IPV_6_TRAFFIC_WITHOUT_SCANNING	String
`overlapOption`	The overlap option. The value can be: • OLD_DATA • NEW_DATA • DROP	String
`smallestFragmentSize`	The smallest fragment size	Number
`smallFragmentThreshold`	The small fragment threshold	Number

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1002/ipsettings

Response

```
{ "ipv4Parameter": { "fragmentTimer": 180, "overlapOption": "OLD_DATA", "smallestFragmentSize": 1480,
"smallFragmentThreshold": 100000, "fragmentReassembly": "DISABLED" }, "ipv6Parameter": { "ipv6Scanning":
"SCAN_IPV_6_TRAFFIC_FOR_ATTACKS", "overlapOption": "OLD_DATA", "smallestFragmentSize": 1280,
"smallFragmentThreshold": 100000 }, "jumboFrameParsing": null }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor

Update the Firewall Logging

This URL updates the firewall logging for the Sensor.

Resource URL

PUT /sensor/<sensor_id>/firewalllogging

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensor_id	Sensor id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
isSuppressionEnabled	To enable the suppression	Boolean	Yes
individualMessage	Individual message	Number	Yes
suppressionInterval	Suppression interval	Number	Yes
uniqueSourceDestinationIPpairs	Unique source destination IP pairs	Number	Yes
loggingType	Logging type can be "DISABLE_DEVICE","LOG_ALL_MATCHED_TRAFFIC","LOG_ALL_DROPPED_DENIED_TRAFFIC","LOG_ALL_PERM	String	Yes
deliveryType	Delivery type can be "MESSAGES_TO_TARGET_SYSLOGSERVER_VIA_MANAGER","MESSAGES_TO_TARGET_SYSLOGSERVER_DIRECT	string	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1001/firewalllogging

Payload

```
{ "loggingType": "LOG_ALL_MATCHED_TRAFFIC", "deliveryType": "MESSAGES_TO_TARGET_SYSLOGSERVER_VIA_MANAGER",
"isSuppressionEnabled": false, "individualMessage": 25, "suppressionInterval": 120,
"uniqueSourceDestinationIPpairs": 10 }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive
3	400	6001	Sending messages directly to syslog server is not supported in I series Sensor
4	400	6002	Suppression interval should be between 1 and 3600
5	400	6003	Individual messages to send before suppressing should be between 1 and 25
6	400	6004	Unique source destination IP pair should be between 1 and 32

Get the Firewall Logging

This URL gets the firewall logging for the Sensor.

Resource URL

GET /sensor/<sensor_id>/firewalllogging

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`isSuppressionEnabled`	To enable the suppression	Boolean
`individualMessage`	Individual message	Number
`suppressionInterval`	Suppression interval	Number
`uniqueSourceDestinationIPpairs`	Unique source destination IP pairs	Number
`loggingType`	Logging type can be "DISABLE_DEVICE","LOG_ALL_MATCHED_TRAFFIC","LOG_ALL_DROPPED_DENIED_TRAFFIC","LOG_	String

Field Name	Description	Data Type
`deliveryType`	Delivery type can be "MESSAGES_TO_TARGET_SYSLOGSERVER_VIA_MANAGER","MESSAGES_TO_TARGET_SYSLOGSERV	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/firewalllogging

Response

```
{ "loggingType": "LOG_ALL_MATCHED_TRAFFIC", "deliveryType": "MESSAGES_TO_TARGET_SYSLOGSERVER_VIA_MANAGER",
"isSuppressionEnabled": false, "individualMessage": 25, "suppressionInterval": 120,
"uniqueSourceDestinationIPpairs": 10 }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor

Get the Alert Suppression

This URL gets the alert suppression for the Sensor.

Resource URL

GET /sensor/<sensor_id>/ipsalerting/alertsuppression

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensor_id	Sensor id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
isEnabled	To enable the alert suppression	Boolean
uniqueSourceDestinationIPpairs	Number of source destination IP pairs	Number
individualAlerts	Number of individual alerts	Number
suppressSeconds	Suppress seconds	Number
alertCorrelation	Alert correlation	Number
packetsLoggedPerFlow	Packets logged per flow	Number
enablePacketLogChannelEncryption	Enable packet log encryption	Boolean

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/ipsalerting/alertsuppression

Response

```
{ "isEnabled": true, "uniqueSourceDestinationIPpairs": 16, "individualAlerts": 2, "suppressSeconds": 2,
"alertCorrelation": 3 "packetsLoggedPerFlow": 6400, "enablePacketLogChannelEncryption": true }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor

Update the Alert Suppression

This URL updates the alert suppression for the Sensor.

Resource URL

PUT /sensor/<sensor_id>/ipsalerting/alertsuppression

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`isEnabled`	To enable the alert suppression	Boolean	Yes
`uniqueSourceDestinationIPpairs`	Source destination IP pairs	Number	Yes
`individualAlerts`	Individual alerts	Number	Yes
`suppressSeconds`	Suppress seconds	Number	Yes
`alertCorrelation`	Alert correlation	Number	Yes
`packetsLoggedPerFlow`	Packets logged	Number	Yes
`enablePacketLogChannelEncryption`	Enable packet	Boolean	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1001/ipsalerting/alertsuppression

Payload

```
{ "isEnabled": true, "uniqueSourceDestinationIPpairs": 16, "individualAlerts": 2, "suppressSeconds": 2,
"alertCorrelation": 3 "packetsLoggedPerFlow": 6400, "enablePacketLogChannelEncryption": true }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
3	400	5701	Unique source destination IP pair should be between 1 and 32
4	400	5702	Individual alerts should be between 1 and 25
5	400	5703	Suppress seconds should be between 1 and 300
6	400	5704	Alert correlation should be between 1 and 10
7	400	5705	TCP 2MSL timer interval should be at least 3 seconds more than the alert correlation time

Add Failover

This URL creates the failover pair.

Resource URL

POST /domain/<domain_id>/failoverpair?SSLOverwrite=<true or false>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Sensor id	Number	Yes
`SSLOverwrite`	True or false, to ignore the SSL key difference with primary & secondary Sensor	Boolean	No

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`failoverPairId`	Unique failover pair id, not required for POST	Number	No
`model`	Sensor model	String	Yes
`name`	Failover pair name	String	Yes
`templateDeviceId`	Template/Primary device id	Number	Yes
`peerDeviceId`	Peer/Secondary device id	Number	Yes
`templateDeviceName`	Template/ Primary device name	String	No
`peerDeviceName`	Peer/ Secondary device name	String	No
`isFailOpen`	Is failopen	Boolean	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique id of the created failover pair	Number

Example

Request

PUT https://<NSM_IP>/domain/0/failoverpair

Payload

```
{ "name": "NS9100_failover", "templateDeviceId": 1004, "peerDeviceId": 1003, "templateDeviceName":
"NS9100_NSM_API_FO_2", "peerDeviceName": "NS9100_NSM_API_FO_1", "isFailOpen": false }
```

Response

```
{ " createdResourceId ": 119 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	404	1105	Invalid domain
3	400	5901	Cluster/Sensor with the same name was defined
4	400	5902	The Sensors have different IPv6 processing options configured
5	400	5903	OOB NAC deployment mode is set on secondary Sensor interfaces
6	400	5904	The Sensors have different FIPS configurations
7	400	5905	The Sensors have different sensor configuration as per license configured
8	400	5906	Either delete the primary's NTBA configuration or set the secondary's NTBA configuration to match the primary's
9	400	5907	Either delete the secondary's NTBA configuration or set the primary's NTBA configuration to match the secondary's
10	400	5908	Both primary and secondary Sensors need to be configured for the same NTBA
11	400	5909	Both primary and secondary Sensor id are same
12	400	5910	Both primary and secondary Sensor model is different
13	400	5911	Both primary and secondary Sensor version is different
14	400	5913	Cluster name is required
15	400	5914	Cluster name should not be greater than 65 chars

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
16	400	5915	Name must contain only letters, numerals, hyphens or underscores
17	400	5916	Primary and secondary Sensors have different SSL private/public keys

Get the Failover Pair

This URL get the failover pair.

Resource URL

GET /domain/<domain_id>/failoverpair /<failoverpair_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domainId	Domain id	Number	Yes
failoverpair_id	Failover pair id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
failoverPairId	Unique failover pair id, not required for POST	Number
model	Sensor model	String
name	Failover pair name	String
templateDeviceId	Template/Primary device id	Number
peerDeviceId	Peer/Secondary device id	Number
templateDeviceName	Template/ Primary device name	String
peerDeviceName	Peer/ Secondary device name	String
isFailOpen	Is failopen	Boolean

Example

Request

GET https://<NSM_IP>/domain/0/failoverpair/119

Response

```
{ "name": "NS9100_failover", "templateDeviceId": 1004, "peerDeviceId": 1003, "templateDeviceName":
"NS9100_NSM_API_FO_2", "peerDeviceName": "NS9100_NSM_API_FO_1", "isFailOpen": false }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	404	5912	Invalid cluster id/cluster not visible to this domain

Get the Failover Pair List

This URL creates the failover pair list available in the domain.

Resource URL

GET /domain/<domain_id>/failoverpair

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`FailoverPairForDomainResponseList`	List of failover pair defined in the domain	Array

Details of FailoverPairForDomainResponseList:

Field Name	Description	Data Type
`failoverPairId`	Unique failover pair id, not required for POST	Number
`model`	Sensor model	String
`name`	Failover pair name	String
`templateDeviceId`	Template/Primary device id	Number
`peerDeviceId`	Peer/Secondary device id	Number
`templateDeviceName`	Template/Primary device name	String
`peerDeviceName`	Peer/Secondary device name	String
`isFailOpen`	Is failopen	Boolean

Example

Request

GET https://<NSM_IP>/domain/0/failoverpair

Response

```
{ "FailoverPairForDomain" : [{ "failoverPairId" : 119, "name" : "NS9100_failover", "templateDeviceId" : 1004,
"peerDeviceId" : 1003, "templateDeviceName" : "NS9100_NSM_API_FO_2", "peerDeviceName" : "NS9100_NSM_API_FO_1",
"isFailOpen" : false }, { "failoverPairId" : 120, "name" : "M2950_failover", "templateDeviceId" : 1005,
"peerDeviceId" : 1006, "templateDeviceName" : "M2950_NSM_API_FO_2", "peerDeviceName" : "M2950_NSM_API_FO_1",
"isFailOpen" : false } ] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Get Syslog Configuration

This URL gets the syslog configuration for firewall notification.

Resource URL

GET /domain/<domain_id>/notification/firewall/syslog

Request Parameters

URL Request Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes

Response Parameters

Details of SyslogNotification:

Field Name	Description	Data Type	Mandatory
enableSyslog	Enable syslog notification	Boolean	Yes
parentAndChildDomain	Parent and child domain	Boolean	Yes
serverIp	Server IP address	String	Yes
serverPort	Server port	Number	Yes
facilities	Facilities	String	No
severity	Severity	String	No
Message	Message	String	No

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/ notification/firewall/syslog

Response

```
{ [ "enableSyslog": true, "parentAndChildDomain": true, "serverIp": "1.1.1.2", "serverPort": 515, "facilities":
"CLOCK_DAEMON_NOTE_2", "severity": "EMERGENCY_SYSTEM_UNUSABLE", "message": "$IV_ACK_INFORMATION$
$IV_ADMIN_DOMAIN$ $IV_DESCRIPTION$" ] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Create/Update Syslog Configuration

This URL creates/updates the syslog configuration for firewall notification.

Resource URL

GET /domain/<domain_id>/notification/firewall/syslog

Request Parameters

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Int	Yes

Payload Parameter: SyslogNotification

Details of SyslogNotification:

Field Name	Description	Data Type
`enableSyslog`	Enable syslog notification	Boolean
`parentAndChildDomain`	Parent and child domain	Boolean
`serverIp`	Server IP address	String
`serverPort`	Server port	Number
`facilities`	Facilities	String
`severity`	Severity	String
`Message`	Message	String

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/ notification/firewall/syslog

Request Payload

```
{ "enableSyslog": true, "parentAndChildDomain": true, "serverIp": "1.1.1.2", "serverPort": 515, "facilities":
"CLOCK_DAEMON_NOTE_2", "severity”: "EMERGENCY_SYSTEM_UNUSABLE", "message": "$IV_ACK_INFORMATION$
$IV_ADMIN_DOMAIN$ $IV_DESCRIPTION$" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	1725	Invalid facilities
3	400	1726	Invalid severity mapping

Get Syslog Configuration

This URL gets the syslog configuration for faults notification.

Resource URL

GET /domain/<domain_id>/notification/faults/syslog

Request Parameters

URL Request Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Response Parameters

Details of SyslogNotification:

Field Name	Description	Data Type	Mandatory
`enableSyslog`	Enable syslog notification	Boolean	Yes
`parentAndChildDomain`	Parent and child domain	Boolean	Yes
`serverIp`	Server IP address	String	Yes
`serverPort`	Server port	Number	Yes
`facilities`	Facilities	String	No
`severity`	Severity mapping	Object	No
`forwrdResults`	Forward results	String	No
`Message`	Message	String	No

Details of severity mapping:

Field Name	Description	Data Type	Mandatory
`inforamtionTo`	Information mapping	String	No
`warningTo`	Warning mapping	String	No
`errorTo`	Error mapping	String	No
`criticalTo`	Critical mapping	String	No

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/notification/faults/syslog

Response

```
{ [ "enableSyslog": true, "parentAndChildDomain": true, "serverIp": "1.1.1.2", "serverPort": 515, "facilities":
"CLOCK_DAEMON_NOTE_2", "severityMapping": { "informationTo": "EMERGENCY_SYSTEM_UNUSABLE", "errorTo":
"EMERGENCY_SYSTEM_UNUSABLE", "warningTO": "EMERGENCY_SYSTEM_UNUSABLE", "criticalTo":
```

```
"EMERGENCY_SYSTEM_UNUSABLE" }, "forwrdResults": "INFORMATIONAL_AND_ABOVE", "message": "$IV_ACK_INFORMATION$
$IV_ADMIN_DOMAIN$ $IV_DESCRIPTION$" ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Create/Update Syslog Configuration

This URL creates/updates the syslog configuration for faults notification.

Resource URL

PUT /domain/<domain_id>/notification/faults/syslog

Request Parameters

URL Request Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Int	Yes

Payload Parameter

Details of SyslogNotification:

Field Name	Description	Data Type
`enableSyslog`	Enable syslog notification	Boolean
`parentAndChildDomain`	Parent and child domain	Boolean
`serverIp`	Server IP address	String
`serverPort`	Server port	Number
`facilities`	Facilities	String
`severity`	Severity mapping	Object
`forwrdResults`	Forward results	String
`Message`	Message	String

Details of severity mapping:

Field Name	Description	Data Type
`inforamtionTo`	Information mapping	String
`warningTo`	Warning mapping	String
`errorTo`	Error mapping	String

Field Name	Description	Data Type
`criticalTo`	Critical mapping	String

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/notification/faults/syslog

Request Payload

```
{ "enableSyslog": true, "parentAndChildDomain": true, "serverIp": "1.1.1.2", "serverPort": 515, "facilities":
"CLOCK_DAEMON_NOTE_2", "severityMapping": { "informationTo": "EMERGENCY_SYSTEM_UNUSABLE", "errorTo":
"EMERGENCY_SYSTEM_UNUSABLE", "warningTO": "EMERGENCY_SYSTEM_UNUSABLE", "criticalTo":
"EMERGENCY_SYSTEM_UNUSABLE" }, "forwrdResults": "INFORMATIONAL_AND_ABOVE", "message": "$IV_ACK_INFORMATION$
$IV_ADMIN_DOMAIN$ $IV_DESCRIPTION$" }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	1725	Invalid facilities
3	400	1726	Invalid severity mapping
4	400	1727	Invalid forward results

Get Tacacs on Domain

This URL gets the Tacacs configuration.

Resource URL

GET domain/<domain_id>/remoteaccess/tacacs

Request Parameters

URL Request Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
enableTACACS	Enable Tacacs	Boolean
tacacsServerIP1	Tacacs server IP 1	String
tacacsServerIP2	Tacacs server IP 2	String
tacacsServerIP3	Tacacs server IP 3	String
tacacsServerIP4	Tacacs server IP 4	String
enableEncryption	Enable encryption	Boolean
encryptionKey	Encryption key	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/remoteaccess/tacacs

Response

```
{ "enableTACACS":true, "tacacsServerIP1":"1.1.1.1", "tacacsServerIP2":"1.1.1.2", "tacacsServerIP3":"1.1.1.3",
"tacacsServerIP4":"1.1.1.4", "enableEncryption":true, "encryptionKey":"abc" }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain id

Update Tacacs on Domain

This URL updates the tacacs configuration.

Resource URL

PUT domain/<domain_id>/remoteaccess/tacacs

Request Parameters

URL Request Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes

Payload Parameter:

Field Name	Description	Data Type	Mandatory
enableTACACS	Enable Tacacs	Boolean	Yes
tacacsServerIP1	Tacacs server IP 1	String	No
tacacsServerIP2	Tacacs server IP 2	String	No
tacacsServerIP3	Tacacs server IP 3	String	No
tacacsServerIP4	Tacacs server IP 4	String	No
enableEncryption	Enable encryption	Boolean	Yes
encryptionKey	Encryption key	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/remoteaccess/tacacs

```
{ "enableTACACS":true, "tacacsServerIP1":"1.1.1.1", "tacacsServerIP2":"1.1.1.2", "tacacsServerIP3":"1.1.1.3",
"tacacsServerIP4":"1.1.1.4", "enableEncryption":true, "encryptionKey":"abc" }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	404	1105	Invalid domain id
3	400	4713	Invalid IP address

Get Tacacs on Sensor

This URL gets the Tacacs configuration.

Resource URL

GET sensor/<sensor_id>/remoteaccess/tacacs

Request Parameters

URL Request Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`inheritSettings`	Inherit domain level settings	Boolean
`enableTACACS`	Enable Tacacs	Boolean
`tacacsServerIP1`	Tacacs server IP 1	String
`tacacsServerIP2`	Tacacs server IP 2	String
`tacacsServerIP3`	Tacacs server IP 3	String
`tacacsServerIP4`	Tacacs server IP 4	String
`enableEncryption`	Enable encryption	Boolean
`encryptionKey`	Encryption key	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/remoteaccess/tacacs

Response

```
{ “inheritSettings”:false, "enableTACACS":true, "tacacsServerIP1":"1.1.1.1", "tacacsServerIP2":"1.1.1.2",
"tacacsServerIP3":"1.1.1.3", "tacacsServerIP4":"1.1.1.4", "enableEncryption":true, "encryptionKey":"abc" }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1125	The Sensor is inactive

Update Tacacs on Sensor

This URL updates the Tacacs configuration.

Resource URL

PUT sensor/<sensor_id>/remoteaccess/tacacs

Request Parameters

URL Request Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Payload parameters

Field Name	Description	Data Type	Mandatory
`inheritSettings`	Inherit settings from domain	Boolean	Yes
`enableTACACS`	Enable Tacacs	Boolean	Yes
`tacacsServerIP1`	Tacacs server IP 1	String	No
`tacacsServerIP2`	Tacacs server IP 2	String	No
`tacacsServerIP3`	Tacacs server IP 3	String	No
`tacacsServerIP4`	Tacacs server IP 4	String	No
`enableEncryption`	Enable encryption	Boolean	Yes
`encryptionKey`	Encryption key	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/remoteaccess/tacacs

```
{ “inheritSettings”:false, "enableTACACS":true, "tacacsServerIP1":"1.1.1.1", "tacacsServerIP2":"1.1.1.2",
"tacacsServerIP3":"1.1.1.3", "tacacsServerIP4":"1.1.1.4", "enableEncryption":true, "encryptionKey":"abc" }
```

Response

```
{ { "status":1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Invalid error
2	404	1106	Invalid Sensor
3	400	1125	The Sensor is inactive

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
4	400	4713	Invalid IP address

Get the List of Active Botnets

This URL gets the list of active botnets in the domain.

Resource URL

GET /domain/<domain_id>/activebotnets?includeChildDomain=<includeChildDomain>&&duration=<duration>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes
`includeChildDomain`	Should the child domains be included	Boolean	No
`duration`	Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOUR • LAST_12_HOUR • LAST_24_HOUR • LAST_48_HOUR • LAST_7_DAYS • LAST_14_DAYS	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`botnetDetailList`	List of active botnets	ObjectList

Details of fields in botnetDetailList:

Field Name	Description	Data Type
name	Name of the active botnet	String
botId	If of the active botnet	Number
ccCommunication	C&C communication	String
events	Number of events	Number
lastEvent	Last event time	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/activebotnets

Response

```
{ "botnetDetailList": [ { "name": "IRCBots", "botId": 6, "ccCommunication": "UN_BLOCKED", "events": 1,
"lastEvent": "Jan 31 10:04 IST" } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	404	4201	Invalid duration filter

Get the List of Zombies for an Active Botnet

This URL gets the list of zombies for an active botnet.

Resource URL

GET /domain/<domain_id>/activebotnetzombies/<bot_id>?includeChildDomain=<includeChildDomain>&&duration=<duration>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes
includeChildDomain	Should the child domains be included	Boolean	No
duration	Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOUR • LAST_12_HOUR • LAST_24_HOUR • LAST_48_HOUR • LAST_7_DAYS • LAST_14_DAYS	String	No

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`zombiesDetailList`	List of zombies for the botnet	ObjectList

Details of fields in zombiesDetailList:

Field Name	Description	Data Type
`ipAddress`	IP address	String
`dnsName`	DNS name	String

Field Name	Description	Data Type
`ccCommunication`	C&C communication	String
`events`	Number of events	Number
`lastEvent`	Time of last event	String
`comment`	Comment	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/activebotnetzombies/6

Response

```
{ "zombiesDetailList": [ { "ipAddress": "192.168.2.2", "dnsName": "", "ccCommunication": "UN_BLOCKED", "events":
2, "lastEvent": "Jan 31 16:53 IST", "comment": "" } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	404	4201	Invalid duration filter
3	404	4202	Invalid botnet id

Get the Signature Set Automatic Update Configuration

This URL gets the signature set automatic update configuration on the Manager.

Resource URL

GET /autoupdateconfiguration/sigset

Request Parameters

None

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`automaticDownloadDetails`	Contains the details of the automatic download to Manager configuration	Object
`automaticDeploymentDetails`	Contains the details of the automatic deployment to sensor configuration	Object

Details of fields in automaticDownloadDetails:

Field Name	Description	Data Type
`enableDownload`	Whether the automatic download is enabled	Boolean
`schedule`	Schedule for the update. Values can be following: • FREQUENTLY • DAILY • WEEKLY	String
`startTime`	Time when the update should start. Should be in hh:mm format.	String
`endTime`	Time when the update should start. Should be in hh:mm format.	String
`recur`	The recurring duration	String

Details of fields in automaticDeploymentDetails:

Field Name	Description	Data Type
`enableDeployInRealTime`	Whether the automatic deployment in real time is enabled	Boolean
`enableDeployAtScheduledInterval`	Whether the automatic deployment in scheduled time is enabled	Boolean

Field Name	Description	Data Type
`schedule`	Schedule for the update. Values can be following: • FREQUENTLY • DAILY • WEEKLY	String
`startTime`	Time when the update should start. Should be in hh:mm format.	String
`endTime`	Time when the update should start. Should be in hh:mm format.	String
`recur`	The recurring duration	String

Example

Request

GET https://<NSM_IP>/sdkapi/ autoupdateconfiguration/sigset

Response

```
{ "automaticDownloadDetails": { "enableDownload": true, "schedule": "FREQUENTLY", "startTime": "0:0", "endTime":
"23:0", "recur": "10 Hr" }, "automaticDeploymentDetails": { "enableDeployInRealTime": true,
"enableDeployAtScheduledInterval": true, "schedule": "FREQUENTLY", "startTime": "7:50", "endTime": "23:0",
"recur": "10 Min" } }
```

Error Information

None

Get the Botnet Automatic Update Configuration

This URL gets the botnet automatic update configuration on the Manager.

Resource URL

GET /autoupdateconfiguration/botnet

Request Parameters

None

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`automaticDownloadDetails`	Contains the details of the automatic download to Manager configuration	Object
`automaticDeploymentDetails`	Contains the details of the automatic deployment to Sensor configuration	Object

Details of fields in automaticDownloadDetails:

Field Name	Description	Data Type
`enableDownload`	Whether the automatic download is enabled	Boolean

Field Name	Description	Data Type
`schedule`	Schedule for the update. Values can be following: • FREQUENTLY • DAILY • WEEKLY	String
`startTime`	Time when the update should start. Should be in hh:mm format.	String
`endTime`	Time when the update should start. Should be in hh:mm format.	String
`recur`	The recurring duration	String

Details of fields in automaticDeploymentDetails:

Field Name	Description	Data Type
`enableDeployInRealTime`	Whether the automatic deployment in real time is enabled	Boolean
`enableDeployAtScheduledInterval`	Whether the automatic deployment in scheduled time is enabled	Boolean
`schedule`	Schedule for the update. Values can be following: • FREQUENTLY • DAILY • WEEKLY	String
`startTime`	Time when the update should start. Should be in hh:mm format.	String
`endTime`	Time when the update should start. Should be in hh:mm format.	String
`recur`	The recurring duration	String

Example

Request

GET https://<NSM_IP>/sdkapi/ autoupdateconfiguration/botnet

Response

```
{ "automaticDownloadDetails": { "enableDownload": true, "schedule": "FREQUENTLY", "startTime": "0:0", "endTime":
"23:0", "recur": "10 Hr" }, "automaticDeploymentDetails": { "enableDeployInRealTime": true,
"enableDeployAtScheduledInterval": true, "schedule": "FREQUENTLY", "startTime": "7:50", "endTime": "23:0",
"recur": "10 Min" } }
```

Error Information

None

Update the Signature Set Automatic Download Configuration

This URL updates the signature set automatic download configuration.

Resource URL

PUT /autoupdateconfiguration/sigsetdownloadconfig

Request Parameters

URL Parameters:

None

Payload Parameters:

Field Name	Description	Data Type
`enableDownload`	Whether the automatic download is enabled	Boolean
`schedule`	Schedule for the update. Values can be following: • FREQUENTLY • DAILY • WEEKLY	String
`startTime`	Time when the update should start. Should be in hh:mm format.	String
`endTime`	Time when the update should start. Should be in hh:mm format.	String
`recur`	The recurring duration	String

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/autoupdateconfiguration/sigsetdownloadconfig

Payload

```
{ "enableDownload": true, "schedule": "FREQUENTLY", "startTime": "0:0", "endTime": "23:0", "recur": "10 Hr" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	6101	Invalid time format... Time is mandatory and should be in hh:mm format
2	400	6102	Hour should be between 0 and 23

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
3	400	6103	Minute should be between 0 and 55 and multiples of 5
4	400	6104	For frequently: duration should end with Min or Hr... If hr then 1 to 10 and 12 is allowed... If min then 10 15 30 & 45 are allowed...
5	400	6105	For weekly: duration should be name of the days like SUNDAY,MONDAY,etc.
6	400	6106	Schedule should be one of the following: FREQUENTLY, DAILY & WEEKLY
7	400	6107	Recur value is mandatory when schedule is FREQUENTLY or WEEKLY
8	400	6108	Update to Sensor failed

Update the Botnet Automatic Download Configuration

This URL updates the botnet automatic download configuration.

Resource URL

PUT /autoupdateconfiguration/botnetdownloadconfig

Request Parameters

URL Parameters:

None

Payload Parameters:

Field Name	Description	Data Type
`enableDownload`	Whether the automatic download is enabled	Boolean
`schedule`	Schedule for the update. Values can be following: • FREQUENTLY • DAILY • WEEKLY	String
`startTime`	Time when the update should start. Should be in hh:mm format.	String
`endTime`	Time when the update should start. Should be in hh:mm format.	String

Field Name	Description	Data Type
`recur`	The recurring duration	String

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/autoupdateconfiguration/botnetdownloadconfig

Payload

```
{ "enableDownload": true, "schedule": "FREQUENTLY", "startTime": "0:0", "endTime": "23:0", "recur": "10 Hr" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	6101	Invalid time format... Time is mandatory and should be in hh:mm format
2	400	6102	Hour should be between 0 and 23
3	400	6103	Minute should be between 0 and 55 and multiples of 5
4	400	6104	For frequently: duration should end with Min or Hr... If hr then 1 to 10 and 12 is allowed... If min then 10 15 30 & 45 are allowed...
5	400	6105	For weekly: duration should be name of the days like SUNDAY,MONDAY,etc.
6	400	6106	Schedule should be one of the following: FREQUENTLY, DAILY & WEEKLY
7	400	6107	Recur value is mandatory when schedule is FREQUENTLY or WEEKLY
8	400	6108	Update to Sensor failed

Update the Signature Set Automatic Deployment Configuration

This URL updates the signature set automatic deployment configuration.

Resource URL

PUT /autoupdateconfiguration/sigsetdeploymentconfig

Request Parameters

URL Parameters:

None

Payload Parameters:

Field Name	Description	Data Type
`enableDeployInRealTime`	Whether the automatic deployment in real time is enabled	Boolean
`enableDeployAtScheduledInterval`	Whether the automatic deployment in scheduled time is enabled	Boolean
`schedule`	Schedule for the update. Values can be following: • FREQUENTLY • DAILY • WEEKLY	string
`startTime`	Time when the update should start. Should be in hh:mm format.	String
`endTime`	Time when the update should start. Should be in hh:mm format.	String
`recur`	The recurring duration	String

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/autoupdateconfiguration/sigsetdeploymentconfig

Payload

```
{ "enableDeployInRealTime": true, "enableDeployAtScheduledInterval": true, "schedule": "FREQUENTLY",
"startTime": "7:50", "endTime": "23:0", "recur": "10 Min" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	6101	Invalid time format... Time is mandatory and should be in hh:mm format
2	400	6102	Hour should be between 0 and 23
3	400	6103	Minute should be between 0 and 55 and multiples of 5
4	400	6104	For frequently: duration should end with Min or Hr... If hr then 1 to 10 and 12 is allowed... If min then 10 15 30 & 45 are allowed...
5	400	6105	For weekly: duration should be name of the days like SUNDAY,MONDAY,etc.
6	400	6106	Schedule should be one of the following: FREQUENTLY, DAILY & WEEKLY
7	400	6107	Recur value is mandatory when schedule is FREQUENTLY or WEEKLY
8	400	6108	Update to Sensor failed

Update the Botnet Automatic Deployment Configuration

This URL updates the botnet automatic deployment configuration.

Resource URL

PUT /autoupdateconfiguration/botnetdeploymentconfig

Request Parameters

URL Parameters:

None

Payload Parameters:

Field Name	Description	Data Type
`enableDeployInRealTime`	Whether the automatic deployment in real time is enabled	Boolean
`enableDeployAtScheduledInterval`	Whether the automatic deployment in scheduled time is enabled	Boolean

Field Name	Description	Data Type
`schedule`	Schedule for the update. Values can be following: • FREQUENTLY • DAILY • WEEKLY	String
`startTime`	Time when the update should start. Should be in hh:mm format.	String
`endTime`	Time when the update should start. Should be in hh:mm format.	String
`recur`	The recurring duration	String

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/autoupdateconfiguration/botnetdeploymentconfig

Payload

```
{ "enableDeployInRealTime": true, "enableDeployAtScheduledInterval": true, "schedule": "FREQUENTLY",
"startTime": "7:50", "endTime": "23:0", "recur": "10 Min" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	6101	Invalid time format... Time is mandatory and should be in hh:mm format
2	400	6102	Hour should be between 0 and 23
3	400	6103	Minute should be between 0 and 55 and multiples of 5
4	400	6104	For frequently: duration should end with Min or Hr... If hr then 1 to 10 and 12 is allowed... If min then 10 15 30 & 45 are allowed...

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
5	400	6105	For weekly: duration should be name of the days like SUNDAY,MONDAY,etc.
6	400	6106	Schedule should be one of the following: FREQUENTLY, DAILY & WEEKLY
7	400	6107	Recur value is mandatory when schedule is FREQUENTLY or WEEKLY
8	400	6108	Update to Sensor failed

Get Malware Downloads

This URL gets the list malware downloads from the Manager.

Resource URL

GET /domain/<domain_id>/malwaredownloads?duration=<duration>&resultType=<resultType>&confidenceType=<confidenceType>&includeChildDomain=<includeChildDomain>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain`	Domain id	Number	Yes
`duration`	Duration can be • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	No
`resultType`	Result type can be • ANY_RESULT • BLOCKED • UNBLOCKED	String	No
`confidenceType`	Confidence type can be • ANY_MALWARE_CONFIDENCE • VERY_HIGH_MALWARE_CONFIDENCE • HIGH_MALWARE_CONFIDENCE • LOW_MALWARE_CONFIDENCE • MEDIUM_MALWARE_CONFIDENCE • VERY_LOW_MALWARE_CONFIDENCE	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`MalwareSummaryDetailList`	List of malware summary detail defined in the domain	Array

Details of object in MalwareSummaryDetailList:

Field Name	Description	Data Type
`filehash`	File hash	String
`overAllConfidence`	Over all confidence can be: "VERY_LOW"/"LOW"/"MEDIUM"/ "HIGH"/"VERY_HIGH"/"UNKNOW"	Boolean
`individualEngineConfidence`	Individual engine confidence	Object
`lastDownload`	Last download time	String
`totalDownloads`	Total downloads	Number
`fileSize`	File size	String
`lastFileName`	Last file name	String
`lastResult`	Last result	String
`comment`	Comment	String

Details of object in individualEngineConfidence:

Field Name	Description	Data Type
`CustomFingerPrints`	Custom finger prints can be: "VERY_LOW"/"LOW"/"MEDIUM"/ "HIGH"/"VERY_HIGH"/"UNKNOW"	String
`GTIFileReputation`	GTI file reputation can be: "VERY_LOW"/"LOW"/"MEDIUM"/ "HIGH"/"VERY_HIGH"/"UNKNOW"	String
`PDFEmulation`	PDF emulation can be: "VERY_LOW"/"LOW"/"MEDIUM"/ "HIGH"/"VERY_HIGH"/"UNKNOW"	String
`GatewayAntiMalware`	Gateway Anti-Malware can be: "VERY_LOW"/"LOW"/"MEDIUM"/ "HIGH"/"VERY_HIGH"/"UNKNOW"	String

Example

Request

GET https://<NSM_IP>/domain/0/malwaredownloads

Response

```
{ "malwareSummaryDetailList": [ { "filehash": "493d146a59a155ed2eb890f5fd3bb182", "overAllConfidence": "LOW",
"individualEngineConfidence": { "CustomFingerPrints": "UNKNOWN", "GTIFileReputation": "VERY_LOW",
"PDFEmulation": "UNKNOWN", "GatewayAntiMalware": "LOW" }, "lastDownload": "Mon Mar 10 17:37:49 IST 2014",
"totalDownloads": 2, "fileSize": "1024" } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	404	1105	Invalid domain
3	400	3801	Invalid result filter value
4	400	3802	Invalid duration filter value

Get Malware Alerts

This URL get the list malware alerts for the malware file hash.

Resource URL

GET /domain/<domain_id>/malwaredownloads/ filehash/<filehash>?duration=<duration>&resultType=<resultType>&confidenceType=<confidenceType>&includeChildDomain=<includeChildDomain>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain`	Domain id	Number	Yes
`duration`	Duration can be • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	No
`resultType`	Result type can be • ANY_RESULT • BLOCKED • UNBLOCKED	String	No
`confidenceType`	Confidence type can be • ANY_MALWARE_CONFIDENCE • VERY_HIGH_MALWARE_CONFIDENCE • HIGH_MALWARE_CONFIDENCE • LOW_MALWARE_CONFIDENCE • MEDIUM_MALWARE_CONFIDENCE	String	No

Field Name	Description	Data Type	Mandatory
	- VERY_LOW_MALWARE_CONFIDENCE		

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
malwareAlertDetailsList	List of malware alert detail defined in the domain	Array

Details of object in MalwareAlertDetail:

Field Name	Description	Data Type
time	Time stamp	String
attacker	IP details	Object
target	IP details	Object
result	Result	String
protocol	Protocol	String
confidence	Confidence can be: "VERY_LOW"/"LOW"/"MEDIUM"/ "HIGH"/"VERY_HIGH"/"UNKNOW"	String
fileName	File name	String
engine	Engine	String
attackDescription	Attack description	Object

Details of object in attacker/target:

Field Name	Description	Data Type
ipAddress	IP address	String
country	Country	String

Details of object in attackDescription:

Field Name	Description	Data Type
attackName	Attack name	String
result	Result can be: "ATTACK_SUCCESSFUL"/"INCONCLUSIVE"/" ATTACK_FAILED"/"ATTACK_BLOCKED"/" NOT_APPLICABLE"/" DOS_BLOCKING_ACTIVATED"/" BLOCKING_SIMULATED_ATTACK_SUCCESSFUL"/	String

Field Name	Description	Data Type
	"BLOCKING_SIMULATED_INCONCLUSIVE"/" BLOCKING_SIMULATED_ATTACK_FAILED"/" BLOCKING_SIMULATED_NOT_APPLICABLE"	
`direction`	Direction can be: "INBOUND"/" OUTBOUND"/" UNKNOWN"/" BOTH"	

Example

Request

GET https://<NSM_IP>/domain/0/malwaredownloads/filehash/493d146a59a155ed2eb890f5fd3bb182

Response

```
" { "malwareAlertDetailsList": [ { "time": "Mar 11 13:09 IST", "attacker": { "ipAddress": "1.1.1.9", "country":
"---" }, "target": { "ipAddress": "1.1.1.10", "country": "---" }, "result": "Inconclusive", "protocol": "http",
"confidence": "LOW", "engine": "Gateway Anti-Malware", "attackDescription": { "attackName": "MALWARE: Malicious
file detected by Network Threat Behavioural Analysis engine", "result": "INCONCLUSIVE", "direction":
"OUTBOUND" } }, { "time": "Mar 11 13:09 IST", "attacker": { "ipAddress": "1.1.1.9", "country": "---" },
"target": { "ipAddress": "1.1.1.10", "country": "---" }, "result": "Inconclusive", "protocol": "http",
"confidence": "VERY_LOW", "engine": "GTI File Reputation", "attackDescription": { "attackName": "MALWARE:
Malicious File transfer detected by McAfee Global Threat Intelligence Service", "result": "INCONCLUSIVE",
"direction": "OUTBOUND" } } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	404	1105	Invalid domain
3	404	3401	Invalid file hash value
4	400	3801	Invalid result filter value
5	400	3802	Invalid duration filter value

Nessus Scan Report Import

This URL to import the nessus scan report file into Manager.

Resource URL

PUT domain/<domain_id>/integration/vulnerability/importscanreport

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`MultiPart`	Holds the body part objects	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
`BodyPart[0]`	Holds the report detail	Application/json object	Yes

Details of report detail:

Field Name	Description	Data Type
`reportFileName`	File name	String
`reportType`	Report type	String
`description`	Description	String
`enableOnImport`	Enable on import	Boolean

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
`BodyPart[1]`	Holds the .nessus file as input stream	Application/octet-stream	Yes

Details of .nessus file:

Field Name	Description	Data Type	Mandatory
`File`	Nessus scan report file	ByteArrayInput stream	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Operation status	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/integration/vulnerability/importscanreport

```
----Boundary_1_12424925_1353496814940 Content-Type: application/json { "reportFileName": "Test1.nessus",
"reportType": "NESSUS", "description": "test import", "enableOnImport": true } ----
Boundary_1_12424925_1353496814940 Content-Type: application/octet-stream ÒrÝ?ü0¥ÿ<^}c,¢eXœ^:4 JhÍ2µ□rDYñÇÚd¶/
Â¿í□F~ ÆÏc§¼éá©ÿ_8Öø« C6Ô654îÞg'J6?x ,*T2¡qhã4ÎÅVµGƒo9ŸCÒª„í¹Ì —Áë&1¹ì,Ú‹y ì^î'Vö5U ----
Boundary_1_12424925_1353496814940--
```

Response

```
{ " status ": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid domain id
2	400	7001	Invalid scan report file
3	400	2202	No input stream
4	400	7002	Invalid report type
5	400	7000	Failed to import

Get ATD Integration in Domain

This URL gets the ATD integration configuration in a particular domain.

Resource URL

GET domain/<domain_id>/ipsdevices/atdintegration

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
enableCommunication	Enable communication	Boolean
atdUsername	ATD user name	String
atdPassword	ATD password	String
sensorToATDCommunicationPort	Sensor to ATD communication port	Number
managerToATDCommunicationPort	Manager to ATD communication port	Number
atdApplianceIPAddr	ATD appliance IP address	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/ipsdevices/atdintegration

Response

```
{ "enableCommunication":true, "atdUsername":"admin", "sensorToATDCommunicationPort":8505,
"managerToATDCommunicationPort":443, "atdPassword":"admin123", "atdApplianceIPAddr":"1.1.1.1"} }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid domain id

Update ATD Integration Configuration in Domain

This URL updates the ATD integration configuration in a particular domain.

Resource URL

PUT domain/<domain_id>/ipsdevices/atdintegration

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type
`enableCommunication`	Enable communication	Boolean
`atdUsername`	ATD user name	String
`atdPassword`	ATD password	String
`sensorToATDCommunicationPort`	Sensor to ATD communication port	Number
`managerToATDCommunicationPort`	Manager to ATD communication port	Number
`atdApplianceIPAddr`	ATD appliance IP address	String

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Operation status	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/ipsdevices/atdintegration

```
{ "enableCommunication":true, "atdUsername":"admin", "sensorToATDCommunicationPort":8505,
"managerToATDCommunicationPort":443, "atdPassword":"admin123", "atdApplianceIPAddr":"1.1.1.1"} }
```

Response

```
{ " status ": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid domain id

Get ATD Integration in Sensor

This URL gets the ATD integration configuration in a particular Sensor.

Resource URL

GET sensor/<sensor_id>/atdintegration

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`enableCommunication`	Enable communication	Boolean
`inheritSettings`	Inherit settings	String
`atdUsername`	ATD user name	String
`atdPassword`	ATD password	String
`sensorToATDCommunicationPort`	Sensor to ATD communication port	Number
`managerToATDCommunicationPort`	Manager to ATD communication port	Number
`atdApplianceIPAddr`	ATD appliance IP address	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/0/atdintegration

Response

```
{ "enableCommunication":true, “inheritSettings”:”false”, "atdUsername":"admin", "sensorToATDCommunicationPort":
8505, "managerToATDCommunicationPort":443, "atdPassword":"admin123", "atdApplianceIPAddr":"1.1.1.1"} }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1106	Invalid Sensor id

Update ATD Integration Configuration in Sensor

This URL updates the ATD integration configuration in a particular Sensor.

Resource URL

PUT sensor/<sensor_id>/atdintegration

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type
`enableCommunication`	Enable communication	Boolean
`inheritSettings`	Inherit settings	String
`atdUsername`	ATD user name	String
`atdPassword`	ATD password	String
`sensorToATDCommunicationPort`	Sensor to ATD communication port	Number
`managerToATDCommunicationPort`	Manager to ATD communication port	Number
`atdApplianceIPAddr`	ATD appliance IP address	String

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Operation status	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/0/atdintegration

```
{ “inheritSettings”:”false”, "enableCommunication":true, "atdUsername":"admin", "sensorToATDCommunicationPort":
8505, "managerToATDCommunicationPort":443, "atdPassword":"admin123", "atdApplianceIPAddr":"1.1.1.1"} }
```

Response

```
{ " status ": 1 }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1106	Invalid Sensor id

Export the Sensor Configuration

This URL exports the Sensor configuration to an xml file.

Resource URL

PUT /sensor/<sensor_id>/ exportconfiguration

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`SensorConfigExportElement`	The details of what to export from sensor	Object	Yes

Details of SensorConfigExportElement:

Field Name	Description	Data Type	Mandatory
`fileDestination`	Location as to where to store the file	String	Yes
`exportFOConfig`	Export failover configuration	Boolean	No
`exportFirewallConfig`	Export firewall configuration	Boolean	No
`exportSSLConfig`	Export SSL configuration	Boolean	No
`exportExceptionsConfig`	Export exceptions configuration	Boolean	No
`exportNACConfig`	Export exceptions configuration	Boolean	No
`exportMonitoringPortConfig`	Export monitoring ports configuration	Boolean	No
`exportNTBAConfig`	Export NTBA configuration	Boolean	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1002/exportconfiguration

Payload

```
{ "exportFirewallConfig": true, "exportMonitoringPortConfig": true, "exportFOConfig": true, "exportNACConfig":
true, "exportSSLConfig": true, "exportExceptionsConfig": true, "fileDestination": "C:\\sensorconfigexport\
\sensorAPIallTRUE", "exportNTBAConfig": true }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	5308	No destination file specified

Import the Sensor Configuration

This URL imports the Sensor configuration from the XML file and pushes to the Sensor.

Resource URL

PUT /sensor/<sensor_id>/importconfiguration

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensorId	Sensor id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
MultiPart	Holds the body part objects	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the import file element object	Application/json object	Yes

Details of ImportFileElement:

Field Name	Description	Data Type	Mandatory
fileName	Name of the file	String	Yes

Field Name	Description	Data Type	Mandatory
`fileType`	File type should be "XML"	String	Yes

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
`BodyPart[1]`	Holds the file as input stream	Application/octet-stream	Yes

Details of .xml file:

Field Name	Description	Data Type	Mandatory
`File`	Policy(file input stream)	ByteArrayInput stream	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number
`message`	Message returned from the backend	String

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/<sensor_id>/importconfiguration

Payload

```
----Boundary_1_12424925_1353496814940 Content-Type: application/json {"fileType": "xml", "fileName":
"sensor1002API"} ----Boundary_1_12424925_1353496814940 Content-Type: application/octet-stream <Sensor
swVersion="8.0.2.2"> <PhysicalConfig originalSensorName="M-2950" failoverMode="standalone"> <sensor
description="MCAFEE-NETWORK-SECURITY-PLATFORM" model="M-2950" slotCount="2" //…… …… …..// <NI id="NI162"
interfaceid="Interface132" adid="/Test Child Domain 1.1" vidsid="Vids148" name="Def NI of Interface 4A-4B on
mfa/sensor 1002" nipolicytype="D" nilinktype="D"/> </NIs> </VidsConfig> <NonStandardPorts/> <BotConfigs>
<botconfig status="disable" vidsId="Vids143"> <zeroday inherit="true" scorethreshold="0"/> </botconfig> </
BotConfigs> <L7FieldConfigs/> </Sensor> ----Boundary_1_12424925_1353496814940--
```

Response

```
{ "status": 1, "message": "IN PROGRESS:Queued: Generation of Signature file Segment for Sensor: M-2950 IN
PROGRESS:Generating Signature Segments for Sensor: M-2950. Sig Version: 8.6.25.6 IN PROGRESS:Generating Response
Segments for Sensor: M-2950 IN PROGRESS:Beginning Signature download to the sensor: M-2950 IN
PROGRESS:Transferred files successfully applied for... DOWNLOAD COMPLETE " }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	5301	Invalid file type given for import
3	400	1124	The Sensor is inactive
4	500	2202	Input stream read error

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
5	500	500	Fail over Sensor required for importing this file
6	500	500	Standalone Sensor required for importing this file
7	500	500	IPv6 configuration mismatch. Correct this and try again.
8	500	500	Sensor model is different. Correct this and try again.
9	500	500	Invalid import file. Correct this and try again.
10	500	500	Physical configuration is different. Correct this and try again.
11	400	1140	Sensor is currently running in layer 2 bypass mode
12	400	1141	Concurrent process are running on the update server
13	400	1142	Please wait a minute and then try again, check the system log for details
14	400	1144	Sensor is not a standalone device. Signature set download cannot be done on a failover device
15	400	1147	Total exception objects count exceeded the limit of
16	400	1148	Sensor software version is not compatible with the Manager

Get the DoS Profiles on the manager for Sensors

This URL retrieves the DoS profiles on the Manager for Sensors.

Resource URL

GET /sensor/<sensor_id>/dosprofilesonmanager

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensorId	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
DosProfilesOnManager	The DoS profiles on the Manager for Sensors	Object

Details of DosProfilesOnManager:

Field Name	Description	Data Type
dosProfiles	List of DoS profiles	StringList

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1002/dosprofilesonmanager

Response

```
{ "dosProfiles": [ "profile_Thu_Apr_24_17_50_16_IST_2014.dat.gz",
"profile_Thu_Apr_24_17_50_35_IST_2014.dat.gz" ] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor

Update the DoS Learning Mode on the Sensor

This URL updates the DoS learning mode on the Sensor.

Resource URL

PUT /sensor/<sensor_id>/ dosprofilelearningmode

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`DosProfilesLearning`	Learning mode	Object	Yes

Details of DosProfilesLearning:

Field Name	Description	Data Type	Mandatory
`dosProfileLearning`	Mode of learning. Can be one of the following: • LEARNING_MODE • DETECTION_MODE	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1002/dosprofilelearningmode

Payload

```
{ "dosProfileLearning" : "LEARNING_MODE" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1124	The Sensor is inactive

Get the DoS Packet Forwarding

This URL retrieves the DoS packet forwarding for the Sensor.

Resource URL

GET /sensor/<sensor_id>/ dospacketforwarding

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensorId	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
DosProfilesOnManager	The DoS profiles on the Manager for the Sensor	Object

Details of DosProfilesOnManager:

Field Name	Description	Data Type
dosPacketForwarding	DoS packet forwarding configuration	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1002/dospacketforwarding

Response

```
{ "dosPacketForwarding": "Do Not Copy DoS Packets (Dos Packet Logging is disabled)" }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor

Upload the DoS Profile from the Sensor

This URL uploads the DoS profile from the Sensor.

Resource URL

PUT /sensor/<sensor_id>/uploaddosprofile

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensorId	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number
`message`	Returns the status messages	String

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1002/uploaddosprofile

Response

```
{ "status": 1, "message": "Upload Complete for Dos (from sensor to manager)" }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1124	The Sensor is inactive

Restore the DoS Profile to the Sensor

This URL restores the DoS profile to the Sensor.

Resource URL

PUT /sensor/<sensor_id>/restoredosprofile

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`DosProfileRestoreName`	DoS profile	Object	Yes

Details of DosProfileRestoreName:

Field Name	Description	Data Type	Mandatory
`dosProfileName`	DoS profile name	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Set to 1 if the operation was successful	Number
message	Returns the status messages	String

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1002/retoredosprofile

Payload

```
{ "dosProfileName" : "profile_Thu_Apr_24_17_50_16_IST_2014.dat.gz" }
```

Response

```
{ "status": 1, "message": "Download Complete for Dos (from manager to sensor)" }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1124	The Sensor is inactive
3	400	5601	The profile name does not exist for the Sensor

Delete the DoS Profile

This URL deletes the DoS profile.

Resource URL

DELETE /sensor/<sensor_id>/deletedosprofile

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensorId	Sensor id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
DosProfileRestoreName	DoS profile	Object	Yes

Details of DosProfileRestoreName:

Field Name	Description	Data Type	Mandatory
dosProfileName	DoS profile name	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1002/deletedosprofile

Payload

```
{ "dosProfileName" : "profile_Thu_Apr_24_17_50_16_IST_2014.dat.gz" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1124	The Sensor is inactive
3	400	5601	The profile name does not exist for the Sensor

Export the DoS Profile to the Manager Client

This URL exports the DoS profile to the Manager client.

Resource URL

PUT /sensor/<sensor_id>/ exportdosprofile

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`DosProfileExport`	DoS profile	Object	Yes

Details of DosProfileRestoreName:

Field Name	Description	Data Type	Mandatory
dosProfileName	DoS profile name	String	Yes
destinationFolder	Destination folder of the client	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Set to 1 if the operation was successful	Number
message	Returns the status messages	String

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1002/exportdosprofile

Payload

```
{ "dosProfileName": "profile_Fri_Apr_25_15_49_38_IST_2014.dat.gz", "destinationFolder": "C:\\dos" }
```

Response

```
{ "status": 1, "message": "File Copied to : C:\dos\profile_Fri_Apr_25_15_49_38_IST_2014.dat.gz " }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1124	The Sensor is inactive

Get the Domain Name Exceptions from the Manager

This URL retrieves the domain name exceptions from the Manager.

Resource URL

GET /domainnameexceptions/

Request Parameters

URL Parameters: None

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`dneDetail`	List of domain name exceptions details	ObjectList

Details of dneDetail (list of following object):

Field Name	Description	Data Type
`added`	When and who added the domain name exception	String
`id`	Domain name exception id	Number
`domainName`	Name of domain	String
`comment`	Description of exception	String

Example

Request

GET https://<NSM_IP>/sdkapi/domainnameexceptions

Response

```
{ 'dneDetail': [{ 'added': 'Sep 1 16:20 (admin)', 'id': 9835, 'domainName': 'www.google.com', 'comment':
'Google' }, { 'added': 'Sep 1 16:20 (admin)', 'id': 9836, 'domainName': 'www.yahoo.com' }, { 'added': 'Sep 1
16:20(admin)', 'id': 9837, 'domainName': 'www.abc.com' }] }
```

Error Information

None

Import the Domain Name Exceptions to the Manager

This URL imports the domain name exceptions to the Manager.

Resource URL

POST /domainnameexceptions/import

Request Parameters

URL Parameters: None

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
MultiPart	Holds the body part objects	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the DNE file element object	Application/json object	Yes

Details of DNE file element:

Field Name	Description	Data Type	Mandatory
fileName	Name of the file	String	Yes
fileType	File type should be .csv	String	No

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
BodyPart[1]	Holds the file as input stream	Application/octet-stream	Yes

Details of .csv file:

Field Name	Description	Data Type	Mandatory
File	Domain name exceptions input stream	ByteArrayInput stream	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Set to 1 if the operation was successful	Number

Example

Request

POST https://<NSM_IP>/sdkapi/domainnameexceptions/import

Payload

```
----Boundary_1_12424925_1353496814940 Content-Type: application/json {"fileType": null, "fileName": "dne"} ----
Boundary_1_12424925_1353496814940 Content-Type: application/octet-stream www.google.com, www.yahoo.com,
www.abc.com, www.test1.com, www.test2.com ----Boundary_1_12424925_1353496814940--
```

Response

```
{ "status": 1 }
```

Error Information

Following error code s returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	2202	Input stream read error

Export the Domain Name Exceptions from the Manager

This URL exports the domain name exceptions from the Manager.

Resource URL

GET /domainnameexceptions/export

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
byteStream	Byte stream of the exported file	String

Example

Request

GET https://<NSM_IP>/sdkapi/domainnameexceptions/export

Response

```
{ "byteStream": "www.google.com,\nwww.yahoo.com,\nwww.abc.com,nwww.test1.com,\nwww.test2.com" }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: Internal server error

Update a Domain Name Exception’s Comment

This URL updates a domain name exception's comment.

Resource URL

PUT /domainnameexceptions

Request Parameters

URL Parameters: None

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
domainName	Name of domain	String	Yes
comment	Description of exception	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domainnameexceptions

Payload

```
{ "domainName": "www.google.com", "comment": "Google" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: Internal server error
2	500	1001	Internal error message: Following domain name was not found: <domainname>

Delete Some Domain Name Exceptions

This URL deletes the domain name exceptions specified in the string list.

Resource URL

DELETE /domainnameexceptions

Request Parameters

URL Parameters: None

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
domainName	List of name of domain exception	StringList	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/domainnameexceptions

Payload

```
{ "domainName": ["www.google.com", "abc", "test"] }
```

Response

```
{ "status": 1 }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: Following domain names were not found: <domainname1>, <domainname2>, others have been deleted.

Delete all Domain Name Exceptions

This URL deletes all domain name exceptions.

Resource URL

DELETE /domainnameexceptions/all

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/domainnameexceptions/all

Payload

None

Response

```
{ "status": 1 }
```

Error Information

None

Add Domain Name to Callback Detector Allowlist

This URL adds domain name to callback detection allowlist.

Resource URL

POST /domainnameexceptions

Request Parameters

URL Parameters: None

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
domainName	Name of the new domain	String	Yes
comment	Description of exception	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
createdResourceId	Unique id of the created domain name exception.	Number

Example

Request

POST https://<NSM_IP>/sdkapi/domainnameexceptions

Payload

```
{ "domainName": "www.google1.com", "comment": "updated domain" }
```

Response

```
{ "createdResourceId": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: Internal server error
2	500	1001	Internal error message: Domain name field is required

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
3	500	1001	Invalid domain name. The length should be a maximum of 67 characters.
4	500	1001	Invalid domain name
5	500	1001	Duplicate domain name

Update the Details of Domain Name Exception

This URL updates the details of domain name exception from the callback detection allowlist.

Resource URL

PUT /domainnameexceptions/updatedetail

Request Parameters

URL Parameters: None

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`oldDomainName`	Name of the old domain	String	Yes
`domainName`	Name of the new domain	String	Yes
`comment`	Description of exception	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation is successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domainnameexceptions/updatedetail

Payload

```
{ “oldDomainName”: “www.google.com”, "domainName": "www.google1.com", "comment": "updated domain" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: Internal server error

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
2	500	1001	Internal error message: Domain name field is not found <domainname>
3	500	1001	Invalid domain name. The length should be a maximum of 67 characters.
4	500	1001	Invalid domain name
5	500	1001	Duplicate domain name

Get the Direct Syslog Configuration for the Domain

This URL retrieves the direct syslog configuration for the domain.

Resource URL

GET /domain/<domain_id>/directsyslog

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domainId	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
enableSyslog	Enable logging	Boolean
isInherit	Inherit settings from parent resource	Boolean
serverIp	Syslog server IP	String
serverPort	Syslog server port (UDP)	Number
syslogFacility	Syslog facility	String
syslogPriorityMapping	Attack severity to syslog priority mapping	Object
message	Message format	String
filter	What attacks to log	Object

Details of syslogPriorityMapping:

Field Name	Description	Data Type
informationTo	Informational severity attack mapping	String
lowTo	Low severity attack mapping	String
mediumTO	Medium severity attack mapping	String
highTo	High severity attack mapping	String

Details of filter:

Field Name	Description	Data Type
LogSomeAttacks	Log some attacks	Object

Field Name	Description	Data Type
`LogAllAttacks`	Log all attacks - empty object	Object
`isQuarantineLogging`	Log quarantined attacks	Boolean

Details of LogSomeAttacks:

Field Name	Description	Data Type
`isExplicitlyEnabled`	The attack definition has syslog notification explicitly enabled	Boolean
`minimumSeverity`	Minimum severity of attacks	Object

Details of minimumSeverity:

Field Name	Description	Data Type
`isMinimumSeverity`	Is minimum severity selected	Boolean
`severityType`	Type of the severity	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/directsyslog

Response

```
{ 'enableSyslog': 'true', 'syslogPriorityMapping': { 'lowTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'highTo':
'EMERGENCY_SYSTEM_UNUSABLE', 'informationTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'mediumTO':
'EMERGENCY_SYSTEM_UNUSABLE' }, 'isInherit': 'false', 'serverIp': '10.213.172.94', 'filter': { 'LogSomeAttacks':
{ 'isExplicitlyEnabled': 'false', 'minimumSeverity': { 'isMinimumSeverity': 'false', 'severityType':
'LOW' } } }, 'serverPort': '514', 'syslogFacility': 'SECURITY_AUTHORIZATION_CODE_4', 'message': 'Admin_Domain=
$IV_ADMIN_DOMAIN$Alert_Type=$IV_ALERT_TYPE$Attack_Name=$IV_ATTACK_NAME$AttackConfidence=$IV_ATTACK_CONFIDENCE
$DetectMech=$IV_DETECTION_MECHANISM$Category=$IV_CATEGORY$SubCategory=$IV_SUB_CATEGORY$INTF=$IV_INTERFACE
$Attack_Id=$IV_ATTACK_ID$Attack_Count=$IV_ATTACK_COUNT$Attack_Severity=$IV_ATTACK_SEVERITY$Attack_Signature=
$IV_ATTACK_SIGNATURE$Source_Ip=$IV_SOURCE_IP$Dest_Ip=$IV_DESTINATION_IP$Dest_Port=$IV_DESTINATION_PORT
$Source_Port=$IV_SOURCE_PORT$Malware_Confidence=$IV_MALWARE_CONFIDENCE$Detection_Engine=
$IV_MALWARE_DETECTION_ENGINE$Mal_File_Len=$IV_MALWARE_FILE_LENGTH$Mal_file_md5=$IV_MALWARE_FILE_MD5_HASH
$Mal_File_Name=$IV_MALWARE_FILE_NAME$Mal_File_Type=$IV_MALWARE_FILE_TYPE$Mal_Vir_Name=$IV_MALWARE_VIRUS_NAME
$Direction=$IV_DIRECTION$Nw_Protocol=$IV_NETWORK_PROTOCOL$AppProtocol=$IV_APPLICATION_PROTOCOL$Attack_Time=
$IV_ATTACK_TIME$Qurantine_Time=$IV_QUARANTINE_END_TIME$Result_Status=$IV_RESULT_STATUS$Alert_UUID=
$IV_SENSOR_ALERT_UUID$PeerName=$IV_SENSOR_CLUSTER_MEMBER$Sensor_Name=$IV_SENSOR_NAME$SourceOs=$IV_SOURCE_OS
$DestOs=$IV_DEST_OS$Src_APN=$IV_SRC_APN$Dest_APN=$IV_DEST_APN$Src_IMSI=$IV_SRC_IMSI$Dest_IMSI=$IV_DEST_IMSI
$Src_Phone=$IV_SRC_PHONE_NUMBER$Dest_Phone=$IV_DEST_PHONE_NUMBER$Vlan_ID=$IV_VLAN_ID$' }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	6001	Direct sysog configuration is not present for this domain/ Sensor

Update the Direct Syslog Configuration for the Domain

This URL updates the direct syslog configuration for the domain.

Resource URL

PUT /domain/<domain_id>/directsyslog

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domainId	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
enableSyslog	Enable logging	Boolean	Yes
isInherit	Inherit settings from parent resource	Boolean	Yes
serverIp	Syslog server IP	String	Yes
serverPort	Syslog server port (UDP)	Number	Yes
syslogFacility	Syslog facility. Allowed values are: • SECURITY_AUTHORIZATION_CODE_10 • SECURITY_AUTHORIZATION_CODE_4 • LOG_AUDIT_NOTE_1 • LOG_ALERT_NOTE_1 • CLOCK_DAEMON_NOTE_2 • LOCAL_USER_0 • LOCAL_USER_1 • LOCAL_USER_2 • LOCAL_USER_3 • LOCAL_USER_4 • LOCAL_USER_5 • LOCAL_USER_6 • LOCAL_USER_7	String	Yes
syslogPriorityMapping	Attack severity to syslog priority mapping	Object	Yes
message	Message format	String	Yes
filter	What attacks to log	Object	Yes

Details of syslogPriorityMapping:

Field Name	Description	Data Type	Mandatory
informationTo	Informational severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE	String	Yes

Field Name	Description	Data Type	Mandatory
	• ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES		
`lowTo`	Low severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	Yes
`mediumTO`	Medium severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	yes
`highTo`	High severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	Yes

Details of filter:

Field Name	Description	Data Type	Mandatory
`LogSomeAttacks`	Log some attacks	Object	Yes
`LogAllAttacks`	Log all attacks - empty object	Object	Yes
`isQuarantineLogging`	Log quarantined attacks	Boolean	yes

Details of LogSomeAttacks:

Field Name	Description	Data Type	Mandatory
`isExplicitlyEnabled`	The attack definition has Syslog notification explicitly enabled	Boolean	Yes
`minimumSeverity`	Minimum severity of attacks	Object	Yes

Details of minimumSeverity:

Field Name	Description	Data Type	Mandatory
`isMinimumSeverity`	Is minimum severity selected	Boolean	Yes
`severityType`	Type of the severity. Allowed values are: • INFORMATIONAL • LOW • MEDIUM • HIGH	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/directsyslog

Payload

```
{ 'enableSyslog': 'true', 'syslogPriorityMapping': { 'lowTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'highTo':
'EMERGENCY_SYSTEM_UNUSABLE', 'informationTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'mediumTO':
'EMERGENCY_SYSTEM_UNUSABLE' }, 'isInherit': 'false', 'serverIp': '10.213.172.94', 'filter': { 'LogSomeAttacks':
{ 'isExplicitlyEnabled': 'false', 'minimumSeverity': { 'isMinimumSeverity': 'false', 'severityType':
'LOW' } } }, 'serverPort': '514', 'syslogFacility': 'SECURITY_AUTHORIZATION_CODE_4', 'message': 'Admin_Domain=
$IV_ADMIN_DOMAIN$Alert_Type=$IV_ALERT_TYPE$Attack_Name=$IV_ATTACK_NAME$AttackConfidence=$IV_ATTACK_CONFIDENCE
$DetectMech=$IV_DETECTION_MECHANISM$Category=$IV_CATEGORY$SubCategory=$IV_SUB_CATEGORY$INTF=$IV_INTERFACE
$Attack_Id=$IV_ATTACK_ID$Attack_Count=$IV_ATTACK_COUNT$Attack_Severity=$IV_ATTACK_SEVERITY$Attack_Signature=
$IV_ATTACK_SIGNATURE$Source_Ip=$IV_SOURCE_IP$Dest_Ip=$IV_DESTINATION_IP$Dest_Port=$IV_DESTINATION_PORT
$Source_Port=$IV_SOURCE_PORT$Malware_Confidence=$IV_MALWARE_CONFIDENCE$Detection_Engine=
$IV_MALWARE_DETECTION_ENGINE$Mal_File_Len=$IV_MALWARE_FILE_LENGTH$Mal_file_md5=$IV_MALWARE_FILE_MD5_HASH
$Mal_File_Name=$IV_MALWARE_FILE_NAME$Mal_File_Type=$IV_MALWARE_FILE_TYPE$Mal_Vir_Name=$IV_MALWARE_VIRUS_NAME
$Direction=$IV_DIRECTION$Nw_Protocol=$IV_NETWORK_PROTOCOL$AppProtocol=$IV_APPLICATION_PROTOCOL$Attack_Time=
$IV_ATTACK_TIME$Qurantine_Time=$IV_QUARANTINE_END_TIME$Result_Status=$IV_RESULT_STATUS$Alert_UUID=
$IV_SENSOR_ALERT_UUID$PeerName=$IV_SENSOR_CLUSTER_MEMBER$Sensor_Name=$IV_SENSOR_NAME$SourceOs=$IV_SOURCE_OS
$DestOs=$IV_DEST_OS$Src_APN=$IV_SRC_APN$Dest_APN=$IV_DEST_APN$Src_IMSI=$IV_SRC_IMSI$Dest_IMSI=$IV_DEST_IMSI
$Src_Phone=$IV_SRC_PHONE_NUMBER$Dest_Phone=$IV_DEST_PHONE_NUMBER$Vlan_ID=$IV_VLAN_ID$' }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	6002	IPV6 is not supported for direct syslog configuration

Get the Direct Syslog Configuration for the Sensor

This URL retrieves the direct syslog configuration for the Sensor.

Resource URL

GET /sensor/<sensor_id>/directsyslog

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`enableSyslog`	Enable logging	Boolean
`isInherit`	Inherit settings from parent resource	Boolean
`serverIp`	Syslog server IP	String
`serverPort`	Syslog server port (UDP)	Number
`syslogFacility`	Syslog facility	String
`syslogPriorityMapping`	Attack severity to syslog priority mapping	Object
`message`	Message format	String
`filter`	What attacks to log	Object

Details of syslogPriorityMapping:

Field Name	Description	Data Type
`informationTo`	Informational severity attack mapping	String

Field Name	Description	Data Type
`lowTo`	Low severity attack mapping	String
`mediumTO`	Medium severity attack mapping	String
`highTo`	High severity attack mapping	String

Details of filter:

Field Name	Description	Data Type
`LogSomeAttacks`	Log some attacks	Object
`LogAllAttacks`	Log all attacks - empty object	Object
`isQuarantineLogging`	Log quarantined attacks	Boolean

Details of LogSomeAttacks:

Field Name	Description	Data Type
`isExplicitlyEnabled`	The attack definition has syslog notification explicitly enabled	Boolean
`minimumSeverity`	Minimum severity of attacks	Object

Details of minimumSeverity:

Field Name	Description	Data Type
`isMinimumSeverity`	Is minimum severity selected	Boolean
`severityType`	Type of the severity	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/directsyslog

Response

```
{ 'enableSyslog': 'true', 'syslogPriorityMapping': { 'lowTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'highTo':
'EMERGENCY_SYSTEM_UNUSABLE', 'informationTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'mediumTO':
'EMERGENCY_SYSTEM_UNUSABLE' }, 'isInherit': 'false', 'serverIp': '10.213.172.94', 'filter': { 'LogSomeAttacks':
{ 'isExplicitlyEnabled': 'false', 'minimumSeverity': { 'isMinimumSeverity': 'false', 'severityType':
'LOW' } } }, 'serverPort': '514', 'syslogFacility': 'SECURITY_AUTHORIZATION_CODE_4', 'message': 'Admin_Domain=
$IV_ADMIN_DOMAIN$Alert_Type=$IV_ALERT_TYPE$Attack_Name=$IV_ATTACK_NAME$AttackConfidence=$IV_ATTACK_CONFIDENCE
$DetectMech=$IV_DETECTION_MECHANISM$Category=$IV_CATEGORY$SubCategory=$IV_SUB_CATEGORY$INTF=$IV_INTERFACE
$Attack_Id=$IV_ATTACK_ID$Attack_Count=$IV_ATTACK_COUNT$Attack_Severity=$IV_ATTACK_SEVERITY$Attack_Signature=
$IV_ATTACK_SIGNATURE$Source_Ip=$IV_SOURCE_IP$Dest_Ip=$IV_DESTINATION_IP$Dest_Port=$IV_DESTINATION_PORT
$Source_Port=$IV_SOURCE_PORT$Malware_Confidence=$IV_MALWARE_CONFIDENCE$Detection_Engine=
$IV_MALWARE_DETECTION_ENGINE$Mal_File_Len=$IV_MALWARE_FILE_LENGTH$Mal_file_md5=$IV_MALWARE_FILE_MD5_HASH
$Mal_File_Name=$IV_MALWARE_FILE_NAME$Mal_File_Type=$IV_MALWARE_FILE_TYPE$Mal_Vir_Name=$IV_MALWARE_VIRUS_NAME
$Direction=$IV_DIRECTION$Nw_Protocol=$IV_NETWORK_PROTOCOL$AppProtocol=$IV_APPLICATION_PROTOCOL$Attack_Time=
$IV_ATTACK_TIME$Qurantine_Time=$IV_QUARANTINE_END_TIME$Result_Status=$IV_RESULT_STATUS$Alert_UUID=
$IV_SENSOR_ALERT_UUID$PeerName=$IV_SENSOR_CLUSTER_MEMBER$Sensor_Name=$IV_SENSOR_NAME$SourceOs=$IV_SOURCE_OS
$DestOs=$IV_DEST_OS$Src_APN=$IV_SRC_APN$Dest_APN=$IV_DEST_APN$Src_IMSI=$IV_SRC_IMSI$Dest_IMSI=$IV_DEST_IMSI
$Src_Phone=$IV_SRC_PHONE_NUMBER$Dest_Phone=$IV_DEST_PHONE_NUMBER$Vlan_ID=$IV_VLAN_ID$' }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1106	Invalid Sensor
2	404	1124	The Sensor is inactive
3	400	6001	Direct sysog configuration is not present for this domain/ Sensor

Update the Direct Syslog Configuration for the Sensor

This URL updates the direct syslog configuration for the Sensor.

Resource URL

PUT /sensor/<sensor_id>/directsyslog

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`enableSyslog`	Enable logging	Boolean	Yes
`isInherit`	Inherit settings from parent resource	Boolean	Yes
`serverIp`	Syslog server IP	String	Yes
`serverPort`	Syslog server port (UDP)	number	Yes
`syslogFacility`	Syslog facility. Allowed values are: • SECURITY_AUTHORIZATION_CODE_10 • SECURITY_AUTHORIZATION_CODE_4 • LOG_AUDIT_NOTE_1 • LOG_ALERT_NOTE_1 • CLOCK_DAEMON_NOTE_2 • LOCAL_USER_0 • LOCAL_USER_1 • LOCAL_USER_2 • LOCAL_USER_3 • LOCAL_USER_4 • LOCAL_USER_5 • LOCAL_USER_6	String	Yes

Field Name	Description	Data Type	Mandatory
	• LOCAL_USER_7		
`syslogPriorityMapping`	Attack severity to syslog priority mapping	Object	Yes
`message`	Message format	String	Yes
`filter`	What attacks to log	Object	Yes

Details of syslogPriorityMapping:

Field Name	Description	Data Type	Mandatory
`informationTo`	Informational severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	Yes
`lowTo`	Low severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	Yes
`mediumTO`	Medium severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	yes

Field Name	Description	Data Type	Mandatory
`highTo`	High severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	Yes

Details of filter:

Field Name	Description	Data Type	Mandatory
`LogSomeAttacks`	Log some attacks	Object	Yes
`LogAllAttacks`	Log all attacks - empty object	Object	Yes
`isQuarantineLogging`	Log quarantined attacks	Boolean	yes

Details of LogSomeAttacks:

Field Name	Description	Data Type	Mandatory
`isExplicitlyEnabled`	The attack definition has syslog notification explicitly enabled	Boolean	Yes
`minimumSeverity`	Minimum severity of attacks	Object	Yes

Details of minimumSeverity:

Field Name	Description	Data Type	Mandatory
`isMinimumSeverity`	Is minimum severity selected	Boolean	Yes
`severityType`	Type of the severity. Allowed values are: • INFORMATIONAL • LOW • MEDIUM • HIGH	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1001/directsyslog

Payload

```
{ 'enableSyslog': 'true', 'syslogPriorityMapping': { 'lowTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'highTo':
'EMERGENCY_SYSTEM_UNUSABLE', 'informationTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'mediumTO':
'EMERGENCY_SYSTEM_UNUSABLE' }, 'isInherit': 'false', 'serverIp': '10.213.172.94', 'filter': { 'LogSomeAttacks':
{ 'isExplicitlyEnabled': 'false', 'minimumSeverity': { 'isMinimumSeverity': 'false', 'severityType':
'LOW' } } }, 'serverPort': '514', 'syslogFacility': 'SECURITY_AUTHORIZATION_CODE_4', 'message': 'Admin_Domain=
$IV_ADMIN_DOMAIN$Alert_Type=$IV_ALERT_TYPE$Attack_Name=$IV_ATTACK_NAME$AttackConfidence=$IV_ATTACK_CONFIDENCE
$DetectMech=$IV_DETECTION_MECHANISM$Category=$IV_CATEGORY$SubCategory=$IV_SUB_CATEGORY$INTF=$IV_INTERFACE
$Attack_Id=$IV_ATTACK_ID$Attack_Count=$IV_ATTACK_COUNT$Attack_Severity=$IV_ATTACK_SEVERITY$Attack_Signature=
$IV_ATTACK_SIGNATURE$Source_Ip=$IV_SOURCE_IP$Dest_Ip=$IV_DESTINATION_IP$Dest_Port=$IV_DESTINATION_PORT
$Source_Port=$IV_SOURCE_PORT$Malware_Confidence=$IV_MALWARE_CONFIDENCE$Detection_Engine=
$IV_MALWARE_DETECTION_ENGINE$Mal_File_Len=$IV_MALWARE_FILE_LENGTH$Mal_file_md5=$IV_MALWARE_FILE_MD5_HASH
$Mal_File_Name=$IV_MALWARE_FILE_NAME$Mal_File_Type=$IV_MALWARE_FILE_TYPE$Mal_Vir_Name=$IV_MALWARE_VIRUS_NAME
$Direction=$IV_DIRECTION$Nw_Protocol=$IV_NETWORK_PROTOCOL$AppProtocol=$IV_APPLICATION_PROTOCOL$Attack_Time=
$IV_ATTACK_TIME$Qurantine_Time=$IV_QUARANTINE_END_TIME$Result_Status=$IV_RESULT_STATUS$Alert_UUID=
$IV_SENSOR_ALERT_UUID$PeerName=$IV_SENSOR_CLUSTER_MEMBER$Sensor_Name=$IV_SENSOR_NAME$SourceOs=$IV_SOURCE_OS
$DestOs=$IV_DEST_OS$Src_APN=$IV_SRC_APN$Dest_APN=$IV_DEST_APN$Src_IMSI=$IV_SRC_IMSI$Dest_IMSI=$IV_DEST_IMSI
$Src_Phone=$IV_SRC_PHONE_NUMBER$Dest_Phone=$IV_DEST_PHONE_NUMBER$Vlan_ID=$IV_VLAN_ID$' }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1106	Invalid Sensor
2	404	1124	The Sensor is inactive
3	400	6002	IPV6 is not supported for direct syslog configuration

Test the Direct Syslog Configuration for Domain

This URL tests the direct syslog configuration for the domain.

Resource URL

PUT /sensor/<sensor_id>/directsyslog

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`enableSyslog`	Enable logging	Boolean	Yes
`isInherit`	Inherit settings from parent resource	Boolean	Yes

Field Name	Description	Data Type	Mandatory
`serverIp`	Syslog server IP	String	Yes
`serverPort`	Syslog server port (UDP)	Number	Yes
`syslogFacility`	Syslog Facility. Allowed values are: • SECURITY_AUTHORIZATION_CODE_10 • SECURITY_AUTHORIZATION_CODE_4 • LOG_AUDIT_NOTE_1 • LOG_ALERT_NOTE_1 • CLOCK_DAEMON_NOTE_2 • LOCAL_USER_0 • LOCAL_USER_1 • LOCAL_USER_2 • LOCAL_USER_3 • LOCAL_USER_4 • LOCAL_USER_5 • LOCAL_USER_6 • LOCAL_USER_7	String	Yes
`syslogPriorityMapping`	Attack severity to syslog priority mapping	Object	Yes
`message`	Message format	String	Yes
`filter`	What attacks to log	Object	Yes

Details of syslogPriorityMapping:

Field Name	Description	Data Type	Mandatory
`informationTo`	Informational severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	Yes
`lowTo`	Low severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR	String	Yes

Field Name	Description	Data Type	Mandatory
	• WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES		
`mediumTO`	Medium severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	yes
`highTo`	High severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	Yes

Details of filter:

Field Name	Description	Data Type	Mandatory
`LogSomeAttacks`	Log some attacks	Object	Yes
`LogAllAttacks`	Log all attacks - empty object	Object	Yes
`isQuarantineLogging`	Log quarantined attacks	Boolean	yes

Details of LogSomeAttacks:

Field Name	Description	Data Type	Mandatory
`isExplicitlyEnabled`	The attack definition has syslog notification explicitly enabled	Boolean	Yes
`minimumSeverity`	Minimum severity of attacks	Object	Yes

Details of minimumSeverity:

Field Name	Description	Data Type	Mandatory
`isMinimumSeverity`	Is minimum severity selected	Boolean	Yes
`severityType`	Type of the severity. Allowed values are: • INFORMATIONAL • LOW • MEDIUM • HIGH	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/directsyslog/testconnection

Payload

```
{ 'enableSyslog': 'true', 'syslogPriorityMapping': { 'lowTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'highTo':
'EMERGENCY_SYSTEM_UNUSABLE', 'informationTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'mediumTO':
'EMERGENCY_SYSTEM_UNUSABLE' }, 'isInherit': 'false', 'serverIp': '10.213.172.94', 'filter': { 'LogSomeAttacks':
{ 'isExplicitlyEnabled': 'false', 'minimumSeverity': { 'isMinimumSeverity': 'false', 'severityType':
'LOW' } } }, 'serverPort': '514', 'syslogFacility': 'SECURITY_AUTHORIZATION_CODE_4', 'message': 'Admin_Domain=
$IV_ADMIN_DOMAIN$Alert_Type=$IV_ALERT_TYPE$Attack_Name=$IV_ATTACK_NAME$AttackConfidence=$IV_ATTACK_CONFIDENCE
$DetectMech=$IV_DETECTION_MECHANISM$Category=$IV_CATEGORY$SubCategory=$IV_SUB_CATEGORY$INTF=$IV_INTERFACE
$Attack_Id=$IV_ATTACK_ID$Attack_Count=$IV_ATTACK_COUNT$Attack_Severity=$IV_ATTACK_SEVERITY$Attack_Signature=
$IV_ATTACK_SIGNATURE$Source_Ip=$IV_SOURCE_IP$Dest_Ip=$IV_DESTINATION_IP$Dest_Port=$IV_DESTINATION_PORT
$Source_Port=$IV_SOURCE_PORT$Malware_Confidence=$IV_MALWARE_CONFIDENCE$Detection_Engine=
$IV_MALWARE_DETECTION_ENGINE$Mal_File_Len=$IV_MALWARE_FILE_LENGTH$Mal_file_md5=$IV_MALWARE_FILE_MD5_HASH
$Mal_File_Name=$IV_MALWARE_FILE_NAME$Mal_File_Type=$IV_MALWARE_FILE_TYPE$Mal_Vir_Name=$IV_MALWARE_VIRUS_NAME
$Direction=$IV_DIRECTION$Nw_Protocol=$IV_NETWORK_PROTOCOL$AppProtocol=$IV_APPLICATION_PROTOCOL$Attack_Time=
$IV_ATTACK_TIME$Qurantine_Time=$IV_QUARANTINE_END_TIME$Result_Status=$IV_RESULT_STATUS$Alert_UUID=
$IV_SENSOR_ALERT_UUID$PeerName=$IV_SENSOR_CLUSTER_MEMBER$Sensor_Name=$IV_SENSOR_NAME$SourceOs=$IV_SOURCE_OS
$DestOs=$IV_DEST_OS$Src_APN=$IV_SRC_APN$Dest_APN=$IV_DEST_APN$Src_IMSI=$IV_SRC_IMSI$Dest_IMSI=$IV_DEST_IMSI
$Src_Phone=$IV_SRC_PHONE_NUMBER$Dest_Phone=$IV_DEST_PHONE_NUMBER$Vlan_ID=$IV_VLAN_ID$' }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	6002	IPV6 is not supported for direct syslog configuration
3	400	6002	Direct syslog is disabled or inherit settings has been selected

Test the Direct Syslog Configuration for the Sensor

This URL tests the direct syslog configuration for the Sensor.

Resource URL

PUT /sensor/<sensor_id>/ directsyslog/testconnection

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensorId	Sensor id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
enableSyslog	Enable logging	Boolean	Yes
isInherit	Inherit settings from parent resource	Boolean	Yes
serverIp	Syslog server IP	String	Yes
serverPort	Syslog server port (UDP)	Number	Yes
syslogFacility	Syslog facility. Values allowed are: • SECURITY_AUTHORIZATION_CODE_10 • SECURITY_AUTHORIZATION_CODE_4 • LOG_AUDIT_NOTE_1 • LOG_ALERT_NOTE_1 • CLOCK_DAEMON_NOTE_2 • LOCAL_USER_0 • LOCAL_USER_1 • LOCAL_USER_2 • LOCAL_USER_3 • LOCAL_USER_4 • LOCAL_USER_5 • LOCAL_USER_6 • LOCAL_USER_7	String	Yes
syslogPriorityMapping	Attack severity to syslog priority mapping	Object	Yes
message	Message format	String	Yes
filter	What attacks to log	Object	Yes

Details of syslogPriorityMapping:

Field Name	Description	Data Type	Mandatory
informationTo	Informational severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	Yes
lowTo	Low severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	Yes
mediumTO	Medium severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	yes
highTo	High severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION	String	Yes

Field Name	Description	Data Type	Mandatory
	• INFORMATIONAL_MESSGES • DEBUG_MESSAGES		

Details of filter:

Field Name	Description	Data Type	Mandatory
`LogSomeAttacks`	Log some attacks	Object	Yes
`LogAllAttacks`	Log all attacks - empty object	Object	Yes
`isQuarantineLogging`	Log quarantined attacks	Boolean	yes

Details of LogSomeAttacks:

Field Name	Description	Data Type	Mandatory
`isExplicitlyEnabled`	The attack definition has syslog notification explicitly enabled	Boolean	Yes
`minimumSeverity`	Minimum severity of attacks	Object	Yes

Details of minimumSeverity:

Field Name	Description	Data Type	Mandatory
`isMinimumSeverity`	Is minimum severity selected	Boolean	Yes
`severityType`	Type of the severity. Allowed values are: • INFORMATIONAL • LOW • MEDIUM • HIGH	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1001/directsyslog/testconnection

Payload

```
{ 'enableSyslog': 'true', 'syslogPriorityMapping': { 'lowTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'highTo':
'EMERGENCY_SYSTEM_UNUSABLE', 'informationTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'mediumTO':
'EMERGENCY_SYSTEM_UNUSABLE' }, 'isInherit': 'false', 'serverIp': '10.213.172.94', 'filter': { 'LogSomeAttacks':
{ 'isExplicitlyEnabled': 'false', 'minimumSeverity': { 'isMinimumSeverity': 'false', 'severityType':
'LOW' } } }, 'serverPort': '514', 'syslogFacility': 'SECURITY_AUTHORIZATION_CODE_4', 'message': 'Admin_Domain=
$IV_ADMIN_DOMAIN$Alert_Type=$IV_ALERT_TYPE$Attack_Name=$IV_ATTACK_NAME$AttackConfidence=$IV_ATTACK_CONFIDENCE
$DetectMech=$IV_DETECTION_MECHANISM$Category=$IV_CATEGORY$SubCategory=$IV_SUB_CATEGORY$INTF=$IV_INTERFACE
$Attack_Id=$IV_ATTACK_ID$Attack_Count=$IV_ATTACK_COUNT$Attack_Severity=$IV_ATTACK_SEVERITY$Attack_Signature=
$IV_ATTACK_SIGNATURE$Source_Ip=$IV_SOURCE_IP$Dest_Ip=$IV_DESTINATION_IP$Dest_Port=$IV_DESTINATION_PORT
$Source_Port=$IV_SOURCE_PORT$Malware_Confidence=$IV_MALWARE_CONFIDENCE$Detection_Engine=
$IV_MALWARE_DETECTION_ENGINE$Mal_File_Len=$IV_MALWARE_FILE_LENGTH$Mal_file_md5=$IV_MALWARE_FILE_MD5_HASH
$Mal_File_Name=$IV_MALWARE_FILE_NAME$Mal_File_Type=$IV_MALWARE_FILE_TYPE$Mal_Vir_Name=$IV_MALWARE_VIRUS_NAME
$Direction=$IV_DIRECTION$Nw_Protocol=$IV_NETWORK_PROTOCOL$AppProtocol=$IV_APPLICATION_PROTOCOL$Attack_Time=
$IV_ATTACK_TIME$Qurantine_Time=$IV_QUARANTINE_END_TIME$Result_Status=$IV_RESULT_STATUS$Alert_UUID=
$IV_SENSOR_ALERT_UUID$PeerName=$IV_SENSOR_CLUSTER_MEMBER$Sensor_Name=$IV_SENSOR_NAME$SourceOs=$IV_SOURCE_OS
$DestOs=$IV_DEST_OS$Src_APN=$IV_SRC_APN$Dest_APN=$IV_DEST_APN$Src_IMSI=$IV_SRC_IMSI$Dest_IMSI=$IV_DEST_IMSI
$Src_Phone=$IV_SRC_PHONE_NUMBER$Dest_Phone=$IV_DEST_PHONE_NUMBER$Vlan_ID=$IV_VLAN_ID$' }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1106	Invalid Sensor
2	404	1124	The Sensor is inactive
3	400	6002	IPV6 is not supported for direct syslog configuration
4	400	6002	Direct syslog is disabled or inherit settings has been selected

Get the Packet Capture Settings

This URL retrieves the packet capture settings.

Resource URL

GET /sensor/<sensor_id>/packetcapture

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Payload Request Parameters: None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status of packet capture	String
`capTureSettings`	Packet capture settings	Object
`rules`	List of packet capture rule	Object

Details of capTureSettings:

Field Name	Description	Data Type
`monitoringSPANPort`	Monitoring SPAN port details	Object
`manager`	Manager settings	Object
`scpServer`	SCP server settings	Object

Details of rules:

Field Name	Description	Data Type
`captureRule`	List of rules	ObjectList

Details of monitoringSPANPort:

Field Name	Description	Data Type
`port`	Monitoring SPAN port	String
`captureDuration`	Duration details	Object

Details of captureDuration:

Field Name	Description	Data Type
captureDurationInMinutes	Capture duration	Number
runTillExplicitlyReleased	Run until released	Boolean

Details of Manager:

Field Name	Description	Data Type
captureSizeinMB	Capture size	Number

Details of scpServer:

Field Name	Description	Data Type
scpServerIP	IP of SCP server	String
scpServerUserName	SCP user name	String
scpServerPassword	SCP server password	String
captureSizeinMB	Capture size	Number

Details of captureRule:

Field Name	Description	Data Type
ruleId	Rule id	Number
monitoringPort	Monitoring port	String
traffic	Traffic	String
protocol	Protocol	String
ipVersion	IP version	String
fragmentsOnly	Fragments only	Boolean
sourceIP	Source IP	String
sourceMask	Source mask	Number
sourcePort	Source port	Number
destinationIP	Destination IP	String
destinationMask	Destination mask	Number
destinationPort	Destination port	Number
vlanId	VLAN id	Number
protocolNumber	Protocol number	Number

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/packetcapture

Response

```
{ "status": "Not yet started", "capTureSettings": { "monitoringSPANPort": { "port": "Capturing Disabled",
"captureDuration": { "captureDurationInMinutes": 120, "runTillExplicitlyReleased": false } }, "manager": null,
"scpServer": null }, "rules": { "captureRule": [ { "ruleId": 716, "monitoringPort": "ALL", "traffic": "ALL",
"protocol": "TCP", "ipVersion": "IPV_6", "fragmentsOnly": true, "sourceIP": "0.0.0.0", "sourceMask": 0,
"sourcePort": 0, "destinationIP": "0.0.0.0", "destinationMask": 0, "destinationPort": 0, "vlanId": 0,
"protocolNumber": 0 }, { "ruleId": 717, "monitoringPort": "ALL", "traffic": "ARP", "protocol": "TCP",
"ipVersion": "IPV_6", "fragmentsOnly": true, "sourceIP": "0.0.0.0", "sourceMask": 0, "sourcePort": 0,
"destinationIP": "0.0.0.0", "destinationMask": 0, "destinationPort": 0, "vlanId": 0, "protocolNumber": 0 } ] } }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive
3	400	6201	Packet capture not supported on this Sensor

Update the Packet Capture Settings

This URL updates the packet capture settings.

Resource URL

PUT /sensor/<sensor_id>/packetcapture

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`capTureSettings`	Packet capture settings can be: monitoring SPAN port/ manager/scp server	Object	No
`templates`	List of template names	StringList	No
`rules`	List of rules	ObjectList	No

Details of capTureSettings:

Field Name	Description	Data Type	Mandatory
`monitoringSPANPort`	Monitoring SPAN port details	Object	No
`manager`	Manager settings	Object	No

Field Name	Description	Data Type	Mandatory
scpServer	SCP server settings	Object	No

Details of monitoringSPANPort:

Field Name	Description	Data Type	Mandatory
port	Monitoring SPAN port	String	No
captureDuration	Duration details	Object	Yes

Details of captureDuration:

Field Name	Description	Data Type	Mandatory
captureDurationInMinutes	Capture duration	Number	No
runTillExplicitlyReleased	Run until released	Boolean	Yes

Details of Manager:

Field Name	Description	Data Type	Mandatory
captureSizeinMB	Capture size	Number	Yes

Details of scp Server:

Field Name	Description	Data Type	Mandatory
scpServerIP	IP of SCP server	String	Yes
scpServerUserName	SCP user name	String	Yes
scpServerPassword	SCP server password	String	Yes
captureSizeinMB	Capture size	Number	Yes

Details of object in rules:

Field Name	Description	Data Type	Mandatory
ruleId	Rule id given if updating existing rule	Number	No
monitoringPort	Monitoring port. Give ALL if choosing for all ports	String	Yes
traffic	Traffic. Can be ALL/ARP/IP	String	Yes
protocol	Protocol. Can be TCP/UDP/ ICMP/PROTOCOL_NUMBER	String	Yes
ipVersion	IP version. Can be IPV_4/IPV_6	String	Yes
fragmentsOnly	Fragments only	Boolean	Yes

Field Name	Description	Data Type	Mandatory
`sourceIP`	Source IP	String	No
`sourceMask`	Source mask	Number	No
`sourcePort`	Source port	Number	No
`destinationIP`	Destination IP	String	No
`destinationMask`	Destination mask	Number	No
`destinationPort`	Destination port	Number	No
`vlanId`	VLAN id	Number	No
`protocolNumber`	Protocol number	Number	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status returned	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1001/packetcapture

Payload

```
{ "capTureSettings": { "monitoringSPANPort": { "port": "ALL", "captureDuration": { "captureDurationInMinutes":
0, "runTillExplicitlyReleased": true } }, "manager": null, "scpServer": null }, "templates": ["test", "test1"],
"rules": [{ "ruleId": 2, "monitoringPort": "ALL", "traffic": "ARP", "protocol": "TCP", "ipVersion": "IPV_4",
"fragmentsOnly": true, "sourceIP": "0.0.0.0", "sourceMask": 0, "sourcePort": 0, "destinationIP": "0.0.0.0",
"destinationMask": 0, "destinationPort": 0, "vlanId": 0, "protocolNumber": 0 }, { "ruleId": 3, "monitoringPort":
"ALL", "traffic": "IP", "protocol": "ICMP", "ipVersion": "IPV_4", "fragmentsOnly": false, "sourceIP":
"192.168.12.0", "sourceMask": 23, "sourcePort": 1, "destinationIP": "192.168.12.0", "destinationMask": 23,
"destinationPort": 1, "vlanId": 1, "protocolNumber": 0 }, { "ruleId": null, "monitoringPort": "ALL", "traffic":
"ALL", "protocol": "TCP", "ipVersion": "IPV_4", "fragmentsOnly": false, "sourceIP": "0.0.0.0", "sourceMask": 0,
"sourcePort": 0, "destinationIP": "0.0.0.0", "destinationMask": 0, "destinationPort": 0, "vlanId": 0,
"protocolNumber": 0 }] }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive
3	400	6201	Packet capture not supported on this Sensor
4	400	6202	Packet capture duration should be between 1 and 9999

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
5	400	6203	Packet capture size should be between 1 and <maxsize>
6	400	6204	SCP server IP, username, password, and capture size are mandatory
7	400	6205	SCP server username should not contain space and special characters other than {-,_,.}
8	400	6206	File upload in progress so could not save the configuration now
9	400	6209	No template present for packet capturing --> <template_name>
10	400	6210	Protocol number should be between 1 and 65535 when PROTOCOL_NUMBER is selected as protocol while you have given --> <protocol_number>
11	400	6211	The rule id give to update is incorrect

Update the Packet Capturing Status

This URL updates the packet capturing status.

Resource URL

PUT /sensor/<sensor_id>/packetcapturestate

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`captureNow`	Packet capture state can be: • START • STOP • CANCEL • DELETE_FILE	String	Yes

Field Name	Description	Data Type	Mandatory
	• UPLOAD_TO_MANAGER • RETRY_SCP_SERVER		

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status returned	Number

Example

Request

PUT https://<NSM_IP>/sensor/1001/packetcapturestate

Payload

```
{ "captureNow": "START" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive
3	400	6201	Packet capture not supported on this Sensor
4	400	6206	File upload in progress so could not save the configuration now
5	400	6207	Packet capture settings where changed but not saved
6	400	6208	No rules present for packet capturing

Get the List/a Particular Rule Template

This URL retrieves the list/a particular rule template.

Resource URL

GET /sensor/<sensor_id>/packetcaptureruletemplate

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Query Parameters:

Field Name	Description	Data Type	Mandatory
`name`	Name of the rule template. Default is empty which returns all the templates	String	no

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`template`	List of rule templates	Array

Details of object in template:

Field Name	Description	Data Type
`templateId`	ID of template	Number
`templateName`	Name of template	String
`visibleToCild`	Visible to child or not	Boolean
`rule`	List of rules	Array

Details of object in rule:

Field Name	Description	Data Type
`ruleId`	Rule id	Number
`traffic`	Traffic	String
`protocol`	Protocol	String
`ipVersion`	IP version	String
`fragmentsOnly`	Fragments only	Boolean
`sourceIP`	Source IP	String
`sourceMask`	Source mask	Number
`sourcePort`	Source port	Number
`destinationIP`	Destination IP	String
`destinationMask`	Destination mask	Number
`destinationPort`	Destination port	Number

Field Name	Description	Data Type
vlanId	VLAN id	Number
protocolNumber	Protocol number	Number

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/packetcaptureruletemplate?name=test

Response

```
{ "tempate": [{ "templateId": 101, "templateName": "test", "visibleToCild": true, "rule": [{ "ruleId": 101,
"traffic": "ALL", "protocol": "TCP", "ipVersion": "IPV_4", "fragmentsOnly": false, "sourceIP": "0.0.0.0",
"sourceMask": 0, "sourcePort": 0, "destinationIP": "0.0.0.0", "destinationMask": 0, "destinationPort": 0,
"vlanId": 0, "protocolNumber": 0 }] }] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive
3	400	6201	Packet capture not supported on this Sensor

Add a Packet Capture Rule Template

This URL adds a packet capture rule template.

Resource URL

POST /sensor/<sensor_id>/packetcaptureruletemplate

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensor_id	Sensor id. Give -1 if all the quarantine hosts are needed	number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
templateName	Name of template	String	Yes
visibleToCild	Visible to child or not	Boolean	Yes
rule	List of rules	Array	Yes

Details of object in rule:

Field Name	Description	Data Type	Mandatory
`traffic`	Traffic	String	Yes
`protocol`	Protocol	String	Yes
`ipVersion`	IP version	String	Yes
`fragmentsOnly`	Fragments only	Boolean	Yes
`sourceIP`	Source IP	String	No
`sourceMask`	Source mask	Number	No
`sourcePort`	Source port	Number	No
`destinationIP`	Destination IP	String	No
`destinationMask`	Destination mask	Number	No
`destinationPort`	Destination port	Number	No
`vlanId`	VLAN id	Number	No
`protocolNumber`	Protocol number	Number	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique id of the created device	Number

Example

Request

POST https://<NSM_IP>/sdkapi/sensor/1001/packetcaptureruletemplate

Payload

```
{ "templateName": "test", "visibleToCild": true, "rule": [{ "traffic": "ALL", "protocol": "TCP", "ipVersion":
"IPV_4", "fragmentsOnly": false, "sourceIP": "0.0.0.0", "sourceMask": 0, "sourcePort": 0, "destinationIP":
"0.0.0.0", "destinationMask": 0, "destinationPort": 0, "vlanId": 0, "protocolNumber": 0 }] }
```

Response

```
{ "createdResourceId":101 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive
3	400	6201	Packet capture not supported on this Sensor

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
4	400	6202	Packet capture duration should be between 1 and 9999
5	400	6203	Packet capture size should be between 1 and <maxSize>
6	400	6204	SCP server IP, username, password, and capture size are mandatory
7	400	6205	SCP server username should not contain space and special characters other than {-,_,.}
8	400	6210	Protocol number should be between 1 and 65535 when PROTOCOL_NUMBER is selected as protocol while you have given --> <protocol_number>

Get the List of PCAP Files Captured

This URL retrieves the list of captured PCAP files.

Resource URL

GET /sensor/<sensor_id>/packetcapturepcapfiles

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`files`	List of PCAP file names	StringList

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/packetcapturepcapfiles

Payload

None

Response

```
{ "files":[“capture_Mon_Aug_18_16_12_49_IST_2014.pcap”, “capture_Mon_Aug_18_16_12_55_IST_2014.pcap”] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive
3	400	6201	Packet capture not supported on this Sensor

Export the PCAP File Captured

This URL exports the captured PCAP file.

Resource URL

PUT /sensor/<sensor_id>/packetcapturepcapfile/export

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id. Give -1 if all the quarantine hosts are needed	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`fileName`	PCAP file name	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`byteStream`	Byte stream of the exported file	String

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1001/packetcapturepcapfile/export

Payload

```
{ "fileName": "capture_Mon_Aug_18_16_12_49_IST_2014.pcap" }
```

Response

```
{ "byteStream": "<pcap file data>" }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive
3	400	6201	Packet capture not supported on this Sensor

Delete the PCAP File Captured

This URL deletes the captured PCAP file.

Resource URL

DELETE /sensor/<sensor_id>/packetcapturepcapfile

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor_id`	Sensor id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`fileName`	PCAP file name	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status returned	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/sensor/1001/packetcapturepcapfile

Payload

```
{ "fileName": "capture_Mon_Aug_18_16_12_49_IST_2014.pcap" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
2	500	1124	The Sensor is inactive
3	400	6201	Packet capture not supported on this Sensor
4	400	1001	Invalid PCAP file. Could not be deleted

Get the List/a Particular Rule Template

This URL retrieves the list/a particular rule template.

Resource URL

GET /domain/<domain_id>/packetcaptureruletemplate

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Query Parameters:

Field Name	Description	Data Type	Mandatory
`name`	Name of the rule template. Default is empty which returns all the templates	String	no

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`tempate`	List of rule templates	Array

Details of object in template:

Field Name	Description	Data Type
`templateId`	Id of template	Number
`templateName`	Name of template	String
`visibleToCild`	Visible to child or not	Boolean
`rule`	List of rules	Array

Details of object in rule:

Field Name	Description	Data Type
`ruleId`	Rule id	Number
`traffic`	Traffic	String
`protocol`	Protocol	String
`ipVersion`	IP version	String
`fragmentsOnly`	Fragments only	Boolean
`sourceIP`	Source IP	String
`sourceMask`	Source mask	Number
`sourcePort`	Source port	Number
`destinationIP`	Destination IP	String
`destinationMask`	Destination mask	Number
`destinationPort`	Destination port	Number
`vlanId`	VLAN id	Number
`protocolNumber`	Protocol number	Number

Example

Request

GET https://<NSM_IP>/sdkapi/domain/101/packetcaptureruletemplate?name=test

Response

```
{ "tempate": [{ "templateId": 101, "templateName": "test", "visibleToCild": true, "rule": [{ "ruleId": 101,
"traffic": "ALL", "protocol": "TCP", "ipVersion": "IPV_4", "fragmentsOnly": false, "sourceIP": "0.0.0.0",
"sourceMask": 0, "sourcePort": 0, "destinationIP": "0.0.0.0", "destinationMask": 0, "destinationPort": 0,
"vlanId": 0, "protocolNumber": 0 }] }] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid domain

Add a Packet Capture Rule Template

This URL adds a packet capture rule template.

Resource URL

POST /domain/<domain_id>/packetcaptureruletemplate

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`templateName`	Name of template	String	Yes
`visibleToCild`	Visible to child or not	Boolean	yes
`rule`	List of rules	Array	yes

Details of object in rule:

Field Name	Description	Data Type	Mandatory
`traffic`	Traffic	String	yes
`protocol`	Protocol	String	yes
`ipVersion`	IP version	String	yes
`fragmentsOnly`	Fragments only	Boolean	yes
`sourceIP`	Source IP	String	no
`sourceMask`	Source mask	Number	no
`sourcePort`	Source port	Number	no
`destinationIP`	Destination IP	String	no
`destinationMask`	Destination mask	Number	no
`destinationPort`	Destination port	Number	no
`vlanId`	VLAN id	Number	no
`protocolNumber`	Protocol number	Number	no

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique id of the created device	Number

Example

Request

POST https://<NSM_IP>/sdkapi/domain/101/packetcaptureruletemplate

Payload

```
{ "templateName": "test", "visibleToCild": true, "rule": [{ "traffic": "ALL", "protocol": "TCP", "ipVersion":
"IPV_4", "fragmentsOnly": false, "sourceIP": "0.0.0.0", "sourceMask": 0, "sourcePort": 0, "destinationIP":
"0.0.0.0", "destinationMask": 0, "destinationPort": 0, "vlanId": 0, "protocolNumber": 0 }] }
```

Response

```
{ "createdResourceId":101 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	4703	Invalid domain
2	400	6202	Packet capture duration should be between 1 and 9999
3	400	6203	Packet capture size should be between 1 and <maxsize>
4	400	6204	SCP server IP, username, password, and capture size are mandatory
5	400	6205	SCP server username should not contain space and special characters other than {-,_,.}
6	400	6210	Protocol number should be between 1 and 65535 when PROTOCOL_NUMBER is selected as protocol while you have given --> <protocol_number>

Update a Packet Capture Rule Template

This URL updates a packet capture rule template.

Resource URL

PUT /domain/<domain_id>/packetcaptureruletemplate/<name>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes
name	Template name	String	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
templateName	Name of template	String	Yes
visibleToCild	Visible to child or not	Boolean	yes

Field Name	Description	Data Type	Mandatory
`rule`	List of rules	Array	yes

Details of object in rule:

Field Name	Description	Data Type	Mandatory
`traffic`	Traffic	String	yes
`protocol`	Protocol	String	yes
`ipVersion`	IP version	String	yes
`fragmentsOnly`	Fragments only	Boolean	yes
`sourceIP`	Source IP	String	no
`sourceMask`	Source mask	Number	no
`sourcePort`	Source port	Number	no
`destinationIP`	Destination IP	String	no
`destinationMask`	Destination mask	Number	no
`destinationPort`	Destination port	Number	no
`vlanId`	VLAN id	Number	no
`protocolNumber`	Protocol number	Number	no

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Status of Update. 1 if successful	Number

Example

Request

POST https://<NSM_IP>/sdkapi/domain/101/packetcaptureruletemplate/test

Payload

```
{ "templateName": "test", "visibleToCild": true, "rule": [{ "traffic": "ALL", "protocol": "TCP", "ipVersion":
"IPV_4", "fragmentsOnly": false, "sourceIP": "0.0.0.0", "sourceMask": 0, "sourcePort": 0, "destinationIP":
"0.0.0.0", "destinationMask": 0, "destinationPort": 0, "vlanId": 0, "protocolNumber": 0 }] }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	4703	Invalid domain

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
2	400	6202	Packet capture duration should be between 1 and 9999
3	400	6203	Packet capture size should be between 1 and <maxsize>
4	400	6204	SCP server IP, username, password, and capture size are mandatory
5	400	6205	SCP server username should not contain space and special characters other than {-,_,.}
6	400	6210	Protocol number should be between 1 and 65535 when PROTOCOL_NUMBER is selected as protocol while you have given --> <protocol_number>
7	400	6213	Invalid template name

Delete a Packet Capture Rule Template

This URL deletes a packet capture rule template.

Resource URL

DELETE /domain/<domain_id>/packetcaptureruletemplate/<name>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes
`name`	Template name	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status of delete. 1 if successful	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/domain/101/packetcaptureruletemplate/test

Payload

None

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	4703	Invalid domain
2	400	6213	Invalid template name

Get All Policy Group

This URL retrieves all the policy group.

Resource URL

GET domain/<domain_id>/policygroup

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`name`	Policy group name	String
`description`	Policy group description	String
`ipsPolicy`	IPS policy name	String
`advancedMalwareInboundPolicy`	Advanced malware inbound policy name	String
`advancedMalwareOutboundPolicy`	Advanced malware outbound policy name	String
`connectionLimitingPolicy`	Connection limiting policy name	String
`firewallPolicy`	Firewall policy name	String
`qosInboundPolicy`	QoS inbound policy name	String
`qosOutboundPolicy`	QoS outbound policy name	String
`protectionOptionsPolicy`	Inspection options policy name	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/policygroup

Response

```
{ "policyGroups": [ { "name": "pg1", "policyGroupId": 21, "description": "desc1", "ipsPolicy": "Default Inline
IPS", "advancedMalwareInboundPolicy": "Default Malware Policy", "advancedMalwareOutboundPolicy": "Default
Malware Policy", "connectionLimitingPolicy": "Test_CLP1", "firewallPolicy": "FirewallPolicy1",
"qosInboundPolicy": "QoSPolicyAdvanced1" } ] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid domain id

Create Policy Group

This URL creates the policy group.

Resource URL

POST domain/<domain_id>/policygroup

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type
`name`	Policy group name	String
`description`	Policy group description	String
`ipsPolicy`	IPS policy name	String
`advancedMalwareInboundPolicy`	Advanced malware inbound policy name	String
`advancedMalwareOutboundPolicy`	Advanced malware outbound policy name	String
`connectionLimitingPolicy`	Connection limiting policy name	String
`firewallPolicy`	Firewall policy name	String
`qosInboundPolicy`	QoS inbound policy name	String
`qosOutboundPolicy`	QoS outbound policy name	String
`protectionOptionsPolicy`	Inspection options policy name	String

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Operation status	Number

Example

Request

POST https://<NSM_IP>/sdkapi/domain/0/policygroup

Payload

```
{ “name”: “pg1”, “policyGroupId”: 21, “description”: “desc1”, “ipsPolicy”: “Default Inline IPS”,
“advancedMalwareInboundPolicy”: “Default Malware Policy”, “advancedMalwareOutboundPolicy”: “Default Malware
Policy”, “connectionLimitingPolicy”: “Test_CLP1”, “firewallPolicy”: “FirewallPolicy1”, “qosInboundPolicy”:
“QoSPolicyAdvanced1” }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid domain id
2	400	2501	Invalid malware policy
3	400	1901	Invalid connection limiting policy
4	400	1801	Invalid firewall policy
5	400	4417	Invalid IPS policy
6	400	9001	Invalid inspection option policy

Get Policy Group

This URL retrieves the policy group.

Resource URL

GET domain/<domain_id>/policygroup/<policygroup_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes
policygroup_id	Policy group id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
name	Policy group name	String
description	Policy group description	String
ipsPolicy	IPS policy name	String
advancedMalwareInboundPolicy	Advanced malware inbound policy name	String

Field Name	Description	Data Type
`advancedMalwareOutboundPolicy`	Advanced malware outbound policy name	String
`connectionLimitingPolicy`	Connection limiting policy name	String
`firewallPolicy`	Firewall policy name	String
`qosInboundPolicy`	Qos inbound policy name	String
`qosOutboundPolicy`	Qos outbound policy name	String
`protectionOptionsPolicy`	Inspection options policy name	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/policygroup/1

Response

```
{ "name": "pg1", "policyGroupId": 21, "description": "desc1", "ipsPolicy": "Default Inline IPS",
"advancedMalwareInboundPolicy": "Default Malware Policy", "advancedMalwareOutboundPolicy": "Default Malware
Policy", "connectionLimitingPolicy": "Test_CLP1", "firewallPolicy": "FirewallPolicy1", "qosInboundPolicy":
"QoSPolicyAdvanced1" }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid domain id
2	400	9000	Invalid policy group

Update Policy Group

This URL updates the policy group.

Resource URL

PUT domain/<domain_id>/policygroup/<policygroup_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes
`policygroup_id`	Policy group id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type
`name`	Policy group name	String

Field Name	Description	Data Type
`description`	Policy group description	String
`ipsPolicy`	IPS policy name	String
`advancedMalwareInboundPolicy`	Advanced malware inbound policy name	String
`advancedMalwareOutboundPolicy`	Advanced malware outbound policy name	String
`connectionLimitingPolicy`	Connection limiting policy name	String
`firewallPolicy`	Firewall policy name	String
`qosInboundPolicy`	QoS inbound policy name	String
`qosOutboundPolicy`	QoS outbound policy name	String
`protectionOptionsPolicy`	Inspection options policy name	String

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Operation status	Int

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/domain/0/policygroup/1

Payload

```
{ "name": "pg1", "policyGroupId": 21, "description": "desc1", "ipsPolicy": "Default Inline IPS",
"advancedMalwareInboundPolicy": "Default Malware Policy", "advancedMalwareOutboundPolicy": "Default Malware
Policy", "connectionLimitingPolicy": "Test_CLP1", "firewallPolicy": "FirewallPolicy1", "qosInboundPolicy":
"QoSPolicyAdvanced1" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid domain id
2	400	2501	Invalid malware policy
3	400	1901	Invalid connection limiting policy
4	400	1801	Invalid firewall policy
5	400	4417	Invalid IPS policy
6	400	9001	Invalid Inspection option policy

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
7	400	9000	Invalid policy group

Delete Policy Group

This URL deletes the policy group.

Resource URL

PUT domain/<domain_id>/policygroup/<policygroup_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes
policygroup_id	Policy group id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Operation status	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/domain/0/policygroup/1

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid domain id
2	400	9000	Invalid policy group

Get All Policy Assignments Interface

This URL retrieves all policies assigned for the interfaces of all the devices in the given domain.

Resource URL

GET domain/<domain_id>/policyassignments/interface

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
deviceName	Device name	String
deviceId	Device id	Number
interfaceName	Interface name	String
interfaceId	Interface id	Number
policygroup	Policy group name	String
ipsPolicy	IPS Policy name	String
advancedMalwareInboundPolicy	Advanced malware inbound policy name	String
advancedMalwareOutboundPolicy	Advanced malware outbound policy name	String
connectionLimitingPolicy	Connection limiting policy name	String
firewallPolicy	Firewall policy name	String
qosInboundPolicy	QoS inbound policy name	String
qosOutboundPolicy	QoS outbound policy name	String
protectionOptionsPolicy	Inspection options policy name	String
qosInboundRateLimitingProfile	QoS inbound rate limiting profile	String
qosOutboundRateLimitingProfile	QoS outbound rate limiting profile	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/policyassignemnts/interface

Response

```
policyAssignmentsList { [ { "deviceName": "API_2950_2", "deviceId": 1001, "interfaceName": "5A-5B",
"interfaceId": 137, "ipsPolicy": "Default Inline IPS", "firewallPolicy": "NSAT_Adv_Rules_for_Interface",
"firewallPortPolicy": "NSAT_Adv_Rules_for_Port", "qosInboundPolicy": "SrvRL_Inbound", "qosOutboundPolicy":
"SrvRL_Outbound", "qosInboundRateLimitingProfile": "AppID-RL Inbound", "qosOutboundRateLimitingProfile": "AppID-
RL Outbound" } ] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid domain id

Get Policy Assignments Interface

This URL retrieves all policies assigned for particular interfaces for the device in the given domain.

Resource URL

GET domain/<domain_id>/policyassignments/interface/<interface_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes
Interface_id	Interface id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
deviceName	Device name	String
deviceId	Device id	Number
interfaceName	Interface name	String
interfaceId	Interface id	Number
policygroup	Policy group name	String
ipsPolicy	IPS policy name	String
advancedMalwareInboundPolicy	Advanced malware inbound policy name	String
advancedMalwareOutboundPolicy	Advanced malware outbound policy name	String
connectionLimitingPolicy	Connection limiting policy name	String
firewallPolicy	Firewall policy name	String
qosInboundPolicy	QoS inbound policy name	String

Field Name	Description	Data Type
qosOutboundPolicy	QoS outbound policy name	String
protectionOptionsPolicy	Inspection options policy name	String
qosInboundRateLimitingProfile	QoS inbound rate limiting profile	String
qosOutboundRateLimitingProfile	QoS outbound rate limiting profile	String
atdUserForInboundATDAnalysis	ATD user for inbound malware analysis	String
atdUserForOutboundATDAnalysis	ATD user for outbound malware analysis	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/policyassignemnts/interface/137

Response

```
policyAssignmentsList { [ { "deviceName": "API_2950_2", "deviceId": 1001, "interfaceName": "5A-5B",
"interfaceId": 137, "ipsPolicy": "Default Inline IPS", "firewallPolicy": "NSAT_Adv_Rules_for_Interface",
"firewallPortPolicy": "NSAT_Adv_Rules_for_Port", "qosInboundPolicy": "SrvRL_Inbound", "qosOutboundPolicy":
"SrvRL_Outbound", "qosInboundRateLimitingProfile": "AppID-RL Inbound", "qosOutboundRateLimitingProfile": "AppID-
RL Outbound" } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid domain id
2	400	1107	Invalid Interface id

Get All Policy Assignments Device

This URL retrieves all policies assigned for the devices in the given domain.

Resource URL

GET domain/<domain_id>/policyassignments/device

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
deviceName	Device name	String
deviceId	Device id	Number

Field Name	Description	Data Type
firewallPolicyLast	Post firewall policy	String
firewallPolicyFirst	Pre-firewall policy	String
reconnaissancePolicy	Reconnaissance policy	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/policyassignemnts/interface

Response

```
policyAssignmentsList { [ { "deviceName": "API_2950_2", "deviceId": 1001, "firewallPolicyLast":
"NSAT_Adv_Rules_for_Interface", "firewallPolicyFirst": "NSAT_Adv_Rules_for_Interface } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid domain id
2	400	1106	Invalid Sensor id

Get Policy Assignments Device

This URL retrieves all policies assigned for the device in the given domain.

Resource URL

GET domain/<domain_id>/policyassignments/device/<device_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	yes
device_id	Device id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
deviceName	Device name	String
deviceId	Device id	Number
firewallPolicyLast	Post firewall policy	String
firewallPolicyFirst	Pre-firewall policy	String
reconnaissancePolicy	Reconnaissance policy	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/policyassignemnts/interface/1001

Response

```
policyAssignmentsList { [ { "deviceName": "API_2950_2", "deviceId": 1001, "firewallPolicyLast":
"NSAT_Adv_Rules_for_Interface", "firewallPolicyFirst": "NSAT_Adv_Rules_for_Interface } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid domain id
2	400	1106	Invalid Sensor id

Update Policy Assignments Interface

This URL updates all policies assigned for particular interfaces for the device in the given domain.

Resource URL

PUT domain/<domain_id>/policyassignments/interface/<interface_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes
Interface_id	Interface id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type
deviceName	Sensor name	String
policygroup	Policy group name	String
ipsPolicy	IPS policy name	String
advancedMalwareInboundPolicy	Advanced malware inbound policy name	String
advancedMalwareOutboundPolicy	Advanced malware outbound policy name	String
connectionLimitingPolicy	Connection limiting policy name	String
firewallPolicy	Firewall policy name	String
qosInboundPolicy	QoS inbound policy name	String
qosOutboundPolicy	QoS outbound policy name	String

Field Name	Description	Data Type
protectionOptionsPolicy	Inspection options policy name	String
qosInboundRateLimitingProfile	QoS inbound rate limiting profile	String
qosOutboundRateLimitingProfile	QoS outbound rate limiting profile	String
atdUserForInboundATDAnalysis	ATD user for inbound malware analysis	String
atdUserForOutboundATDAnalysis	ATD user for outbound malware analysis	String

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Operation status	int

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/policyassignments/interface/137

Payload

```
{ "deviceName":"Sensor-name", "ipsPolicy": "Default Inline IPS", "firewallPolicy":
"NSAT_Adv_Rules_for_Interface", "firewallPortPolicy": "NSAT_Adv_Rules_for_Port", "qosInboundPolicy": null,
"qosOutboundPolicy": "SrvRL_Outbound", "qosInboundRateLimitingProfile": "AppID-RL Inbound",
"qosOutboundRateLimitingProfile”: null }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid domain id
2	400	1107	Invalid interface id

Update Policy Assignments Device

This URL retrieves all policies assigned for the device in the given domain.

Resource URL

PUT domain/<domain_id>/policyassignments/device/<device_id>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain id	Number	Yes
device_id	Device id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type
`firewallPolicyLast`	Post firewall policy	String
`firewallPolicyFirst`	Pre-firewall policy	String
`reconnaissancePolicy`	Reconnaissance policy	String

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Operation status	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/policyassignments/device/1001

Payload

```
{ "firewallPolicyLast": "NSAT_Adv_Rules_for_Interface", "firewallPolicyFirst": "NSAT_Adv_Rules_for_Interface }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid domain id
2	400	1106	Invalid Sensor id

Get the Ignore Rules

These URL's retrieves the details of the ignore rules.

Resource URL

GET /domain/<domainId>/attackfilter82?context = NTBA/SENSOR:

This URL is to retrieve all the details of all the ignore rules created within the given context and domain.

GET /domain/<domainId>/attackfilter82/<ruleId>?context = NTBA/SENSOR:

This URL is to get the details of the ignore rule created with the given rule Id within given context and domain.

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes
`ruleId`	Ignore rule id	Number	Yes (Only to get details of any specific ignore rule)

Query Parameters:

Field Name	Description	Data Type	Mandatory
`context`	Context of the ignore rule. Its values can be: • NTBA • SENSOR	String	Yes (If not specified default is SENSOR)

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`attackFilter`	The details of the ignore rule created within the given domain	Object

Details of attackFilter:

Field Name	Description	Data Type
`id`	The unique identifier for an ignore rule	Number
`state`	Field to indicate whether an ignore rule is active or inactive. The values can be: • ENABLED • DISABLED	String
`name`	Ignore rule name	String

Field Name	Description	Data Type
`attack`	Attack details on which ignore rule is to be applied	Object
`resource`	Details of interface on which ignore rule should is to be applied	Object
`attacker`	Attacker details for ignore rule	Object
`target`	Target details for ignore rule	Object
`lastUpdatedByTime`	Last update time of an ignore rule	Number
`lastUpdatedByUserName`	The user by whom the ignore rule was last updated	String
`comment`	Comments for ignore rule	String
`ownerDomain`	The domain in which the ignore rule is created	String

Details of attack:

Field Name	Description	Data Type
`attackName`	Names of the attack	String
`attackDirection`	Direction of the attack. The values can be: • INBOUND • OUTBOUND • ANY	String

Details of resource:

Field Name	Description	Data Type
`resourceId`	The ID of the interface/resource	Number
`resourceName`	Name of the interface	String
`resourceType`	Indicated the type of interface on which ignore rule is created. Its values can be: • 0: Resource type is domain (for domain level rules) • 1: Resource type is Sensor (for sensor level rules) • 2: Resource type is Vids (for interface and sub-interface level rules) • 3: Resource type is NTBA_ZONE (for rules defined for NTBA inside and outside zones) • 4: Resource type is NTBA_SENSOR (for rules at NTBA level) • 5: Resource type is NTBA_DOMAIN	Number

Field Name	Description	Data Type
`sensorId`	Id of the Sensor on which the rule is applicable	Number

Details of attacker:

Field Name	Description	Data Type
`AttackerEndPoint`	Attacker rule objects on which ignore rules will be applicable.	String
`AttackerPort`	Port type. Its value can be: • TCP • UDP • TCP_UDP • ANY	String
`AttackerPortNumber`	• Port numbers	String

Details of target:

Field Name	Description	Data Type
`TargetEndPoint`	Target rule objects on which ignore rules will be applicable	String
`TargetPort`	Port type. Its value can be: • TCP • UDP • TCP_UDP • ANY	String
`TargetPortNumber`	• Port numbers	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/attackfilter82?context=SENSOR

Response

```
{ "id": 142, "state": "ENABLED", "name": "TEST IGNORE RULE_1", "attack": { "attackName": [ "0x45d20400" ],
"attackDirection": "INBOUND" }, "resource": [ { "resourceID": 118, "resourceName": "M-2950-1/1A-1B",
"resourceType": 2, "sensorID": 1002 } ], "attacker": { "AttackerEndPoint": [ "0012_0040_0045_src",
"109_110_111_112_src" ], "AttackerPort": "TCP", "AttackerPortNumber": "25" }, "target": { "TargetEndPoint":
[ "0012_0040_0045_src", "118_117_116_116_dest" ], "TargetPort": "TCP", "TargetPortNumber": "25" },
"lastUpdatedByTime": 1409726699000, "lastUpdatedByUserName": "admin", "comment": "McAfee NETWORK SECURITY
MANAGER", "ownerDomain": "My Company" }
```

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/attackfilter82/142?context=SENSOR

Response

```
{ "id": 142, "state": "ENABLED", "name": "TEST IGNORE RULE_1", "attack": { "attackName": [ "0x45d20400" ],
"attackDirection": "INBOUND" }, "resource": [ { "resourceID": 118, "resourceName": "M-2950-1/1A-1B",
"resourceType": 2, "sensorID": 1002 } ], "attacker": { "AttackerEndPoint": [ "0012_0040_0045_src",
"109_110_111_112_src" ], "AttackerPort": "TCP", "AttackerPortNumber": "25" }, "target": { "TargetEndPoint":
[ "0012_0040_0045_src", "118_117_116_116_dest" ], "TargetPort": "TCP", "TargetPortNumber": "25" },
"lastUpdatedByTime": 1409726699000, "lastUpdatedByUserName": "admin", "comment": "McAfee NETWORK SECURITY
MANAGER", "ownerDomain": "My Company" }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1408	Invalid rule id/provided rule id not visible to this domain

Create an Ignore Rule

This URL creates a new ignore rule.

Resource URL

POST /domain/<domainId>/attackfilter82

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`attackFilter`	The details of the ignore rules created within the given domain	Object	Yes

Details of attackFilter:

Field Name	Description	Data Type	Mandatory
`id`	The unique identifier for an ignore rule	Number	No
`state`	Field to indicate whether an ignore rule e is active or inactive. The values can be: • ENABLED • DISABLED	String	Yes
`name`	Ignore rule name	String	Yes
`attack`	Attack details on which ignore rule is to be applied	Object	No
`resource`	Details of interface on which ignore rule is to be applied	Object	No
`attacker`	Attacker details for ignore rule	Object	No

Field Name	Description	Data Type	Mandatory
`target`	Target details for ignore rule	Object	No
`lastUpdatedByTime`	Time when an ignore rule was last updated	Number	No
`lastUpdatedByUserName`	The user by whom the ignore rule was last updated	String	No
`comment`	Comments for ignore rule	String	No
`ownerDomain`	The domain in which the ignore rule is created	String	No

Details of attack:

Field Name	Description	Data Type	Mandatory
`attackName`	Names of the attack	String	Yes
`attackDirection`	Direction of the attack. The values can be: • INBOUND • OUTBOUND • ANY	String	Yes

Details of resource:

Field Name	Description	Data Type	Mandatory
`resourceId`	The id of the interface/ resource	Number	No
`resourceName`	Name of the interface	String	Yes (If not specified, default is MATCH ANY)
`resourceType`	Indicated the type of interface on which ignore rule is created. Its values can be: • 0: Resource type is domain (for domain level rules) • 1: Resource type is Sensor (for sensor level rules) • 2: Resource type is Vids (for interface and sub-interface level rules) • 3: Resource type is NTBA_ZONE (for rules defined for NTBA inside and outside zones) • 4: Resource type is NTBA_SENSOR (for rules at NTBA level) • 5: Resource type is NTBA_DOMAIN	Number	No

Field Name	Description	Data Type	Mandatory
`sensorId`	ID of the Sensor on which the rule is applicable	Number	No

Details of attacker:

Field Name	Description	Data Type	Mandatory
`AttackerEndPoint`	Attacker rule objects on which ignore rules will be applicable.	String	Yes (Default is Match ANY)
`AttackerPort`	Port type. Its value can be: • TCP • UDP • TCP_UDP • ANY	String	Yes (If not specified default is ANY)
`AttackerPortNumber`	• Port numbers	String	Yes (Not applicable for ANY port type)

Details of target:

Field Name	Description	Data Type	Mandatory
`TargetEndPoint`	Target rule objects on which ignore rules will be applicable	String	Yes (Default is Match ANY)
`TargetPort`	Port type. Its value can be: • TCP • UDP • TCP_UDP • ANY	String	Yes (If not specified default is ANY)
`TargetPortNumber`	• Port numbers	String	Yes (not applicable for ANY port type)

Note: One of the attacker and target request parameters must be specified.

Query Parameters:

Field Name	Description	Data Type	Mandatory
`context`	Context of the ignore rule. Its values can be: • NTBA • SENSOR	String	Yes (If not specified default is SENSOR)

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Rule id of the created ignore rule	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/attackfilter82?context=SENSOR

Payload

```
{ "state": "ENABLED", "name": "TEST IGNORE RULE_3", "attack": { "attackName": [ "0x45d20400" ],
"attackDirection": "INBOUND" }, "resource": [ { "resourceName": "M-2950-1/1A-1B" } ], "attacker":
{ "AttackerEndPoint": [ "0012_0040_0045_src", "109_110_111_112_src" ], "AttackerPort": "TCP",
"AttackerPortNumber": "25" }, "target": { "TargetEndPoint": [ "0012_0040_0045_src", "118_117_116_116_dest" ],
"TargetPort": "TCP", "TargetPortNumber": "25" }, "comment": "McAfee NETWORK SECURITY MANAGER", }
```

Response

```
{ "createdResourceId": 145 }
```

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/attackfilter82?context=NTBA

Payload

```
{ "state": "ENABLED", "name": "NTBA IGNORE RULE", "attack": { "attackName": [ "0x43f00900", "0x43f00800",
"0x43f00c00" ], "attackDirection": "ANY" }, "resource": [ { "resourceName": "ntba-nsmapi" } ], "attacker":
{ "AttackerEndPoint": [ "0012_0040_0045_src" ], "AttackerPort": "UDP", "AttackerPortNumber": "23" }, "target":
{ "TargetEndPoint": [ "00012_0030_0038_dest" ], "TargetPort": "UDP", "TargetPortNumber": "23" }, "comment":
"McAfee NETWORK SECURITY MANAGER" }
```

Response

```
{ "createdResourceId": 146 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1408	Invalid rule id/provided rule id is not visible this domain
2	400	1720	Invalid rule object/rule object is not visible in this domain
3	400	2513	Name must only letters, numerical, spaces, commas, periods, hyphen or underscore
4	400	1437	Rule name should not be longer than 64 characters
5	400	1433	This rule is invalid because it would match all alerts. Please specify at least one alert criterion
6	400	1434	Port number must be given for TCP, UDP, TCP_UDP port types.
7	400	1415	Port not valid, please enter a number between 1 and 65535
8	400	1422	Resource is not visible in this domain

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
9	400	1001	Rule with same name already exist
10	400	1435	The same combination of IPv4 and IPv6 should be used in attacker and target endpoints.
11	400	1421	The attacker and target port fields are using an invalid protocol combination.
12	400	1436	One of the attacker or target criteria must be specified

Update an Ignore Rule

This URL updates an ignore rule.

Resource URL

POST /domain/<domainId>/attackfilter82/<ruleId>?context=SENSOR/NTBA

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes
`ruleId`	Rule id of the ignore rule to be updated	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`attackFilter`	The details of the ignore rules created within the given domain	Object	Yes

Details of attackFilter:

Field Name	Description	Data Type	Mandatory
`id`	The unique identifier for an ignore rule	Number	No
`state`	Field to indicate whether an ignore rule is active or inactive. The values can be: • ENABLED • DISABLED	String	Yes

Field Name	Description	Data Type	Mandatory
`name`	Ignore rule name	String	Yes
`attack`	Attack details on which ignore rule is to be applied	Object	No
`resource`	Details of interface on which Ignore Rule should is to be applied	Object	No
`attacker`	Attacker details for ignore rule	Object	No
`target`	Target details for ignore rule	Object	No
`lastUpdatedByTime`	Time when an ignore rule was last updated	Number	No
`lastUpdatedByUserName`	The user by whom the ignore rule was last updated	String	No
`comment`	Comments for ignore rule	String	No
`ownerDomain`	The domain in which the ignore rule is created	String	No

Details of attack:

Field Name	Description	Data Type	Mandatory
`attackName`	Names of the attack	String	Yes
`attackDirection`	Direction of the attack. The values can be: • INBOUND • OUTBOUND • ANY	String	Yes

Details of resource:

Field Name	Description	Data Type	Mandatory
`resourceId`	The id of the interface/ resource	Number	No
`resourceName`	Name of the interface	String	Yes (If not specified, default is MATCH ANY)
`resourceType`	Indicated the type of interface on which ignore rule is created. Its values can be: • 0: Resource type is domain (for domain level rules) • 1: Resource type is Sensor (for Sensor level rules)	Number	No

Field Name	Description	Data Type	Mandatory
	• 2: Resource type is Vids (for interface and sub-interface level rules) • 3: Resource type is NTBA_ZONE (for rules defined for NTBA inside and outside zones) • 4: Resource type is NTBA_SENSOR (for rules at NTBA level) • 5: Resource type is NTBA_DOMAIN		
`sensorId`	ID of the Sensor on which the rule is applicable	Number	No

Details of attacker:

Field Name	Description	Data Type	Mandatory
`AttackerEndPoint`	Attacker rule objects on which ignore rules will be applicable. The applicable rule object types for ignore rule are: • IPv4 address range • IPv4 endpoint • IPv4 network • IPv6 address range • IPv6 endpoint • IPv6 network • Network group for exception object	String	Yes (Default is Match ANY)
`AttackerPort`	Port type. Its value can be: • TCP • UDP • TCP_UDP • ANY	String	Yes (If not specified default is ANY)
`AttackerPortNumber`	• Port numbers	String	Yes (not applicable for ANY port type)

Details of target:

Field Name	Description	Data Type	Mandatory
`TargetEndPoint`	Target rule objects on which ignore rules will be applicable. The applicable rule object types are: • IPv4 address range • IPv4 endpoint • IPv4 network • IPv6 address Range	String	Yes (If not specified, default is MATCH ANY)

Field Name	Description	Data Type	Mandatory
	• IPv6 endpoint • IPv6 network • Network group for exception object		
`TargetPort`	Port type. Its value can be: • TCP • UDP • TCP_UDP • ANY	String	Yes (If not specified, default is ANY port type)
`TargetPortNumber`	• Port numbers	String	Yes (not applicable for ANY port type)

Note: One of the attacker and target request parameters must be specified.

Query Parameters:

Field Name	Description	Data Type	Mandatory
`context`	Context of the ignore rule. Its values can be: • NTBA • SENSOR	String	Yes (If not specified default is SENSOR)

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Value 1 indicates resource is updated successfully	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/attackfilter82/143 ?context=SENSOR

Payload

```
{ "state": "ENABLED", "name": "TEST IGNORE RULE_3", "attack": { "attackName": [ "" ], "attackDirection":
"INBOUND" }, "resource": [ { "resourceName": "M-2950-1/1A-1B" } ], "attacker": { "AttackerEndPoint":
[ "0012_0040_0045_src", "109_110_111_112_src" ], "AttackerPort": "TCP", "AttackerPortNumber": "25" }, "target":
{ "TargetEndPoint": [ "0012_0040_0045_src", "118_117_116_116_dest" ], "TargetPort": "TCP", "TargetPortNumber":
"25" }, "comment": "McAfee NETWORK SECURITY MANAGER", }
```

Response

```
{ "status": 1 } In the above payload the Attack name from the TEST IGNORE RULE_3 has been removed. After update
the Response on getting details of TEST IGNORE RULE_3 is: { "state": "ENABLED", "name": "TEST IGNORE RULE_3",
"attack": { "attackName": [ "" ], "attackDirection": "INBOUND" }, "resource": [ { "resourceName":
"M-2950-1/1A-1B" } ], "attacker": { "AttackerEndPoint": [ "0012_0040_0045_src", "109_110_111_112_src" ],
"AttackerPort": "TCP", "AttackerPortNumber": "25" }, "target": { "TargetEndPoint": [ "0012_0040_0045_src",
"118_117_116_116_dest" ], "TargetPort": "TCP", "TargetPortNumber": "25" }, "comment": "McAfee NETWORK SECURITY
MANAGER", }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1408	Invalid rule id/provided rule id is not visible to this domain
2	400	1720	Invalid rule object/rule object is not visible in this domain
3	400	2513	Name must only letters, numerical, spaces, commas, periods, hyphen or underscore
4	400	1437	Rule name should not be longer than 64 characters
5	400	1433	This rule is invalid because it would match all alerts. Please specify at least one alert criterion
6	400	1434	Port number must be given for TCP, UDP, TCP_UDP port types.
7	400	1415	Port not valid, please enter a number between 1 and 65535
8	400	1422	Resource is not visible in this domain
9	400	1435	The same combination of IPv4 and IPv6 should be used in attacker and target endpoints.
10	400	1421	The attacker and target port fields are using an invalid protocol combination.
11	400	1436	One of the attacker or target criteria must be specified

Delete an Ignore Rule

This URL deletes an ignore rule.

Resource URL

DELETE /domain/<domainId>/attackfilter82/<ruleId>?context=NTBA/SENSOR

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domain_id`	Domain id	Number	Yes
`ruleId`	Rule id of the ignore rule to be deleted	Number	Yes

Query Parameters:

Field Name	Description	Data Type	Mandatory
`context`	Context of the ignore rule. Its values can be: • NTBA • SENSOR	String	Yes (If not specified default is SENSOR)

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Value 1 indicates ignore rule is deleted successfully	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/domain/0/attackfilter82/143?context=SENSOR

Response

```
{ "status": 1 }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1408	Invalid rule id/provided rule id is not visible to this domain

Get all Inspection Options Policy

This URL retrieves the all inspection options policies.

Resource URL

GET /protectionoptionspolicy

Request Parameters

N/A

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`policyId`	Policy id	Number
`policyName`	Policy name	String
`domainId`	Domain id	Number
`visibleToChild`	Visible to child	Boolean
`description`	Description	String
`lastUpdatedBy`	Last updated by	String
`lastUpdated`	Last updated date	String

Example

Request

GET https://<NSM_IP>/sdkapi/protectionoptionspolicy

Response

```
{ "protectionOptionsPolicyList": [ { "policyId": 1, "policyName": "Default Client and Server Inspection",
"domainId": 0, "visibleToChild": true, "description": "Inspect traffic both from internal endpoints and to
exposed Web and mail servers", "isEditable": false, "lastUpdatedBy": "admin", "lastUpdated": "2017-Jun-25
18:27", "protectionOptions": null }, { "policyId": 2, "policyName": "Default Client Inspection", "domainId": 0,
"visibleToChild": true, "description": "Inspect traffic from internal endpoints as they access the Internet",
"isEditable": false, "lastUpdatedBy": "admin", "lastUpdated": "2017-Jun-25 18:27", "protectionOptions":
null } ] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid domain id

Get Inspection Options Policy

This URL retrieves the inspection options policy.

Resource URL

GET /protectionoptionspolicy/<policy_id>

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
`policy_id`	Policy id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`policyId`	Policy id	Number
`policyName`	Policy name	String
`domainId`	Domain id	Number
`visibleToChild`	Visible to child	Boolean
`description`	Description	String
`lastUpdatedBy`	Last updated by	String
`lastUpdated`	Last updated date	String
`protectionOptions`	All options tabs	Object

Details of protectionOptions:

Field Name	Description	Data Type
`inspectionOptions`	Inspection options	Object
`advancedBotnetDetectionOptions`	Advanced botnet detection options	Object
`gtiEndpointReputationAnalysysOptions`	GTI endpoint reputation analysis options	Object
`webserverHuresticAnalysysOptions`	Web server heuristic analysis options	Object
`webserverDOSOptions`	Web server DOS options	Object

Details of inspectionOptions:

Field Name	Description	Data Type
`httpResponseTrafficScanning`	HTTP response traffic scanning	String
`httpResponseDecompression`	HTTP response decompression	String
`chunkedHTTPResponseDecoding`	Chunked HTTP response decoding	String
`htmlEncodedHTTPResponseDecoding`	HTML encoded HTTP response decoding	String
`base64SMTPDecoding`	Base64 SMTP decoding	String

Field Name	Description	Data Type
`description`	Description	String
`quotedPrintableSMTPDecoding`	Quoted printable SMTP decoding	String
`msRPCSMBFragmentReassembly`	MSRPC SMB fragment reassembly	String
`msOfficeDeepFileInspection`	Microsoft Office Deep File Inspection	String
`xffHeaderParsing`	XFF header parsing	String
`layer7DataCollection`	Layer 7 data collection	String
`passiveDeviceProfiling`	Passive device profiling	String
`attackBlockingSimulation`	Attack blocking simulation	String

Possible values for above attributes should be:

1. INBOUND_ONLY
2. OUTBOUND_ONLY
3. DISABLED
4. INBOUND_AND_OUTBOUND

Details of advancedBotnetDetectionOptions:

Field Name	Description	Data Type
`advancedBotnetDetection`	Advanced botnet detection	String
`sensitivity`	Sensitivity	String
`fastFluxDetection`	Fast flux detection	String
`domainGenerationAlgorithmDetection`	Domain generation algorithm detection	String
`domainNameAllowlistProcessing`	Domain name allow list processing	String
`exportTrafficToNTBA`	Export traffic to NTBA	Boolean
`dnsSinkHooling`	DNS sink holing	String

Possible values for above attributes should be:

1. INBOUND_ONLY
2. OUTBOUND_ONLY
3. DISABLED
4. INBOUND_AND_OUTBOUND

Possible values for sensitivity should be:

1. LOW
2. MEDIUM
3. HIGH

Details of gtiEndpointReputationAnalysysOptions:

Field Name	Description	Data Type
`gtiEndpointReputationAnalysys`	GTI endpoint reputation analysis • INBOUND_ONLY • OUTBOUND_ONLY • DISABLED • INBOUND_AND_OUTBOUND	String
`useToInfluenceSmartBlocking`	Use to influence SmartBlocking	Boolean
`excludeInternalEndpoint`	Exclude internal endpoint	Boolean
`cidrsExcluded`	CIDRs excluded	Stringlist
`protocalsExcluded`	Protocols excluded	Stringlist
`urlReputationAnalysis`	URL reputation analysis	String
`urlReputationMinimumRisk`	URL reputation min risk	String

Details of webserverHuresticAnalysysOptions:

Field Name	Description	Data Type
`huresticAnalysys`	Heuristic analysis. Direction value as specified above	String
`websitePathToProtect`	Options: ALL or SPECIFIC	String
`blockedTextList`	Block text list	Stringlist
`websitePathToProtectList`	Website path to protect list	Stringlist

Details of webserverDOSOptions:

Field Name	Description	Data Type
`dosPrevention`	DoS prevention: Direction mode	String
`maxConnectionAllowedToWS`	Max connection allowed to WS	Number
`slowConnectionAttackPrevention`	Slow connection attack prevention	Boolean
`maxHTTPRequestPERSecondTOAnyPath`	Max HTTP request per second to any path	Number
`websitePathToProtect`	Website path to protect options: ALL or SPECIFIC	String
`browserDetectionMethod`	Browser detection method	String
`websitePathToProtectList`	Website path to protect list	Objectlist

Example

Request

GET https://<NSM_IP>/sdkapi/protectionoptionspolicy/2

Response

```
{ "policyId": 2, "policyName": "httpresponse", "domainId": 0, "visibleToChild": true, "description": "Enable
xff", "isEditable": true, "lastUpdatedBy": "admin", "lastUpdated": "2014-Aug-11 16:19", "protectionOptions":
{ "inspectionOptions": { "httpResponseTrafficScanning": "INBOUND_AND_OUTBOUND", "chunkedHTTPResponseDecoding":
"DISABLED", "htmlEncodedHTTPResponseDecoding": "DISABLED", "base64SMTPDecoding": "DISABLED",
"quotedPrintableSMTPDecoding": "DISABLED", "msRPCSMBFragmentReassembly": "DISABLED",
"msOfficeDeepFileInspection": "DISABLED", "xffHeaderParsing": "DISABLED", "layer7DataCollection": "DISABLED",
"passiveDeviceProfiling": "DISABLED", "attackBlockingSimulation": false }, "advancedBotnetDetectionOptions":
{ "advancedBotnetDetection": "INBOUND_AND_OUTBOUND", "sensitivity": "LOW", "exportTrafficToNTBA": false,
"fastFluxDetection": "DISABLED", "domainGenerationAlgorithmDetection": "DISABLED", "dnsSinkholing": false,
"domainNameAllowlistProcessing": true, "cidrsExcluded": [], }, "gtiEndpointReputationAnalysysOptions":
{ "gtiEndpointReputationAnalysys": "DISABLED", "useToInfluenceSmartBlocking": false, "excludeInternalEndpoint":
false "cidrsExcluded": [], "protocalsExcluded": [], "urlReputationAnalysis": null, "urlReputationMinimumRisk":
null }, "webserverHuresticAnalysysOptions": { "huresticAnalysys": "INBOUND_ONLY", "websitePathToProtect": "ALL",
"blockedTextList": [], "websitePathToProtectList": [], }, "webserverDOSOptions": { "dosPrevention":
"INBOUND_ONLY", "maxConnectionAllowedToWS": 750000, "slowConnectionAttackPrevention": false,
"maxHTTPRequestPERSecondTOAnyPath": 10000, "websitePathToProtect": "ALL", "clientBrowserDetection": false,
"browserDetectionMethod": null, "websitePathToProtectList": [], } } }
```

Error Information

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid domain id

Create Inspection Options Policy

This URL creates the inspection options policy.

Resource URL

POST /protectionoptionspolicy/

Request Parameters

Payload Parameters:

Field Name	Description	Data Type
`policyId`	Policy id	Number
`policyName`	Policy name	String
`domainId`	Domain id	Number
`visibleToChild`	Visible to child	Boolean
`description`	Description	String
`protectionOptions`	All options tabs	Object

Details of protectionOptions:

Field Name	Description	Data Type
`inspectionOptions`	Inspection options	Object
`advancedBotnetDetectionOptions`	Advanced botnet detection options	Object
`gtiEndpointReputationAnalysysOptions`	GTI endpoint reputation analysis options	Object
`webserverHuresticAnalysysOptions`	Web server heuristic analysis options	Object
`webserverDOSOptions`	Web server DoS options	Object

Details of inspectionOptions:

Field Name	Description	Data Type
`httpResponseTrafficScanning`	HTTP response traffic scanning	String
`httpResponseDecompression`	HTTP response decompression	String
`chunkedHTTPResponseDecoding`	Chunked HTTP response decoding	String
`htmlEncodedHTTPResponseDecoding`	HTML encoded HTTP response decoding	String
`base64SMTPDecoding`	Base64 SMTP decoding	String
`description`	Description	String
`quotedPrintableSMTPDecoding`	Quoted printable SMTP decoding	String
`msRPCSMBFragmentReassembly`	MSRPC SMB fragment reassembly	String
`msOfficeDeepFileInspection`	Microsoft Office deep file inspection	String
`xffHeaderParsing`	XFF header parsing	String
`layer7DataCollection`	Layer 7 data collection	String
`passiveDeviceProfiling`	Passive device profiling	String
`attackBlockingSimulation`	Attack blocking simulation	String

Possible values for above attributes should be:

1. INBOUND_ONLY
2. OUTBOUND_ONLY
3. DISABLED
4. INBOUND_AND_OUTBOUND

Details of advancedBotnetDetectionOptions:

Field Name	Description	Data Type
`advancedBotnetDetection`	Advanced botnet detection	String
`sensitivity`	Sensitivity	String
`fastFluxDetection`	Fast flux detection	String
`domainGenerationAlgorithmDetection`	Domain generation algorithm detection	String
`domainNameAllowlistProcessing`	Domain name allow list processing	String
`exportTrafficToNTBA`	Export traffic to NTBA	Boolean
`dnsSinkHooling`	DNS sink holing	String

Possible values for above attributes should be:

1. INBOUND_ONLY
2. OUTBOUND_ONLY
3. DISABLED

4. INBOUND_AND_OUTBOUND

Possible values for sensitivity should be:

1. LOW
2. MEDIUM
3. HIGH

Details of gtiEndpointReputationAnalysysOptions:

Field Name	Description	Data Type
`gtiEndpointReputationAnalysys`	GTI endpoint reputation analysis • INBOUND_ONLY • OUTBOUND_ONLY • DISABLED • INBOUND_AND_OUTBOUND	String
`useToInfluenceSmartBlocking`	Use to influence SmartBlocking	Boolean
`excludeInternalEndpoint`	Exclude internal endpoint	Boolean
`cidrsExcluded`	CIDRs excluded	Stringlist
`protocalsExcluded`	Protocols excluded	Stringlist
`urlReputationAnalysis`	URL reputation analysis **Valid Values:** • INBOUND_ONLY • OUTBOUND_ONLY • DISABLED • INBOUND_AND_OUTBOUND	String
`urlReputationMinimumRisk`	URL reputation minium risk: **Valid Values:** 1. HIGH 2. MEDIUM	String

Details of webserverHuresticAnalysysOptions:

Field Name	Description	Data Type
`huresticAnalysys`	Heuristic analysis. Direction value as specified above	String
`websitePathToProtect`	Options: ALL or SPECIFIC	String
`blockedTextList`	Blocked text list	Stringlist
`websitePathToProtectList`	Website path to protect list	Stringlist

Details of webserverDOSOptions:

Field Name	Description	Data Type
dosPrevention	DOS prevention: Direction mode	String
maxConnectionAllowedToWS	Max connection allowed to WS	Number
slowConnectionAttackPrevention	Slow connection attack prevention	Boolean
maxHTTPRequestPERSecondTOAnyPath	Max HTTP request per second to any path	Number
websitePathToProtect	Website path to protect options: ALL or SPECIFIC	String
browserDetectionMethod	Browser detection method	String
websitePathToProtectList	Website path to protect list	Objectlist

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
createdResourceId	Policy id	Int

Example

Request

POST https://<NSM_IP>/sdkapi/protectionoptionspolicy/

```
{ "policyName": "httpresponse", "domainId": 0, "visibleToChild": true, "description": "Enable xff",
"isEditable": true, "protectionOptions": { "inspectionOptions": { "httpResponseTrafficScanning":
"INBOUND_AND_OUTBOUND", "chunkedHTTPResponseDecoding": "DISABLED", "htmlEncodedHTTPResponseDecoding":
"DISABLED", "base64SMTPDecoding": "DISABLED", "quotedPrintableSMTPDecoding": "DISABLED",
"msRPCSMBFragmentReassembly": "DISABLED", “msOfficeDeepFileInspection”: “DISABLED”, "xffHeaderParsing":
"DISABLED", "layer7DataCollection": "DISABLED", "passiveDeviceProfiling": "DISABLED",
"attackBlockingSimulation": false }, "advancedBotnetDetectionOptions": { "advancedBotnetDetection": "DISABLED",
"exportTrafficToNTBA": false }, "gtiEndpointReputationAnalysysOptions": { "gtiEndpointReputationAnalysys":
"DISABLED", "useToInfluenceSmartBlocking": false, "excludeInternalEndpoint": false “urlReputationAnalysis”:
“INBOUND_ONLY”, “urlReputationMinimumRisk:”MEDIUM” }, "webserverHuresticAnalysysOptions": { "huresticAnalysys":
"DISABLED" }, "webserverDOSOptions": { "dosPrevention": "DISABLED", "maxConnectionAllowedToWS": 0,
"slowConnectionAttackPrevention": false, "maxHTTPRequestPERSecondTOAnyPath": 0, "clientBrowserDetection":
false } } }
```

Response

```
{ "createdResourceId": 101 }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid domain id

Update Inspection Options Policy

This URL updates the inspection options policy.

Resource URL

PUT /protectionoptionspolicy/<policy_id>

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
policy_id	Policy id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type
policyId	Policy id	Number
policyName	Policy name	String
domainId	Domain id	Number
visibleToChild	Visible to child	Boolean
description	Description	String
protectionOptions	All options tabs	Object

Details of protectionOptions:

Field Name	Description	Data Type
inspectionOptions	Inspection options	Object
advancedBotnetDetectionOptions	Advanced botnet detection options	Object
gtiEndpointReputationAnalysysOptions	GTI endpoint reputation analysis options	Object
webserverHuresticAnalysysOptions	Web server heuristic analysis options	Object
webserverDOSOptions	Web server DoS options	Object

Details of inspectionOptions:

Field Name	Description	Data Type
httpResponseTrafficScanning	HTTP response traffic scanning	String
httpResponseDecompression	HTTP response decompression	String
chunkedHTTPResponseDecoding	Chunked HTTP response decoding	String
htmlEncodedHTTPResponseDecoding	HTML encoded HTTP response decoding	String
base64SMTPDecoding	Base64 SMTP decoding	String
description	Description	String
quotedPrintableSMTPDecoding	Quoted printable SMTP decoding	String
msRPCSMBFragmentReassembly	MSRPC SMB fragment reassembly	String
msOfficeDeepFileInspection	Microsoft Office deep file inspection	String

Field Name	Description	Data Type
`xffHeaderParsing`	XFF header parsing	String
`layer7DataCollection`	Layer 7 data collection	String
`passiveDeviceProfiling`	Passive device profiling	String
`attackBlockingSimulation`	Attack blocking simulation	String

Possible values for above attributes should be:

1. INBOUND_ONLY
2. OUTBOUND_ONLY
3. DISABLED
4. INBOUND_AND_OUTBOUND

Details of advancedBotnetDetectionOptions:

Field Name	Description	Data Type
`advancedBotnetDetection`	Advanced botnet detection	String
`sensitivity`	Sensitivity	String
`fastFluxDetection`	Fast flux detection	String
`domainGenerationAlgorithmDetection`	Domain generation algorithm detection	String
`domainNameAllowlistProcessing`	Domain name allow list processing	String
`exportTrafficToNTBA`	Export traffic to NTBA	Boolean
`dnsSinkHooling`	DNS sink holing	String

Possible values for above attributes should be:

1. INBOUND_ONLY
2. OUTBOUND_ONLY
3. DISABLED
4. INBOUND_AND_OUTBOUND

Possible values for sensitivity should be:

1. LOW
2. MEDIUM
3. HIGH

Details of gtiEndpointReputationAnalysysOptions:

Field Name	Description	Data Type
`gtiEndpointReputationAnalysys`	GTI endpoint reputation analysis • INBOUND_ONLY • OUTBOUND_ONLY • DISABLED • INBOUND_AND_OUTBOUND	String

Field Name	Description	Data Type
`useToInfluenceSmartBlocking`	Use to influence SmartBlocking	Boolean
`excludeInternalEndpoint`	Exclude internal endpoint	Boolean
`cidrsExcluded`	CIDRs excluded	Stringlist
`protocalsExcluded`	Protocols excluded	Stringlist
`urlReputationAnalysis`	URL reputation analysis	String
`urlReputationMinimumRisk`	URL reputation minium risk: **Valid Values:** 1. HIGH 2. MEDIUM	String

Details of webserverHuresticAnalysysOptions:

Field Name	Description	Data Type
`huresticAnalysys`	Heuristic analysis. Direction value as specified above	String
`websitePathToProtect`	Options: ALL or SPECIFIC	String
`blockedTextList`	Blocked text list	Stringlist
`websitePathToProtectList`	Website path to protect list	Stringlist

Details of webserverDOSOptions:

Field Name	Description	Data Type
`dosPrevention`	DoS prevention: direction mode	String
`maxConnectionAllowedToWS`	Max connection allowed to WS	Number
`slowConnectionAttackPrevention`	Slow connection attack prevention	Boolean
`maxHTTPRequestPERSecondTOAnyPath`	max HTTP request per second to any path	Number
`websitePathToProtect`	Website path to protect options: ALL or SPECIFIC	String
`browserDetectionMethod`	Browser detection method	String
`websitePathToProtectList`	Website path to protect list	Objectlist

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Operation status	Int

Example

Request

PUT https://<NSM_IP>/sdkapi/protectionoptionspolicy/1

```
{ "policyId": 1, "policyName": "Default Client and Server Inspection", "domainId": 0, "visibleToChild": true,
"description": "Inspect traffic both from internal endpoints and to exposed Web and mail servers", "isEditable":
false, "lastUpdatedBy": "admin", "lastUpdated": "Jun 25 18:27", "protectionOptions": { "inspectionOptions":
{ "httpResponseTrafficScanning": "OUTBOUND_ONLY", "chunkedHTTPResponseDecoding": "OUTBOUND_ONLY",
"htmlEncodedHTTPResponseDecoding": "OUTBOUND_ONLY", "base64SMTPDecoding": "INBOUND_AND_OUTBOUND",
"quotedPrintableSMTPDecoding": "INBOUND_AND_OUTBOUND", "msRPCSMBFragmentReassembly": "DISABLED",
"msOfficeDeepFileInspection”: “DISABLED", "xffHeaderParsing": "INBOUND_ONLY", "layer7DataCollection":
"INBOUND_AND_OUTBOUND", "passiveDeviceProfiling": "INBOUND_AND_OUTBOUND", "attackBlockingSimulation": false } ,
"advancedBotnetDetectionOptions": { "advancedBotnetDetection": "DISABLED", "exportTrafficToNTBA": false } ,
"gtiEndpointReputationAnalysysOptions": { "gtiEndpointReputationAnalysys": "DISABLED",
"useToInfluenceSmartBlocking": false, "excludeInternalEndpoint": false, "urlReputationAnalysis”: “INBOUND_ONLY",
"urlReputationMinimumRisk:”MEDIUM" } , "webserverHuresticAnalysysOptions": { "huresticAnalysys": "INBOUND_ONLY",
"websitePathToProtect": "ALL", "blockedTextList": [], "websitePathToProtectList": [], } , "webserverDOSOptions":
{ "dosPrevention": "INBOUND_ONLY", "maxConnectionAllowedToWS": 750000, "slowConnectionAttackPrevention": true,
"maxHTTPRequestPERSecondTOAnyPath": 10000, "websitePathToProtect": "ALL", "clientBrowserDetection": true,
"browserDetectionMethod": "HTML_CHALLENGE", "websitePathToProtectList": [], } } }
```

Response

```
{ "status":1 }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid domain id

Delete Inspection Options Policy

This URL deletes the inspection options policy.

Resource URL

DELETE /protectionoptionspolicy/<policy_id>

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
`policy_id`	Policy id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Operation status	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/protectionoptionspolicy/1

Response

```
{ "status":1 }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid domain id

Get the DXL Integration Configuration for Domain

This URL retrieves the DXL integration configuration for domain.

Resource URL

GET /domain/<domain_id>/dxlintegration

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`inheritSettings`	Inherit settings from parent domain	Boolean
`enableDXL`	DXL is enabled or not	Boolean

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/dxlintegration

Response

```
{ "inheritSettings": true, "enableDXL": true }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Update the DXL Integration Configuration for Domain

This URL updates the DXL integration configuration for domain.

Resource URL

PUT /domain/<domain_id>/dxlintegration

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`inheritSettings`	Inherit settings from parent domain	Boolean	Yes
`enableDXL`	DXL should be enabled or not	Boolean	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/ domain/0/dxlintegration

Payload

```
{ "inheritSettings": true, "enableDXL": true }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	9101	Cannot inherit settings for parent domain
3	400	1001	McAfee ePO configuration is required to enable DXL service

Get the DXL Integration Configuration for Sensor

This URL retrieves the DXL integration configuration for Sensor.

Resource URL

GET /sensor/<sensor_id>/ dxlintegration

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`inheritSettings`	Inherit settings from parent domain	Boolean
`enableDXL`	DXL enable or not	Boolean
`epoServerIporName`	McAfee ePO server IP	String
`epoServerPort`	McAfee ePO server port. Default is 8443	Number
`epoUsername`	McAfee ePO username	String
`epoPassword`	McAfee ePO password	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/dxlintegration

Response

```
{ "inheritSettings": false, "enableDXL": true, "epoServerIporName": "10.213.169.206", "epoServerPort": 8443,
"epoUsername": "admin", "epoPassword": "admin123" }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1106	Invalid Sensor
2	404	1124	The Sensor is inactive
3	404	9201	DXL integration supported only for NS and Virtual IPS Sensors having software version greater than or equal to 9.1

Update the DXL Integration Configuration for Sensor

This URL updates the DXL integration configuration for Sensor.

Resource URL

PUT /sensor/<sensor_id>/dxlintegration

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`inheritSettings`	Inherit settings from parent domain	Boolean	Yes
`enableDXL`	DXL enable or not	Boolean	No
`epoServerIporName`	McAfee ePO server IP	String	No
`epoServerPort`	McAfee ePO server port. Default is 8443	Number	No
`epoUsername`	McAfee ePO username	String	No
`epoPassword`	McAfee ePO password	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1001/dxlintegration

Payload

```
{ "inheritSettings": false, "enableDXL": true, "epoServerIporName": "10.213.169.206", "epoServerPort": 8443,
"epoUsername": "admin", "epoPassword": "admin123" }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1106	Invalid Sensor
2	404	1124	The Sensor is inactive
3	404	9201	DXL integration supported only for NS and Virtual Sensors having software version greater than or equal to 9.1

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
4	400	9102	McAfee ePO server IP address, username and password are mandatory
5	400	9103	McAfee ePO server username can contain space, numbers, alphabets and special characters '_-.\\'
6	400	9104	McAfee ePO server password should be less than 64

Get the Threat Explorer Data

This URL retrieves the threat explorer data.

Resource URL

GET /domain/<domain_id>/threatexplorer/alerts/TopN/<count>/direction/<direction>/duration/<duration>?includeChildDomain=<includeChildDomain>&&action=<action>&&value=<value>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes
`count`	Number of top attacks to display. Values allowed are: 5,10,15,20 or 25	Boolean	No
`direction`	Direction of the attack. Values allowed are: ANY, INBOUND & OUTBOUND	String	No
`duration`	Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	Yes
`includeChildDomain`	Include the child domains. Default is true	Boolean	No
`action`	Should the data be filtered or grouped. Values allowed are: • Group(default) • Filter	String	No
`value`	If action is group, then there is no need of any data, default value is an empty string If the action is filter. We can give multiple filters separated by ":::". The format of value will be <filter_name1>=<filter_value>:::<filter_name2>=<filter_value> .	String	No

Field Name	Description	Data Type	Mandatory
	The filter_name's and filter_values allowed are: • attack -> value should be a valid attack name. • severity -> value can be High, Low, Medium & Informational (all are case sensitive). • category -> value should be a valid category. • subCategory -> value should be a valid sub category. • attackerIp -> value should be a valid IP. • dnsName -> value should be a string. • country -> value should be a valid country name. • user -> value should be a valid user name/unknown. • victimIp -> value should be a valid IP. • victimDnsName -> value should be a string. • victimCountry -> value should be a valid country name. • victimUser -> value should be a valid user name/unknown. • applicationName -> value should be a valid application name. • applicationRisk -> value can be high, low & medium. • applicationCategory -> value should be a valid application category. • fileHash -> value should be a string. • executableHash -> value should be a string. • malwareConfidence -> value should be a valid malware confidence. • fileSize -> value should be a number. • executableConfidence -> value can be clean, high, low, medium, unknown, veryhigh & verylow. • executableClassification -> value can be block, none,		

Field Name	Description	Data Type	Mandatory
	unclassified, and allow. • executableName		

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`ThreatExplorerData`	List of top attacks	Objectlist

Details of fields in ThreatExplorerData:

Field Name	Description	Data Type
topAttacks	List of all the top attacks. The data is same as TE top attacks explained in 1.2.3	Object
topAttackers	List of all the top attackers. The data is same as TE top attackers explained in 1.3.3	Object
topTargets	List of all the top targets. The data is same as TE top targets explained in 1.4.3	Object
topAttackApplications	List of all the top attack applications. The data is same as TE top attack applications explained in 1.5.3	Object
topAttackExecutables	List of all the top executables. The data is same as TE top executables explained in 1.7.3	Object
topMalware	List of all the top malwares. The data is same as TE top malware downloads explained in 1.6.3	Object

Example

Request

GET https:// <NSM_IP>/sdkapi/domain/0/threatexplorer/alerts/TopN/10/direction/ANY/duration/LAST_12_HOURS?action=filter&&value=malwareConfidence=Very High:::country=Thailand

Response

```
{ "topAttacks": { "TETopAttacksList": [ { "attackName": "MALWARE: Malicious File detected by Mcafee Cloud
Service - Mobile Engine", "attackCategory": "Malware", "attackSubcategory": "McAfee-Cloud", "attackSeverity":
"High", "attackCount": 4 } ] }, "topAttackers": { "TETopAttackersList": [ { "attackerIP": "1.1.223.9",
"attackerDNSName": "node-irt.pool-1-1.dynamic.totbb.net.", "attackerCountry": "Thailand", "attackerUser":
"Unknown", "attackCount": 2 }, { "attackerIP": "1.1.223.10", "attackerDNSName": "node-
iru.pool-1-1.dynamic.totbb.net.", "attackerCountry": "Thailand", "attackerUser": "Unknown", "attackCount":
2 } ] }, "topTargets": { "TETopTargetsList": [ { "targetIP": "1.1.223.9", "targetDNSName": "node-
irt.pool-1-1.dynamic.totbb.net.", "targetCountry": "Thailand", "targetUser": "Unknown", "attackCount": 2 },
{ "targetIP": "1.1.223.10", "targetDNSName": "node-iru.pool-1-1.dynamic.totbb.net.", "targetCountry":
"Thailand", "targetUser": "Unknown", "attackCount": 2 } ] }, "topAttackApplications":
{ "TETopAttackApplicationsList": [ { "applicationName": "SMTP", "applicationRisk": "High",
"applicationCategory": "Email", "attackCount": 2 }, { "applicationName": "HTTP", "applicationRisk": "Low",
"applicationCategory": "Infrastructure Services", "attackCount": 2 } ] }, "topAttackExecutables": { },
"topMalware": { "TETopMalwareDownloadsList": [ { "malwareFileHash": "f70664bb0d45665e79ba9113c5e4d0f4",
"malwareConfidence": "Very High", "malwareFileSizeInBytes": "314445", "attackCount": 4 } ] } }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	404	4201	Invalid duration filter

Get the List of Top Attacks

This URL retrieves the list of top attacks.

Resource URL

GET /domain/<domain_id>/threatexplorer/alerts/TopN/<count>/direction/<direction>/duration/<duration>/attacks?includeChildDomain=<includeChildDomain>&&action=<action>&&value=<value>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes
`count`	Number of top attacks to display. Values allowed are: 5,10,15,20 or 25	Boolean	No
`direction`	Direction of the attack. Values allowed are: ANY, INBOUND & OUTBOUND	String	No
`duration`	Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	Yes
`includeChildDomain`	Include the child domains. Default is true	Boolean	No
`action`	Should the data be filtered or grouped. Values allowed are: • Group(default) • Filter	String	No
`value`	If action is group, the values allowed are: • attack (default)	String	No

Field Name	Description	Data Type	Mandatory
	• severity • category • subCategory If the action is filter. We can give multiple filters separated by ":::". The format of value will be <filter_name1>=<filter_value>::: <filter_name2>=<filter_value> . The filter_name's and filter_values allowed are: • attack -> value should be a valid attack name. • severity -> value can be High, Low, Medium & Informational (all are case sensitive). • category -> value should be a valid category. • subCategory -> value should be a valid sub category. • attackerIp -> value should be a valid IP. • dnsName -> value should be a string. • country -> value should be a valid country name. • user -> value should be a valid user name/unknown. • victimIp -> value should be a valid IP. • victimDnsName -> value should be a string. • victimCountry -> value should be a valid country name. • victimUser -> value should be a valid user name/unknown. • applicationName -> value should be a valid application name. • applicationRisk -> value can be high, low & medium. • applicationCategory -> value should be a valid application category. • fileHash -> value should be a string. • executableHash -> value should be a string. • malwareConfidence -> value should be a valid malware confidence.		

Field Name	Description	Data Type	Mandatory
	• fileSize -> value should be a number. • executableConfidence -> value can be clean, high, low, medium, unknown, veryhigh & verylow. • executableClassification -> value can be block, none, unclassified, and allow. • executableName		

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`TETopAttacks`	List of top attacks. Contains TE top attacks list	Object

Details of fields in TETopAttacksList:

Field Name	Description	Data Type
`attackName`	Name of the attack	String
`attackCategory`	Category of the attack	String
`attackSubcategory`	Sub category of the attack	String
`attackSeverity`	Severity of the attack	String
`attackCount`	Numbers of the attack	Number

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/threatexplorer/alerts/TopN/10/direction/ANY/duration/LAST_12_HOURS/attacks?action=filter&&value=malwareConfidence=Very High

Response

```
{ "TETopAttacksList": [ { "attackName": "MALWARE: Malicious File detected by Mcafee Cloud Service - Mobile
Engine", "attackCategory": "Malware", "attackSubcategory": "McAfee-Cloud", "attackSeverity": "High",
"attackCount": 4 } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	3707	Top count should be 5,10,15,20 or 25
3	400	3702	Invalid action

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
4	400	3701	Invalid "GroupBy" string specified
5	400	3704	Invalid filters specified
6	400	3703	Invalid direction
7	400	3601	Invalid duration

Get the List of Top Attackers

This URL retrieves the list of top attackers.

Resource URL

GET /domain/<domain_id>/threatexplorer/alerts/TopN/<count>/direction/<direction>/duration/<duration>/attackers?includeChildDomain=<includeChildDomain>&&action=<action>&&value=<value>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes
`count`	Number of top attacks to display. Values allowed are: 5,10,15,20 or 25	Boolean	No
`direction`	Direction of the attack. Values allowed are: ANY, INBOUND & OUTBOUND	String	No
`duration`	Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	Yes
`includeChildDomain`	Include the child domains. Default is true	Boolean	No
`action`	Should the data be filtered or grouped. Values allowed are: • Group(default) • Filter	String	No

Field Name	Description	Data Type	Mandatory
`value`	If action is group, the values allowed are: • attackerIp (default) • dnsName • country • user If the action is filter. We can give multiple filters separated by ":::". The format of value will be <filter_name1>=<filter_value>:::<filter_name2>=<filter_value> . The filter_name's and filter_values allowed are: • attack -> value should be a valid attack name. • severity -> value can be High, Low, Medium & Informational (all are case sensitive). • category -> value should be a valid category. • subCategory -> value should be a valid sub category. • attackerIp -> value should be a valid IP. • dnsName -> value should be a string. • country -> value should be a valid country name. • user -> value should be a valid user name/unknown. • victimIp -> value should be a valid IP. • victimDnsName -> value should be a string. • victimCountry -> value should be a valid country name. • victimUser -> value should be a valid user name/unknown. • applicationName -> value should be a valid application name. • applicationRisk -> value can be high, low & medium. • applicationCategory -> value should be a valid application category. • fileHash -> value should be a string. • executableHash -> value should be a string.	String	No

Field Name	Description	Data Type	Mandatory
	• malwareConfidence -> value should be a valid malware confidence. • fileSize -> value should be a number. • executableConfidence -> value can be clean, high, low, medium, unknown, veryhigh & verylow. • executableClassification -> value can be block, none, unclassified, and allow. • executableName		

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`TETopAttackers`	List of top attackers. Contains TE top attackers list	Object

Details of fields in TETopAttackersList:

Field Name	Description	Data Type
`attackerIP`	IP of the attacker	String
`attackerDNSName`	DNS name of the attacker	String
`attackerCountry`	Country of the attacker	String
`attackerUser`	Attacker	String
`attackCount`	Numbers of the attack	Number

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/threatexplorer/alerts/TopN/10/direction/ANY/duration/LAST_12_HOURS/attackers?action=filter&&value=malwareConfidence=Very High:::country=Thailand

Response

```
{ "TETopAttackersList": [ { "attackerIP": "1.1.223.9", "attackerDNSName": "node-
irt.pool-1-1.dynamic.totbb.net.", "attackerCountry": "Thailand", "attackerUser": "Unknown", "attackCount": 2 },
{ "attackerIP": "1.1.223.10", "attackerDNSName": "node-iru.pool-1-1.dynamic.totbb.net.", "attackerCountry":
"Thailand", "attackerUser": "Unknown", "attackCount": 2 } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
2	400	3707	Top count should be 5,10,15,20 or 25
3	400	3702	Invalid action
4	400	3701	Invalid "GroupBy" string specified
5	400	3704	Invalid filters specified
6	400	3703	Invalid direction
7	400	3601	Invalid duration

Get the List of Top Targets

This URL retrieves the list of top targets.

Resource URL

GET /domain/<domain_id>/threatexplorer/alerts/TopN/<count>/direction/<direction>/duration/<duration>/targets?includeChildDomain=<includeChildDomain>&&action=<action>&&value=<value>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes
`count`	Number of top attacks to display. Values allowed are: 5,10,15,20 or 25	Boolean	No
`direction`	Direction of the attack. Values allowed are: ANY, INBOUND & OUTBOUND	String	No
`duration`	Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	Yes
`includeChildDomain`	Include the child domains. Default is true	Boolean	No
`action`	Should the data be filtered or grouped.	String	No

Field Name	Description	Data Type	Mandatory
	Values allowed are: • Group(default) • Filter		
`value`	If action is group, the values allowed are: • victimIp(default) • victimDnsName • victimCountry • victimUser If the action is filter. We can give multiple filters separated by ":::". The format of value will be <filter_name1>=<filter_value>:::<filter_name2>=<filter_value> . The filter_name's and filter_values allowed are: • attack -> value should be a valid attack name. • severity -> value can be High, Low, Medium & Informational (all are case sensitive). • category -> value should be a valid category. • subCategory -> value should be a valid sub category. • attackerIp -> value should be a valid IP. • dnsName -> value should be a string. • country -> value should be a valid country name. • user -> value should be a valid user name/unknown. • victimIp -> value should be a valid IP. • victimDnsName -> value should be a string. • victimCountry -> value should be a valid country name. • victimUser -> value should be a valid user name/unknown. • applicationName -> value should be a valid application name. • applicationRisk -> value can be high, low & medium. • applicationCategory -> value should be a	String	No

Field Name	Description	Data Type	Mandatory
	valid application category. • fileHash -> value should be a string. • executableHash -> value should be a string. • malwareConfidence -> value should be a valid malware confidence. • fileSize -> value should be a number. • executableConfidence -> value can be clean, high, low, medium, unknown, veryhigh & verylow. • executableClassification -> value can be block, none, unclassified, and allow. • executableName		

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`TETopTargets`	List of top targets. Contains TE top targets list	Object

Details of fields in TETopTargetsList:

Field Name	Description	Data Type
`targetIP`	IP of the target	String
`targetDNSName`	DNS name of the target	String
`targetCountry`	Country of the target	String
`targetUser`	Target user	String
`attackCount`	Numbers of the attack	Number

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/threatexplorer/alerts/TopN/10/direction/ANY/duration/LAST_12_HOURS/targets?action=filter&&value=malwareConfidence=Very High:::country=Thailand

Response

```
{ "TETopTargetsList": [ { "targetIP": "1.1.223.9", "targetDNSName": "node-irt.pool-1-1.dynamic.totbb.net.",
"targetCountry": "Thailand", "targetUser": "Unknown", "attackCount": 2 }, { "targetIP": "1.1.223.10",
"targetDNSName": "node-iru.pool-1-1.dynamic.totbb.net.", "targetCountry": "Thailand", "targetUser": "Unknown",
"attackCount": 2 } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	3707	Top count should be 5,10,15,20 or 25
3	400	3702	Invalid action
4	400	3701	Invalid "GroupBy" string specified
5	400	3704	Invalid filters specified
6	400	3703	Invalid direction
7	400	3601	Invalid duration

Get the List of Top Attack Applications

This URL retrieves the list of top attack applications.

Resource URL

GET /domain/<domain_id>/threatexplorer/alerts/TopN/<count>/direction/<direction>/duration/<duration>/attack_applications?includeChildDomain=<includeChildDomain>&&action=<action>&&value=<value>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes
`count`	Number of top attacks to display. Values allowed are: 5,10,15,20 or 25	Boolean	No
`direction`	Direction of the attack. Values allowed are: ANY, INBOUND & OUTBOUND	String	No
`duration`	Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	Yes
`includeChildDomain`	Include the child domains. Default is true	Boolean	No

Field Name	Description	Data Type	Mandatory
`action`	Should the data be filtered or grouped. Values allowed are : • group(default) • filter	String	No
`value`	If action is group, the values allowed are: • applicationName(default) • applicationRisk • applicationCategory If the action is filter. We can give multiple filters separated by ":::". The format of value will be <filter_name1>=<filter_value>:::<filter_name2>=<filter_value> . The filter_name's and filter_values allowed are: • attack -> value should be a valid attack name. • severity -> value can be High, Low, Medium & Informational (all are case sensitive). • category -> value should be a valid category. • subCategory -> value should be a valid sub category. • attackerIp -> value should be a valid IP. • dnsName -> value should be a string. • country -> value should be a valid country name. • user -> value should be a valid user name/unknown. • victimIp -> value should be a valid IP. • victimDnsName -> value should be a string. • victimCountry -> value should be a valid country name. • victimUser -> value should be a valid user name/unknown. • applicationName -> value should be a valid application name. • applicationRisk -> value can be high, low & medium.	String	No

Field Name	Description	Data Type	Mandatory
	• applicationCategory -> value should be a valid application category. • fileHash -> value should be a string. • executableHash -> value should be a string. • malwareConfidence -> value should be a valid malware confidence. • fileSize -> value should be a number. • executableConfidence -> value can be clean, high, low, medium, unknown, veryhigh & verylow. • executableClassification -> value can be block, none, unclassified, and allow. • executableName		

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`TETopAttackApplications`	List of top attack applications. Contains TE top attack applications list	Object

Details of fields in TETopAttackApplicationsLists:

Field Name	Description	Data Type
`applicationName`	Name of the application used in the attack	String
`applicationRisk`	Risk level of the application	String
`applicationCategory`	Category of the attack application	String
`attackCount`	Numbers of the attack	Number

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/threatexplorer/alerts/TopN/10/direction/ANY/duration/LAST_12_HOURS/attack_applications?action=filter&&value=malwareConfidence=Very High:::country=Thailand

Response

```
{ "TETopAttackApplicationsList": [ { "applicationName": "SMTP", "applicationRisk": "High",
"applicationCategory": "Email", "attackCount": 2 }, { "applicationName": "HTTP", "applicationRisk": "Low",
"applicationCategory": "Infrastructure Services", "attackCount": 2 } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	3707	Top count should be 5,10,15,20 or 25
3	400	3702	Invalid action
4	400	3701	Invalid "GroupBy" string specified
5	400	3704	Invalid filters specified
6	400	3703	Invalid direction
7	400	3601	Invalid duration

Get the List of Top Malwares

This URL retrieves the list of top malwares.

Resource URL

GET /domain/<domain_id>/threatexplorer/alerts/TopN/<count>/direction/<direction>/duration/<duration>/malware?includeChildDomain=<includeChildDomain>&&action=<action>&&value=<value>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes
`count`	Number of top attacks to display. Values allowed are: 5,10,15,20 or 25	Boolean	No
`direction`	Direction of the attack. Values allowed are: ANY, INBOUND & OUTBOUND	String	No
`duration`	Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	Yes
`includeChildDomain`	Include the child domains. Default is true	Boolean	No

Field Name	Description	Data Type	Mandatory
`action`	Should the data be filtered or grouped. Values allowed are: • Group(default) • Filter	String	No
`value`	If action is group, the values allowed are: • fileHash (default) • malwareConfidence • fileSize If the action is filter. We can give multiple filters separated by ":::". The format of value will be <filter_name1>=<filter_value>:::<filter_name2>=<filter_value> . The filter_name's and filter_values allowed are: • attack -> value should be a valid attack name. • severity -> value can be High, Low, Medium & Informational (all are case sensitive). • category -> value should be a valid category. • subCategory -> value should be a valid sub category. • attackerIp -> value should be a valid IP. • dnsName -> value should be a string. • country -> value should be a valid country name. • user -> value should be a valid user name/unknown. • victimIp -> value should be a valid IP. • victimDnsName -> value should be a string. • victimCountry -> value should be a valid country name. • victimUser -> value should be a valid user name/unknown. • applicationName -> value should be a valid application name. • applicationRisk -> value can be high, low & medium.	String	No

Field Name	Description	Data Type	Mandatory
	• applicationCategory -> value should be a valid application category. • fileHash -> value should be a string. • executableHash -> value should be a string. • malwareConfidence -> value should be a valid malware confidence. • fileSize -> value should be a number. • executableConfidence -> value can be clean, high, low, medium, unknown, veryhigh & verylow. • executableClassification -> value can be block, none, unclassified, and allow. • executableName		

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`TETopMalware`	List of top malwares. Contains TE top malware downloads list	Object

Details of fields in TETopMalwareDownloadsList:

Field Name	Description	Data Type
`malwareFileHash`	Malware hash value	String
`malwareConfidence`	Confidence level of malware	String
`malwareFileSizeInBytes`	Size of malware file	String
`attackCount`	Numbers of the attack	Number

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/threatexplorer/alerts/TopN/10/direction/ANY/duration/LAST_12_HOURS/malware?action=filter&&value=malwareConfidence=Very High:::country=Thailand

Response

```
{ "TETopMalwareDownloadsList": [ { "malwareFileHash": "f70664bb0d45665e79ba9113c5e4d0f4", "malwareConfidence":
"Very High", "malwareFileSizeInBytes": "314445", "attackCount": 4 } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	3707	Top count should be 5,10,15,20 or 25
3	400	3702	Invalid action
4	400	3701	Invalid "GroupBy" string specified
5	400	3704	Invalid filters specified
6	400	3703	Invalid direction
7	400	3601	Invalid duration

Get the List of Top Executables

This URL retrieves the list of top executables.

Resource URL

GET /domain/<domain_id>/threatexplorer/alerts/TopN/<count>/direction/<direction>/duration/<duration>/executables?includeChildDomain=<includeChildDomain>&&action=<action>&&value=<value>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes
`count`	Number of top attacks to display. Values allowed are: 5,10,15,20 or 25	Boolean	No
`direction`	Direction of the attack. Values allowed are: ANY, INBOUND & OUTBOUND	String	No
`duration`	Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	Yes
`includeChildDomain`	Include the child domains. Default is true	Boolean	No

Field Name	Description	Data Type	Mandatory
`action`	Should the data be filtered or grouped. Values allowed are: • Group(default) • Filter	String	No
`value`	If action is group, the values allowed are: • ExecutableHash(default) • ExecutableConfidence • ExecutableClassification • ExecutableName If the action is filter. We can give multiple filters separated by ":::". The format of value will be <filter_name1>=<filter_value>::: <filter_name2>=<filter_value> . The filter_name's and filter_values allowed are: • attack -> value should be a valid attack name. • severity -> value can be High, Low, Medium & Informational (all are case sensitive). • category -> value should be a valid category. • subCategory -> value should be a valid sub category. • attackerIp -> value should be a valid IP. • dnsName -> value should be a string. • country -> value should be a valid country name. • user -> value should be a valid user name/unknown. • victimIp -> value should be a valid IP. • victimDnsName -> value should be a string. • victimCountry -> value should be a valid country name. • victimUser -> value should be a valid user name/unknown. • applicationName -> value should be a valid application name. • applicationRisk -> value can be high, low & medium.	String	No

Field Name	Description	Data Type	Mandatory
	• applicationCategory -> value should be a valid application category. • fileHash -> value should be a string. • executableHash -> value should be a string. • malwareConfidence -> value should be a valid malware confidence. • fileSize -> value should be a number. • executableConfidence -> value can be clean, high, low, medium, unknown, veryhigh & verylow. • executableClassification -> value can be block, none, unclassified, and allow. • executableName		

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`TETopExecutables`	List of top executables. Contains TE top executables list	Object

Details of fields in TETopMalwareDownloadsList:

Field Name	Description	Data Type
`executableHash`	Executable hash value	String
`executableConfidence`	Confidence level of executable	String
`executableName`	Name of the executable	String
`executableClassification`	Classification of the executable	String
`attackCount`	Numbers of the attack	Number

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/threatexplorer/alerts/TopN/10/direction/ANY/duration/LAST_12_HOURS/executables?action=filter&&value=executableConfidence=veryLow

Response

```
{ "TETopExecutablesList": [ { "executableHash": "6691f88cbd9122d990fe9e17197e2771", "executableConfidence":
"veryLow", "executableName": "BitTorrent.exe", "executableClassification": "Allowed", "attackCount": 327 },
{ "executableHash": "fb104d17018b4ca9f0c1a9bed02d15fc", "executableConfidence": "veryLow", "executableName":
"firefox.exe", "executableClassification": "Allowed", "attackCount": 13 }, { "executableHash":
"f71d97b6b631d565af7c6e0bdf9d49f4", "executableConfidence": "veryLow", "executableName": "IEXPLORE.EXE.MUI",
"executableClassification": "Allowed", "attackCount": 6 }, { "executableHash":
```

"bcd9cbf0621f9a6767276a2e0bf1dd15", "executableConfidence": "veryLow", "executableName": "googletalk.exe", "executableClassification": "Allowed", "attackCount": 5 }] }

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	3707	Top count should be 5,10,15,20 or 25
3	400	3702	Invalid action
4	400	3701	Invalid "GroupBy" string specified
5	400	3704	Invalid filters specified
6	400	3703	Invalid direction
7	400	3601	Invalid duration

Get Host Summary

This URL retrieves the host analysis summary for given IP address for the time frame.

Resource URL

GET /networkforensics/<ipaddress>?startime=<start_time>&&duration=<duration>&&ntba=<ntba_id>

URL Parameters: **ipaddress**

Query Parameter1: **starttime=**

Date in the format yyyy-MM-dd HH:mm

Query Parameter 2: **duration**=

- NEXT_60_SECONDS
- NEXT_5_MINUTES
- NEXT_60_MINUTES
- NEXT_30_MINUTES

Query Parameter 3: **ntba id**

Request Parameters

Query Request Parameters:

Field Name	Description	Data Type	Mandatory
`starttime`	Start time for analysis	String	No
`duration`	Duration	String	No
`Ntba_id`	NTBA id	Number	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
NetworkForensicsSummary	Summary of IP address	Object

Details of fields in NetworkForensicsSummary:

Field Name	Description	Data Type
`endpointSummary`	Endpoint summary	Object
`ClientConnections`	Client connections	Object
`ServerConnections`	Server connections	Object

Details of fields in endpointSummary:

Field Name	Description	Data Type
ipAddress	IP address	String
analysisWindow	Analysis window	String

Field Name	Description	Data Type
zone	Zone	String
country	Country	String
etf	Etf	String
dataSource	Data source	String

Details of fields in ClientConnections:

Field Name	Description	Data Type
`connections`	Connections	String
`applications`	Applications	String
`endpointExecutables`	Endpoint executables	String
`tcpServices`	Server connections	String
`tcpHighPorts`	Tcp high ports	String
`udpServices`	Udp services	String
`udpHighPorts`	Udp high ports	String

Details of ServerConnections:

Field Name	Description	Data Type
`connections`	Connections	String
`applications`	Applications	String
`tcpServices`	TCP services	String
`tcpHighPorts`	TCP high ports	String
`udpServices`	UDP services	String
`udpHighPorts`	UDP high ports	String

Example

Request

GET https://<NSM_IP>/sdkapi/networkforensics /1.1.1.1/?duration=NEXT_30_MINUTES&&starttime=2012-APR-20 12:15&ntba=1001

Response

```
{ " endpointSummary ": { " analysisWindow ": "", " zone ": "South", " country ": "India", " dataSource ":
"Allowed", " ipAddress ": “” } " ClientConnections ": { " connections ": "10-Aug-2014 12:00", " applications ":
"", " endpointExecutables ": "BitTorrent.exe" } " ServerConnections ": { " connections ": "10-Aug-2014 12:00", "
applications ": "", } }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	5000	Invalid IP address

Get Top Suspicious Flows

This URL retrieves the top suspicious flows for the given IP address.

Resource URL

GET /networkforensics/<ipaddress>/suspiciousflows ?startime=<start_time>&&duration=<duration>&&ntba=<ntba_id>

URL Parameters: **ipaddress**

Query Parameter1: **starttime=**

Date in the format yyyy-MM-dd HH:mm

Query Parameter 2: **duration**=

- NEXT_60_SECONDS
- NEXT_5_MINUTES
- NEXT_60_MINUTES
- NEXT_30_MINUTES

Query Parameter 3: **ntba id**

Request Parameters

Query Request Parameters:

Field Name	Description	Data Type	Mandatory
`starttime`	Start time for analysis	String	No
`duration`	Duration	String	No
`Ntba_id`	NTBA id	Number	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`TopConversations`	Top conversations	Object

Details of fields in TopConversations:

Field Name	Description	Data Type
`time`	Time	String
`suspciousActivity`	Suspicious activity	String
`sourceEndpoint`	Source host	String

Field Name	Description	Data Type
sourcePort	Source port	Number
sourceEcecutable	Source executable name	String
destinationEndpoint	Destination endpoint	String
destinationPort	Destination port	Number
applications	Application names	String
attackName	Attack name	String
attackResult	Attack result	String
fileOrUrlAccessed	File or URL accessed	String

Example

Request

GET https://<NSM_IP>/sdkapi/networkforensics /1.1.1.1/ suspiciousflows?duration=NEXT_30_MINUTES&&starttime=2012-APR-20 12:15&ntba=1001

Response

```
{ "suspciousFlows": [ { " time ": "10-Aug-2014 12:00", " suspciousActivity ": "", " sourceEcecutable ":
"BitTorrent.exe", "executableClassification": "Allowed", "attackName": “” } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	4301	Invalid duration
2	400	4302	Invalid time format
3	400	5000	Invalid IP address

Get the Gateway Anti-Malware Updating Configuration for Domain

This URL retrieves the Gateway Anti-Malware updating configuration for domain.

Resource URL

GET /domain/<domain_id>/gamupdatesettings

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`inheritSettings`	Inherit settings from parent domain	Boolean
`enableAutoUpdate`	Enable automatic update of Gateway Anti-Malware	Boolean
`updateInterval`	Time interval of next update	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/gamupdatesettings

Response

```
{ "inheritSettings": false, "enableAutoUpdate": false, "updateInterval": "6 hrs" }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Update the Gateway Anti-Malware Updating Configuration for Domain

This URL updates the Gateway Anti-Malware updating configuration for domain.

Resource URL

PUT /domain/<domain_id>/gamupdatesettings

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`inheritSettings`	Inherit settings from parent domain	Boolean	Yes
`enableAutoUpdate`	Enable automatic update of Gateway Anti-Malware	Boolean	Yes
`updateInterval`	Time interval of next update	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/gamupdatesettings

Payload

```
{ "inheritSettings": false, "enableAutoUpdate": false, "updateInterval": "6 hrs" }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	9101	Cannot inherit settings for parent domain
3	400	9302	Gateway Anti-Malware update time interval should be one of the following : ["1.5 hrs", "3 hrs", "6 hrs", "12 hrs", "24 hrs"]

Get the Gateway Anti-Malware Updating Configuration for Sensor

This URL retrieves the Gateway Anti-Malware updating configuration for Sensor.

Resource URL

GET /sensor/<sensor_id>/gamupdatesettings

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`inheritSettings`	Inherit settings from parent domain	Boolean
`enableAutoUpdate`	Enable automatic update of Gateway Anti-Malware	Boolean
`updateInterval`	Time interval of next update	String
`lastUpdate`	Last update on the Sensor	String
`GAM_DAT_VERSION`	Version: Latest and active version of Gateway Anti-Malware DAT on Sensor	Object
`GAM_ENGINE_VERSION`	Version: Latest and active version of Gateway Anti-Malware engine on Sensor	Object
`AV_DAT_VERSION`	Version: Latest and active version of AV DAT on Sensor	Object
`ANTI_MALWARE_ENGINE_VERSION`	Version: Latest and active version of Anti-Malware engine on Sensor	Object

Details of Version:

Field Name	Description	Data Type
`activeVersion`	Active version on the Sensor	String
`latestVersion`	Latest version available	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/gamupdatesettings

Response

```
{ "inheritSettings": false, "enableAutoUpdate": false, "updateInterval": "6.0 hrs", "lastUpdate": "Sat Jan 17
14:34:39 IST 1970", "GAM_DAT_VERSION": { "activeVersion": "3177", "latestVersion": "3185" },
"GAM_ENGINE_VERSION": { "activeVersion": "7001.1302.1842 ", "latestVersion": "7001.1302.1842" },
"AV_DAT_VERSION": { "activeVersion": "7607", "latestVersion": "7611" }, "ANTI_MALWARE_ENGINE_VERSION":
{ "activeVersion": "5600", "latestVersion": "5600" } }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1106	Invalid Sensor
2	400	1124	The Sensor is inactive
3	400	9301	Gateway Anti-Malware update is not supported on this Sensor

Update the Gateway Anti-Malwares Updating Configuration for Sensor

This URL updates the Gateway Anti-Malware updating configuration for Sensor.

Resource URL

PUT /sensor/<sensor_id>/gamupdatesettings

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`inheritSettings`	Inherit settings from parent domain	Boolean	Yes
`enableAutoUpdate`	Enable automatic update of Gateway Anti-Malware	Boolean	Yes
`updateInterval`	Time interval of next update	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1001/gamupdatesettings

Payload

```
{ "inheritSettings": false, "enableAutoUpdate": false, "updateInterval": "6 hrs" }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1106	Invalid Sensor
2	404	1124	The Sensor is inactive
3	400	9301	GAM update is not supported on this Sensor
4	400	9302	GAM update time interval should be one of the following : ["1.5 hrs", "3 hrs", "6 hrs", "12 hrs", "24 hrs"]

Get the User Details

These URL's retrieve the details of the user with the user id passed as parameter.

Resource URL

GET /user/ {userId}:

This URL is to retrieve the details of user with the given user id.

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`userId`	Unique identifier of an user	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`userCredentials`	This field contains the user id and password details of the user	Object
`userDetails`	This field contains general details like name, contact etc. for a user.	Object
`roleAssignment`	This field contains the details about the domain and role.	Object
`dashBoardAssignment`	This field contains the details of the dash boards assigned to the user.	Object

Details of userCredentials:

Field Name	Description	Data Type
`loginID`	Unique identifier for a user.	String
`password`	Secret key required to login. Its value will not be visible as it is confidential and should only be known to the user.	String

Details of userDetails:

Field Name	Description	Data Type
`firstAndLastName`	First and last name of the user	String
`email`	Email address of the user	String
`company`	Company of the user	String

Field Name	Description	Data Type
`phone`	Contact number of the user	String
`address`	Address of the user	Object
`state`	State to which the user belongs to	String
`country`	Country to which the user belongs to	String

Details of address:

Field Name	Description	Data Type
`address1`	Address line 1. Containing one segment of the users address.	String
`address2`	Address line 2. Containing other segment of the users address.	String

Details of roleAssignment:

Field Name	Description	Data Type
`domainId`	The domain in which the user was created.	String
`role`	This field contains the information regarding the role assigned to the user. It can have any value from the list of roles already defined in the Manager, i.e. • ePO dashboard data retriever • NOC operator • Report generator • Security expert • Super user • System administrator • No role **Note:** In addition to the above mentioned roles, the user can also be assigned a custom created role.	String

Details of dashBoardAssignment:

Field Name	Description	Data Type
`dashBoardList`	List of all the dashboards to be assigned to user	Array

Example

Request

GET https://<NSM_IP>/sdkapi/user/1

Response

```
{ "userCredentials": { "loginID": "admin", "password": "" }, "userDetails": { "firstAndLastName":
"Administrator", "email": "Administrator Email", "company": "", "phone": "", "address": { "address1": "",
"address2": "" }, "state": "", "country": "" }, "roleAssignment": { "domainId": 0, "role": "Super User" },
"dashBoardAssignment": { "dashBoardList": ["Dashboard_1","Dashboard_2"] } }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	5110	Invalid user id

Create a User

Creates a new user resource.

Resource URL

POST /user

Request Parameters

Payload Request Parameters:

Field Name	Description	Data Type
`userCredentials`	This field contains the user id and password details of the user	Object
`userDetails`	This field contains general details like name, contact etc. for a user	Object
`roleAssignment`	This field contains the details about domain and role	Object

Details of userCredentials:

Field Name	Description	Data Type	Mandatory
`loginID`	Unique identifier for a user	String	Yes
`password`	Secret key required to login. Its value will not be visible as it is confidential and should only be known to the user.	String	Yes

Details of userDetails:

Field Name	Description	Data Type	Mandatory
`firstAndLastName`	First and last name of the user	String	Yes
`email`	Email address of the user	String	Yes
`company`	Company of the user	String	No
`phone`	Contact number of the user	String	No

Field Name	Description	Data Type	Mandatory
`address`	Address of the user	Object	No
`state`	State to which the user belongs to	String	No
`country`	Country to which the user belongs to	String	No

Details of address:

Field Name	Description	Data Type	Mandatory
`address1`	Address line 1. Contains one segment of the users address.	String	No
`address2`	Address line 2. Contains the other segment of the users address.	String	No

Details of roleAssignment:

Field Name	Description	Data Type	Mandatory
`domainId`	The domain in which the user was created.	String	No
`role`	This field contains the information regarding the role assigned to the user. It can have any value from the list of roles already defined in the Manager, i.e. • ePO dashboard data retriever • NOC operator • Report generator • Security expert • Super user • System administrator • No role In addition to the above mentioned roles, the user can also be assigned a custom created role.	String	No (In this case No Role will be assigned by default if no value is specified)

Details of dashBoardAssignment:

Field Name	Description	Data Type
`dashBoardList`	List of all the dashboards to be assigned to user	Array

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	User Id of the created user	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/user

Payload

```
{ "userCredentials": { "loginID": "nsmuser", "password": "nsmuser1234" }, "userDetails": { "firstAndLastName":
"NSM USER", "email": "nsmuser@admin.com", "company": "Intel Secutity", "phone": "", "address": { "address1":
"Intel Security", "address2": "Intel Security" }, "state": "Karnataka", "country": "India" }, "roleAssignment":
{ "domainId": 0, "role": "Super User" }, "dashBoardAssignment": { "dashBoardList":
["Dashboard_1","Dashboard_2"] } }
```

Response

```
{ "createdResourceId": 103 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	5102	Invalid login id provided
2	400	5103	Login id already in use
3	400	5104	Password is required
4	400	5105	Invalid password provided
5	400	5106	Name is required
6	400	5107	Email id is required
7	400	5108	Login Id exceeding maximum length
8	400	5109	Password exceeding maximum length
9	400	5111	Domain cannot be changed
10	400	5610	Dashboard not available.

Update a User

This URL updates the details of a user.

Resource URL

POST /user/{userId}

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
userId	Unique identifier of a user	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type
userCredentials	This field contains the user id and password details of the user	Object
userDetails	This field contains general details like name, contact etc. for a user.	Object
roleAssignment	This field contains the details about domain and role.	Object

Details of userCredentials:

Field Name	Description	Data Type	Mandatory
loginID	Unique identifier for a user.	String	Yes
password	Secret key required to login. Its value will not be visible as it is confidential and should only be known to the user.	String	Yes

Details of userDetails:

Field Name	Description	Data Type	Mandatory
firstAndLastName	First and last name of the user	String	Yes
email	Email address of the user	String	Yes
company	Company of the user	String	No
phone	Contact number of the user	String	No
address	Address of the user	Object	No
state	State to which user belongs to	String	No
country	Country to which user belongs to	String	No

Details of address:

Field Name	Description	Data Type	Mandatory
address1	Address line 1. Contains one segment of the users address.	String	No
address2	Address line 2. Contains other segment of the users address.	String	No

Details of roleAssignment:

Field Name	Description	Data Type	Mandatory
`domainId`	The domain in which the user was created.	String	No
`role`	This field contains the information regarding the role assigned to the user. It can have any value from the list of roles already defined in the Manager, i.e. • ePO dashboard data retriever • NOC operator • Report generator • Security expert • Super user • System administrator • No role In addition to the above mentioned roles, the user can also be assigned a custom created role.	String	No (In this case "No Role" will be assigned by default if no value is specified)

Details of dashBoardAssignment:

Field Name	Description	Data Type
`dashBoardList`	List of all the dashboards to be assigned to user	Array

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Value 1 indicates resource is updated successfully	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/user/103

Payload

```
{ "userCredentials": { "loginID": "nsmuser", "password": "nsmuser1234" }, "userDetails": { "firstAndLastName":
"NSM USER", "email": "nsmuser@admin.com", "company": "Intel Secutity", "phone": "", "address": { "address1":
"Intel Security", "address2": "Intel Security" }, "state": "Karnataka", "country": "India" }, "roleAssignment":
{ "domainId": 0, "role": " Security Expert" }, "dashBoardAssignment": { "dashBoardList":
["Dashboard_1","Dashboard_2"] } }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	5102	Invalid login id provided
2	400	5103	Login id already in use
3	400	5104	Password is required
4	400	5105	Invalid password provided
5	400	5106	Name is required
6	400	5107	Email id is required
7	400	5108	Login id exceeding maximum length
8	400	5109	Password exceeding maximum length
9	400	5111	Domain cannot be changed
10	400	5610	Dashboard not available

Delete a User

This URL deletes the record of an existing user.

Resource URL

DELETE /user/{userId}

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
`userId`	Unique identifier for a user	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Value 1 indicates user record is deleted successfully	Number

Example

Request

DELETE https://<NSM_IP>/user/103

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	5110	Invalid user Id

Configure Alert Pruning Settings

This URL is used to specify the parameters like start time, maximum alerts to store etc. for scheduling alert pruning.

Resource URL

PUT /Maintenance/prunealerts

Request Parameters

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`AlertPruningForm`	Containing details required to schedule alert pruning	Object	Yes

Details of AlertPruningForm:

Field Name	Description	Data Type	Mandatory
`enableAlertPruning`	whether alert pruning should be enabled or not	Boolean	Yes
`pruningStartTime`	Start time for alert pruning process	String	Yes
`maxAlertsToStoreForDashboard`	Maximum number of alerts that will be stored for dashboards	Number	Yes
`maxAlertsToStoreForReport`	Maximum number of alerts that will be stored for reports	Number	Yes
`maxALertAgeForReport`	Maximum number of days for which the alert details will be stored	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/Maintenance/prunealerts

Payload

```
{ "enableAlertPruning":"true", "pruningStartTime":"12:40", "maxAlertsToStoreForDashboard":"10000",
"maxAlertsToStoreForReport":"10000", "maxALertAgeForReport":"20" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	9509	Time should be in HH:MM (24 Hrs format), minutes should be multiple of 5
2	400	9510	Number of alerts to store must be greater than or equal to 10000
3	400	9511	Number of alerts to store for dashboard should not be greater than number of alerts to store for reports.
4	400	9512	Maximum alert age can't be greater than 999 days

Get the Details of Custom Roles

These URL's retrieve the details of the all the roles.

Resource URL

GET /role

This URL is used to retrieve the details of all the roles.

Request Parameters

No request parameters are required for this URL.

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`customRoleList`	An array containing details of all the roles.	Array

Details of CustomRole object (an element in customRoleList):

Field Name	Description	Data Type
`roleName`	Name of the role, as displayed in the Manager	String
`description`	The description of the role, that is given while creating the role	String
`privileges`	List of the privileges that the role has. It can have following values like: • Manage Manager - View only • NTBA policy - Edit • Deploy changes - IPS etc. Other available privileges as visible in the Manager based on the types of devices added in the Manager.	Array

Example

Request

GET https://<NSM_IP>/sdkapi/role

Response

```
{ "customRoleList": [ { "roleName": "ePO Dashboard Data Retriever", "description": "Special role for use with
the ePO Extension to pull NSP data from ePO for display in ePO Dashboards.", "privileges": [ "ePO Dashboard Data
Retrieval" ] }, { "roleName": "Crypto Administrator", "description": "Add and remove devices.", "privileges":
[ "Devices - Edit" ] }, { "roleName": "Audit Administrator", "description": "Administer user activity logs.",
"privileges": [ "User Auditing - Edit" ] } ] }
```

Create a Role

Creates a new role.

Resource URL

POST /role

Request Parameters

Payload Request Parameters:

Field Name	Description	Data Type
`roleName`	Name of the role, as displayed in the Manager	String
`description`	The description of the role, that is given while creating the role	String
`privileges`	List of the privileges that the role has. It can have following values like: • Manage Manager - View only • NTBA policy - Edit • Deploy changes - IPS etc. Other available privileges as visible in the Manager based on the types of devices added in the Manager.	Array

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	User id of the new role	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/role

Payload

```
{ "roleName": "TEST1", "description": "Full rights to the Network Security Manager", "privileges": [ "Alerts -
View Packet Logs", "Analysis", "Configuration Reports - IPS - Create", "Configuration Reports - IPS - Run Only",
"Dashboard", "Deploy Changes - IPS", "ePO Dashboard Data Retrieval", "Event Reports - IPS - Create", "Event
Reports - IPS - Run Only", "IPS Policy - Edit", "IPS Policy - View Only", "Manage IPS - Edit", "Manage IPS -
View Only", "Manage Manager - Edit", "Manage Manager - View Only", "Run Vulnerability Scan", "System - Edit",
"System - View Only", "TA Alert Assignment Supervisor", "TA Alerts - Manage", "TA Alerts - View Only", "TA
Dashboards - General Monitors - Create", "TA Dashboards - General Monitors - View Only", "TA Dashboards - IPS
Monitors - Create", "TA Dashboards - IPS Monitors - View Only", "TA Edit IPS Policy", "TA Endpoints - Manage",
"TA Endpoints - View Only", "TA Retrieve ePO Data", "Users and Roles - Edit", "Users and Roles - View Only" ] }
```

Response

```
{ "createdResourceId": 103 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	9508	Input privileges are not available for assignment

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
2	400	9505	At least one role privilege is required
3	400	9506	Role name is a required field
4	400	9507	Role description is a required field

Delete a Role

This URL deletes an existing custom role.

Resource URL

DELETE /role/{roleName}

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
`roleName`	Name of the custom role that is to be deleted	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Value 1 indicates the resource is deleted successfully	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/role/{CustomRole}

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	9504	The role that you want to delete is in use

Get the Direct Syslog Configuration for the Domain

This URL retrieves the direct syslog configuration for the domain.

Resource URL

GET /domain/<domain_id>/directsyslog

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`enableSyslog`	Enable logging	Boolean
`isInherit`	Inherit settings from parent resource	Boolean
`serverIp`	Syslog server IP	String
`serverPort`	Syslog server port (UDP)	Number
`syslogFacility`	Syslog facility	String
`syslogPriorityMapping`	Attack severity to syslog priority mapping	Object
`message`	Message format	String
`filter`	What attacks to log	Object

Details of syslogPriorityMapping:

Field Name	Description	Data Type
`informationTo`	Informational severity attack mapping	String
`lowTo`	Low severity attack mapping	String
`mediumTO`	Medium severity attack mapping	String
`highTo`	High severity attack mapping	String

Details of filter:

Field Name	Description	Data Type
`LogSomeAttacks`	Log some attacks	Object

Field Name	Description	Data Type
`LogAllAttacks`	Log all attacks - empty object	Object
`isQuarantineLogging`	Log quarantined attacks	Boolean

Details of LogSomeAttacks:

Field Name	Description	Data Type
`isExplicitlyEnabled`	The attack definition has syslog notification explicitly enabled	Boolean
`minimumSeverity`	Minimum severity of attacks	Object

Details of minimumSeverity:

Field Name	Description	Data Type
`isMinimumSeverity`	Is minimum severity selected	Boolean
`severityType`	Type of the severity	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/directsyslog

Response

```
{ 'enableSyslog': 'true', 'syslogPriorityMapping': { 'lowTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'highTo':
'EMERGENCY_SYSTEM_UNUSABLE', 'informationTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'mediumTO':
'EMERGENCY_SYSTEM_UNUSABLE' }, 'isInherit': 'false', 'serverIp': '10.213.172.94', 'filter': { 'LogSomeAttacks':
{ 'isExplicitlyEnabled': 'false', 'minimumSeverity': { 'isMinimumSeverity': 'false', 'severityType':
'LOW' } } }, 'serverPort': '514', 'syslogFacility': 'SECURITY_AUTHORIZATION_CODE_4', 'message': 'Admin_Domain=
$IV_ADMIN_DOMAIN$Alert_Type=$IV_ALERT_TYPE$Attack_Name=$IV_ATTACK_NAME$AttackConfidence=$IV_ATTACK_CONFIDENCE
$DetectMech=$IV_DETECTION_MECHANISM$Category=$IV_CATEGORY$SubCategory=$IV_SUB_CATEGORY$INTF=$IV_INTERFACE
$Attack_Id=$IV_ATTACK_ID$Attack_Count=$IV_ATTACK_COUNT$Attack_Severity=$IV_ATTACK_SEVERITY$Attack_Signature=
$IV_ATTACK_SIGNATURE$Source_Ip=$IV_SOURCE_IP$Dest_Ip=$IV_DESTINATION_IP$Dest_Port=$IV_DESTINATION_PORT
$Source_Port=$IV_SOURCE_PORT$Malware_Confidence=$IV_MALWARE_CONFIDENCE$Detection_Engine=
$IV_MALWARE_DETECTION_ENGINE$Mal_File_Len=$IV_MALWARE_FILE_LENGTH$Mal_file_md5=$IV_MALWARE_FILE_MD5_HASH
$Mal_File_Name=$IV_MALWARE_FILE_NAME$Mal_File_Type=$IV_MALWARE_FILE_TYPE$Mal_Vir_Name=$IV_MALWARE_VIRUS_NAME
$Direction=$IV_DIRECTION$Nw_Protocol=$IV_NETWORK_PROTOCOL$AppProtocol=$IV_APPLICATION_PROTOCOL$Attack_Time=
$IV_ATTACK_TIME$Qurantine_Time=$IV_QUARANTINE_END_TIME$Result_Status=$IV_RESULT_STATUS$Alert_UUID=
$IV_SENSOR_ALERT_UUID$PeerName=$IV_SENSOR_CLUSTER_MEMBER$Sensor_Name=$IV_SENSOR_NAME$SourceOs=$IV_SOURCE_OS
$DestOs=$IV_DEST_OS$Src_APN=$IV_SRC_APN$Dest_APN=$IV_DEST_APN$Src_IMSI=$IV_SRC_IMSI$Dest_IMSI=$IV_DEST_IMSI
$Src_Phone=$IV_SRC_PHONE_NUMBER$Dest_Phone=$IV_DEST_PHONE_NUMBER$Vlan_ID=$IV_VLAN_ID$' }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	6001	Direct sysog configuration is not present for this domain/ Sensor

Update the Direct Syslog Configuration for the Domain

This URL updates the direct syslog configuration for the domain.

Resource URL

PUT /domain/<domain_id>/directsyslog

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domainId	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
enableSyslog	Enable logging	Boolean	Yes
isInherit	Inherit settings from parent resource	Boolean	Yes
serverIp	Syslog server IP	String	Yes
serverPort	Syslog server port (UDP)	Number	Yes
syslogFacility	Syslog facility. Allowed values are: • SECURITY_AUTHORIZATION_CODE_10 • SECURITY_AUTHORIZATION_CODE_4 • LOG_AUDIT_NOTE_1 • LOG_ALERT_NOTE_1 • CLOCK_DAEMON_NOTE_2 • LOCAL_USER_0 • LOCAL_USER_1 • LOCAL_USER_2 • LOCAL_USER_3 • LOCAL_USER_4 • LOCAL_USER_5 • LOCAL_USER_6 • LOCAL_USER_7	String	Yes
syslogPriorityMapping	Attack severity to syslog priority mapping	Object	Yes
message	Message format	String	Yes
filter	What attacks to log	Object	Yes

Details of syslogPriorityMapping:

Field Name	Description	Data Type	Mandatory
informationTo	Informational severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE	String	Yes

Field Name	Description	Data Type	Mandatory
	• ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES		
`lowTo`	Low severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	Yes
`mediumTO`	Medium severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	yes
`highTo`	High severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	Yes

Details of filter:

Field Name	Description	Data Type	Mandatory
`LogSomeAttacks`	Log some attacks	Object	Yes
`LogAllAttacks`	Log all attacks - empty object	Object	Yes
`isQuarantineLogging`	Log quarantined attacks	Boolean	yes

Details of LogSomeAttacks:

Field Name	Description	Data Type	Mandatory
`isExplicitlyEnabled`	The attack definition has Syslog notification explicitly enabled	Boolean	Yes
`minimumSeverity`	Minimum severity of attacks	Object	Yes

Details of minimumSeverity:

Field Name	Description	Data Type	Mandatory
`isMinimumSeverity`	Is minimum severity selected	Boolean	Yes
`severityType`	Type of the severity. Allowed values are: • INFORMATIONAL • LOW • MEDIUM • HIGH	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/directsyslog

Payload

```
{ 'enableSyslog': 'true', 'syslogPriorityMapping': { 'lowTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'highTo':
'EMERGENCY_SYSTEM_UNUSABLE', 'informationTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'mediumTO':
'EMERGENCY_SYSTEM_UNUSABLE' }, 'isInherit': 'false', 'serverIp': '10.213.172.94', 'filter': { 'LogSomeAttacks':
{ 'isExplicitlyEnabled': 'false', 'minimumSeverity': { 'isMinimumSeverity': 'false', 'severityType':
'LOW' } } }, 'serverPort': '514', 'syslogFacility': 'SECURITY_AUTHORIZATION_CODE_4', 'message': 'Admin_Domain=
$IV_ADMIN_DOMAIN$Alert_Type=$IV_ALERT_TYPE$Attack_Name=$IV_ATTACK_NAME$AttackConfidence=$IV_ATTACK_CONFIDENCE
$DetectMech=$IV_DETECTION_MECHANISM$Category=$IV_CATEGORY$SubCategory=$IV_SUB_CATEGORY$INTF=$IV_INTERFACE
$Attack_Id=$IV_ATTACK_ID$Attack_Count=$IV_ATTACK_COUNT$Attack_Severity=$IV_ATTACK_SEVERITY$Attack_Signature=
$IV_ATTACK_SIGNATURE$Source_Ip=$IV_SOURCE_IP$Dest_Ip=$IV_DESTINATION_IP$Dest_Port=$IV_DESTINATION_PORT
$Source_Port=$IV_SOURCE_PORT$Malware_Confidence=$IV_MALWARE_CONFIDENCE$Detection_Engine=
$IV_MALWARE_DETECTION_ENGINE$Mal_File_Len=$IV_MALWARE_FILE_LENGTH$Mal_file_md5=$IV_MALWARE_FILE_MD5_HASH
$Mal_File_Name=$IV_MALWARE_FILE_NAME$Mal_File_Type=$IV_MALWARE_FILE_TYPE$Mal_Vir_Name=$IV_MALWARE_VIRUS_NAME
$Direction=$IV_DIRECTION$Nw_Protocol=$IV_NETWORK_PROTOCOL$AppProtocol=$IV_APPLICATION_PROTOCOL$Attack_Time=
$IV_ATTACK_TIME$Qurantine_Time=$IV_QUARANTINE_END_TIME$Result_Status=$IV_RESULT_STATUS$Alert_UUID=
$IV_SENSOR_ALERT_UUID$PeerName=$IV_SENSOR_CLUSTER_MEMBER$Sensor_Name=$IV_SENSOR_NAME$SourceOs=$IV_SOURCE_OS
$DestOs=$IV_DEST_OS$Src_APN=$IV_SRC_APN$Dest_APN=$IV_DEST_APN$Src_IMSI=$IV_SRC_IMSI$Dest_IMSI=$IV_DEST_IMSI
$Src_Phone=$IV_SRC_PHONE_NUMBER$Dest_Phone=$IV_DEST_PHONE_NUMBER$Vlan_ID=$IV_VLAN_ID$' }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	6002	IPV6 is not supported for direct syslog configuration

Get the Direct Syslog Configuration for the Sensor

This URL retrieves the direct syslog configuration for the Sensor.

Resource URL

GET /sensor/<sensor_id>/directsyslog

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`enableSyslog`	Enable logging	Boolean
`isInherit`	Inherit settings from parent resource	Boolean
`serverIp`	Syslog server IP	String
`serverPort`	Syslog server port (UDP)	Number
`syslogFacility`	Syslog facility	String
`syslogPriorityMapping`	Attack severity to syslog priority mapping	Object
`message`	Message format	String
`filter`	What attacks to log	Object

Details of syslogPriorityMapping:

Field Name	Description	Data Type
`informationTo`	Informational severity attack mapping	String

Field Name	Description	Data Type
lowTo	Low severity attack mapping	String
mediumTO	Medium severity attack mapping	String
highTo	High severity attack mapping	String

Details of filter:

Field Name	Description	Data Type
LogSomeAttacks	Log some attacks	Object
LogAllAttacks	Log all attacks - empty object	Object
isQuarantineLogging	Log quarantined attacks	Boolean

Details of LogSomeAttacks:

Field Name	Description	Data Type
isExplicitlyEnabled	The attack definition has syslog notification explicitly enabled	Boolean
minimumSeverity	Minimum severity of attacks	Object

Details of minimumSeverity:

Field Name	Description	Data Type
isMinimumSeverity	Is minimum severity selected	Boolean
severityType	Type of the severity	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/directsyslog

Response

```
{ 'enableSyslog': 'true', 'syslogPriorityMapping': { 'lowTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'highTo':
'EMERGENCY_SYSTEM_UNUSABLE', 'informationTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'mediumTO':
'EMERGENCY_SYSTEM_UNUSABLE' }, 'isInherit': 'false', 'serverIp': '10.213.172.94', 'filter': { 'LogSomeAttacks':
{ 'isExplicitlyEnabled': 'false', 'minimumSeverity': { 'isMinimumSeverity': 'false', 'severityType':
'LOW' } } }, 'serverPort': '514', 'syslogFacility': 'SECURITY_AUTHORIZATION_CODE_4', 'message': 'Admin_Domain=
$IV_ADMIN_DOMAIN$Alert_Type=$IV_ALERT_TYPE$Attack_Name=$IV_ATTACK_NAME$AttackConfidence=$IV_ATTACK_CONFIDENCE
$DetectMech=$IV_DETECTION_MECHANISM$Category=$IV_CATEGORY$SubCategory=$IV_SUB_CATEGORY$INTF=$IV_INTERFACE
$Attack_Id=$IV_ATTACK_ID$Attack_Count=$IV_ATTACK_COUNT$Attack_Severity=$IV_ATTACK_SEVERITY$Attack_Signature=
$IV_ATTACK_SIGNATURE$Source_Ip=$IV_SOURCE_IP$Dest_Ip=$IV_DESTINATION_IP$Dest_Port=$IV_DESTINATION_PORT
$Source_Port=$IV_SOURCE_PORT$Malware_Confidence=$IV_MALWARE_CONFIDENCE$Detection_Engine=
$IV_MALWARE_DETECTION_ENGINE$Mal_File_Len=$IV_MALWARE_FILE_LENGTH$Mal_file_md5=$IV_MALWARE_FILE_MD5_HASH
$Mal_File_Name=$IV_MALWARE_FILE_NAME$Mal_File_Type=$IV_MALWARE_FILE_TYPE$Mal_Vir_Name=$IV_MALWARE_VIRUS_NAME
$Direction=$IV_DIRECTION$Nw_Protocol=$IV_NETWORK_PROTOCOL$AppProtocol=$IV_APPLICATION_PROTOCOL$Attack_Time=
$IV_ATTACK_TIME$Qurantine_Time=$IV_QUARANTINE_END_TIME$Result_Status=$IV_RESULT_STATUS$Alert_UUID=
$IV_SENSOR_ALERT_UUID$PeerName=$IV_SENSOR_CLUSTER_MEMBER$Sensor_Name=$IV_SENSOR_NAME$SourceOs=$IV_SOURCE_OS
$DestOs=$IV_DEST_OS$Src_APN=$IV_SRC_APN$Dest_APN=$IV_DEST_APN$Src_IMSI=$IV_SRC_IMSI$Dest_IMSI=$IV_DEST_IMSI
$Src_Phone=$IV_SRC_PHONE_NUMBER$Dest_Phone=$IV_DEST_PHONE_NUMBER$Vlan_ID=$IV_VLAN_ID$' }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1106	Invalid Sensor
2	404	1124	The Sensor is inactive
3	400	6001	Direct sysog configuration is not present for this domain/ Sensor

Update the Direct Syslog Configuration for the Sensor

This URL updates the direct syslog configuration for the Sensor.

Resource URL

PUT /sensor/<sensor_id>/directsyslog

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`enableSyslog`	Enable logging	Boolean	Yes
`isInherit`	Inherit settings from parent resource	Boolean	Yes
`serverIp`	Syslog server IP	String	Yes
`serverPort`	Syslog server port (UDP)	number	Yes
`syslogFacility`	Syslog facility. Allowed values are: • SECURITY_AUTHORIZATION_CODE_10 • SECURITY_AUTHORIZATION_CODE_4 • LOG_AUDIT_NOTE_1 • LOG_ALERT_NOTE_1 • CLOCK_DAEMON_NOTE_2 • LOCAL_USER_0 • LOCAL_USER_1 • LOCAL_USER_2 • LOCAL_USER_3 • LOCAL_USER_4 • LOCAL_USER_5 • LOCAL_USER_6	String	Yes

Field Name	Description	Data Type	Mandatory
	• LOCAL_USER_7		
`syslogPriorityMapping`	Attack severity to syslog priority mapping	Object	Yes
`message`	Message format	String	Yes
`filter`	What attacks to log	Object	Yes

Details of syslogPriorityMapping:

Field Name	Description	Data Type	Mandatory
`informationTo`	Informational severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	Yes
`lowTo`	Low severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	Yes
`mediumTO`	Medium severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	yes

Field Name	Description	Data Type	Mandatory
highTo	High severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	Yes

Details of filter:

Field Name	Description	Data Type	Mandatory
LogSomeAttacks	Log some attacks	Object	Yes
LogAllAttacks	Log all attacks - empty object	Object	Yes
isQuarantineLogging	Log quarantined attacks	Boolean	yes

Details of LogSomeAttacks:

Field Name	Description	Data Type	Mandatory
isExplicitlyEnabled	The attack definition has syslog notification explicitly enabled	Boolean	Yes
minimumSeverity	Minimum severity of attacks	Object	Yes

Details of minimumSeverity:

Field Name	Description	Data Type	Mandatory
isMinimumSeverity	Is minimum severity selected	Boolean	Yes
severityType	Type of the severity. Allowed values are: • INFORMATIONAL • LOW • MEDIUM • HIGH	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1001/directsyslog

Payload

```
{ 'enableSyslog': 'true', 'syslogPriorityMapping': { 'lowTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'highTo':
'EMERGENCY_SYSTEM_UNUSABLE', 'informationTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'mediumTO':
'EMERGENCY_SYSTEM_UNUSABLE' }, 'isInherit': 'false', 'serverIp': '10.213.172.94', 'filter': { 'LogSomeAttacks':
{ 'isExplicitlyEnabled': 'false', 'minimumSeverity': { 'isMinimumSeverity': 'false', 'severityType':
'LOW' } } }, 'serverPort': '514', 'syslogFacility': 'SECURITY_AUTHORIZATION_CODE_4', 'message': 'Admin_Domain=
$IV_ADMIN_DOMAIN$Alert_Type=$IV_ALERT_TYPE$Attack_Name=$IV_ATTACK_NAME$AttackConfidence=$IV_ATTACK_CONFIDENCE
$DetectMech=$IV_DETECTION_MECHANISM$Category=$IV_CATEGORY$SubCategory=$IV_SUB_CATEGORY$INTF=$IV_INTERFACE
$Attack_Id=$IV_ATTACK_ID$Attack_Count=$IV_ATTACK_COUNT$Attack_Severity=$IV_ATTACK_SEVERITY$Attack_Signature=
$IV_ATTACK_SIGNATURE$Source_Ip=$IV_SOURCE_IP$Dest_Ip=$IV_DESTINATION_IP$Dest_Port=$IV_DESTINATION_PORT
$Source_Port=$IV_SOURCE_PORT$Malware_Confidence=$IV_MALWARE_CONFIDENCE$Detection_Engine=
$IV_MALWARE_DETECTION_ENGINE$Mal_File_Len=$IV_MALWARE_FILE_LENGTH$Mal_file_md5=$IV_MALWARE_FILE_MD5_HASH
$Mal_File_Name=$IV_MALWARE_FILE_NAME$Mal_File_Type=$IV_MALWARE_FILE_TYPE$Mal_Vir_Name=$IV_MALWARE_VIRUS_NAME
$Direction=$IV_DIRECTION$Nw_Protocol=$IV_NETWORK_PROTOCOL$AppProtocol=$IV_APPLICATION_PROTOCOL$Attack_Time=
$IV_ATTACK_TIME$Qurantine_Time=$IV_QUARANTINE_END_TIME$Result_Status=$IV_RESULT_STATUS$Alert_UUID=
$IV_SENSOR_ALERT_UUID$PeerName=$IV_SENSOR_CLUSTER_MEMBER$Sensor_Name=$IV_SENSOR_NAME$SourceOs=$IV_SOURCE_OS
$DestOs=$IV_DEST_OS$Src_APN=$IV_SRC_APN$Dest_APN=$IV_DEST_APN$Src_IMSI=$IV_SRC_IMSI$Dest_IMSI=$IV_DEST_IMSI
$Src_Phone=$IV_SRC_PHONE_NUMBER$Dest_Phone=$IV_DEST_PHONE_NUMBER$Vlan_ID=$IV_VLAN_ID$' }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1106	Invalid Sensor
2	404	1124	The Sensor is inactive
3	400	6002	IPV6 is not supported for direct syslog configuration

Test the Direct Syslog Configuration for Domain

This URL tests the direct syslog configuration for the domain.

Resource URL

PUT /sensor/<sensor_id>/directsyslog

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`enableSyslog`	Enable logging	Boolean	Yes
`isInherit`	Inherit settings from parent resource	Boolean	Yes

Field Name	Description	Data Type	Mandatory
`serverIp`	Syslog server IP	String	Yes
`serverPort`	Syslog server port (UDP)	Number	Yes
`syslogFacility`	Syslog Facility. Allowed values are: • SECURITY_AUTHORIZATION_CODE_10 • SECURITY_AUTHORIZATION_CODE_4 • LOG_AUDIT_NOTE_1 • LOG_ALERT_NOTE_1 • CLOCK_DAEMON_NOTE_2 • LOCAL_USER_0 • LOCAL_USER_1 • LOCAL_USER_2 • LOCAL_USER_3 • LOCAL_USER_4 • LOCAL_USER_5 • LOCAL_USER_6 • LOCAL_USER_7	String	Yes
`syslogPriorityMapping`	Attack severity to syslog priority mapping	Object	Yes
`message`	Message format	String	Yes
`filter`	What attacks to log	Object	Yes

Details of syslogPriorityMapping:

Field Name	Description	Data Type	Mandatory
`informationTo`	Informational severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	Yes
`lowTo`	Low severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR	String	Yes

Field Name	Description	Data Type	Mandatory
	• WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES		
`mediumTO`	Medium severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	yes
`highTo`	High severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	Yes

Details of filter:

Field Name	Description	Data Type	Mandatory
`LogSomeAttacks`	Log some attacks	Object	Yes
`LogAllAttacks`	Log all attacks - empty object	Object	Yes
`isQuarantineLogging`	Log quarantined attacks	Boolean	yes

Details of LogSomeAttacks:

Field Name	Description	Data Type	Mandatory
`isExplicitlyEnabled`	The attack definition has syslog notification explicitly enabled	Boolean	Yes
`minimumSeverity`	Minimum severity of attacks	Object	Yes

Details of minimumSeverity:

Field Name	Description	Data Type	Mandatory
isMinimumSeverity	Is minimum severity selected	Boolean	Yes
severityType	Type of the severity. Allowed values are: • INFORMATIONAL • LOW • MEDIUM • HIGH	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/directsyslog/testconnection

Payload

```
{ 'enableSyslog': 'true', 'syslogPriorityMapping': { 'lowTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'highTo':
'EMERGENCY_SYSTEM_UNUSABLE', 'informationTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'mediumTO':
'EMERGENCY_SYSTEM_UNUSABLE' }, 'isInherit': 'false', 'serverIp': '10.213.172.94', 'filter': { 'LogSomeAttacks':
{ 'isExplicitlyEnabled': 'false', 'minimumSeverity': { 'isMinimumSeverity': 'false', 'severityType':
'LOW' } } }, 'serverPort': '514', 'syslogFacility': 'SECURITY_AUTHORIZATION_CODE_4', 'message': 'Admin_Domain=
$IV_ADMIN_DOMAIN$Alert_Type=$IV_ALERT_TYPE$Attack_Name=$IV_ATTACK_NAME$AttackConfidence=$IV_ATTACK_CONFIDENCE
$DetectMech=$IV_DETECTION_MECHANISM$Category=$IV_CATEGORY$SubCategory=$IV_SUB_CATEGORY$INTF=$IV_INTERFACE
$Attack_Id=$IV_ATTACK_ID$Attack_Count=$IV_ATTACK_COUNT$Attack_Severity=$IV_ATTACK_SEVERITY$Attack_Signature=
$IV_ATTACK_SIGNATURE$Source_Ip=$IV_SOURCE_IP$Dest_Ip=$IV_DESTINATION_IP$Dest_Port=$IV_DESTINATION_PORT
$Source_Port=$IV_SOURCE_PORT$Malware_Confidence=$IV_MALWARE_CONFIDENCE$Detection_Engine=
$IV_MALWARE_DETECTION_ENGINE$Mal_File_Len=$IV_MALWARE_FILE_LENGTH$Mal_file_md5=$IV_MALWARE_FILE_MD5_HASH
$Mal_File_Name=$IV_MALWARE_FILE_NAME$Mal_File_Type=$IV_MALWARE_FILE_TYPE$Mal_Vir_Name=$IV_MALWARE_VIRUS_NAME
$Direction=$IV_DIRECTION$Nw_Protocol=$IV_NETWORK_PROTOCOL$AppProtocol=$IV_APPLICATION_PROTOCOL$Attack_Time=
$IV_ATTACK_TIME$Qurantine_Time=$IV_QUARANTINE_END_TIME$Result_Status=$IV_RESULT_STATUS$Alert_UUID=
$IV_SENSOR_ALERT_UUID$PeerName=$IV_SENSOR_CLUSTER_MEMBER$Sensor_Name=$IV_SENSOR_NAME$SourceOs=$IV_SOURCE_OS
$DestOs=$IV_DEST_OS$Src_APN=$IV_SRC_APN$Dest_APN=$IV_DEST_APN$Src_IMSI=$IV_SRC_IMSI$Dest_IMSI=$IV_DEST_IMSI
$Src_Phone=$IV_SRC_PHONE_NUMBER$Dest_Phone=$IV_DEST_PHONE_NUMBER$Vlan_ID=$IV_VLAN_ID$' }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	6002	IPV6 is not supported for direct syslog configuration
3	400	6002	Direct syslog is disabled or inherit settings has been selected

Test the Direct Syslog Configuration for the Sensor

This URL tests the direct syslog configuration for the Sensor.

Resource URL

PUT /sensor/<sensor_id>/ directsyslog/testconnection

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensorId	Sensor id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
enableSyslog	Enable logging	Boolean	Yes
isInherit	Inherit settings from parent resource	Boolean	Yes
serverIp	Syslog server IP	String	Yes
serverPort	Syslog server port (UDP)	Number	Yes
syslogFacility	Syslog facility. Values allowed are: • SECURITY_AUTHORIZATION_CODE_10 • SECURITY_AUTHORIZATION_CODE_4 • LOG_AUDIT_NOTE_1 • LOG_ALERT_NOTE_1 • CLOCK_DAEMON_NOTE_2 • LOCAL_USER_0 • LOCAL_USER_1 • LOCAL_USER_2 • LOCAL_USER_3 • LOCAL_USER_4 • LOCAL_USER_5 • LOCAL_USER_6 • LOCAL_USER_7	String	Yes
syslogPriorityMapping	Attack severity to syslog priority mapping	Object	Yes
message	Message format	String	Yes
filter	What attacks to log	Object	Yes

Details of syslogPriorityMapping:

Field Name	Description	Data Type	Mandatory
`informationTo`	Informational severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	Yes
`lowTo`	Low severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	Yes
`mediumTO`	Medium severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION • INFORMATIONAL_MESSGES • DEBUG_MESSAGES	String	yes
`highTo`	High severity attack mapping. Values allowed are: • EMERGENCY_SYSTEM_UNUSABLE • ALERT_ACTION_IMMEDIATELY • CRITICAL_CONDITIONS • ERROR • WARNING_CONDITIONS • NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION	String	Yes

Field Name	Description	Data Type	Mandatory
	• INFORMATIONAL_MESSGES • DEBUG_MESSAGES		

Details of filter:

Field Name	Description	Data Type	Mandatory
`LogSomeAttacks`	Log some attacks	Object	Yes
`LogAllAttacks`	Log all attacks - empty object	Object	Yes
`isQuarantineLogging`	Log quarantined attacks	Boolean	yes

Details of LogSomeAttacks:

Field Name	Description	Data Type	Mandatory
`isExplicitlyEnabled`	The attack definition has syslog notification explicitly enabled	Boolean	Yes
`minimumSeverity`	Minimum severity of attacks	Object	Yes

Details of minimumSeverity:

Field Name	Description	Data Type	Mandatory
`isMinimumSeverity`	Is minimum severity selected	Boolean	Yes
`severityType`	Type of the severity. Allowed values are: • INFORMATIONAL • LOW • MEDIUM • HIGH	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1001/directsyslog/testconnection

Payload

```
{ 'enableSyslog': 'true', 'syslogPriorityMapping': { 'lowTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'highTo':
'EMERGENCY_SYSTEM_UNUSABLE', 'informationTo': 'EMERGENCY_SYSTEM_UNUSABLE', 'mediumTO':
'EMERGENCY_SYSTEM_UNUSABLE' }, 'isInherit': 'false', 'serverIp': '10.213.172.94', 'filter': { 'LogSomeAttacks':
{ 'isExplicitlyEnabled': 'false', 'minimumSeverity': { 'isMinimumSeverity': 'false', 'severityType':
'LOW' } } }, 'serverPort': '514', 'syslogFacility': 'SECURITY_AUTHORIZATION_CODE_4', 'message': 'Admin_Domain=
$IV_ADMIN_DOMAIN$Alert_Type=$IV_ALERT_TYPE$Attack_Name=$IV_ATTACK_NAME$AttackConfidence=$IV_ATTACK_CONFIDENCE
$DetectMech=$IV_DETECTION_MECHANISM$Category=$IV_CATEGORY$SubCategory=$IV_SUB_CATEGORY$INTF=$IV_INTERFACE
$Attack_Id=$IV_ATTACK_ID$Attack_Count=$IV_ATTACK_COUNT$Attack_Severity=$IV_ATTACK_SEVERITY$Attack_Signature=
$IV_ATTACK_SIGNATURE$Source_Ip=$IV_SOURCE_IP$Dest_Ip=$IV_DESTINATION_IP$Dest_Port=$IV_DESTINATION_PORT
$Source_Port=$IV_SOURCE_PORT$Malware_Confidence=$IV_MALWARE_CONFIDENCE$Detection_Engine=
$IV_MALWARE_DETECTION_ENGINE$Mal_File_Len=$IV_MALWARE_FILE_LENGTH$Mal_file_md5=$IV_MALWARE_FILE_MD5_HASH
$Mal_File_Name=$IV_MALWARE_FILE_NAME$Mal_File_Type=$IV_MALWARE_FILE_TYPE$Mal_Vir_Name=$IV_MALWARE_VIRUS_NAME
$Direction=$IV_DIRECTION$Nw_Protocol=$IV_NETWORK_PROTOCOL$AppProtocol=$IV_APPLICATION_PROTOCOL$Attack_Time=
$IV_ATTACK_TIME$Qurantine_Time=$IV_QUARANTINE_END_TIME$Result_Status=$IV_RESULT_STATUS$Alert_UUID=
$IV_SENSOR_ALERT_UUID$PeerName=$IV_SENSOR_CLUSTER_MEMBER$Sensor_Name=$IV_SENSOR_NAME$SourceOs=$IV_SOURCE_OS
$DestOs=$IV_DEST_OS$Src_APN=$IV_SRC_APN$Dest_APN=$IV_DEST_APN$Src_IMSI=$IV_SRC_IMSI$Dest_IMSI=$IV_DEST_IMSI
$Src_Phone=$IV_SRC_PHONE_NUMBER$Dest_Phone=$IV_DEST_PHONE_NUMBER$Vlan_ID=$IV_VLAN_ID$' }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	1106	Invalid Sensor
2	404	1124	The Sensor is inactive
3	400	6002	IPV6 is not supported for direct syslog configuration
4	400	6002	Direct syslog is disabled or inherit settings has been selected

Get the Radius Configuration for Domain

This URL retrieves the radius configuration for the domain.

Resource URL

GET /domain/<domain_id>/remoteaccess/radius

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domainId	Domain id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
inheritSettings	Inherit settings from parent	Boolean
enableRadiusCLIAuthentication	Enable radius configuration flag	Boolean
primaryRadiusServer	Primary radius server	Object
secondayRadiusServer	Seconday radius server	Object
syslogFacility	Syslog facility	String
syslogPriorityMapping	Attack severity to syslog priority mapping	Object
message	Message format	String
filter	What attacks to log	Object

Details of primaryRadiusServer and secondayRadiusServer:

Field Name	Description	Data Type
serverIpAddr	IP address	String
sharedSecret	Shared secret key	String
authenticationPort	Authentication port	Number
connectionTimeoutInSeconds	Connection time out in seconds	Number
enableAccounting	Enable accounting flag	Boolean
accountingPort	Accounting port	Number

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/remoteaccess/radius

Response

```
{ "inheritSettings": false, "enableRadiusCLIAuthentication": true, "primaryRadiusServer": { "serverIpAddr":
"1.1.1.3", "sharedSecret": "adsadasl3232", "authenticationPort": 1812, "connectionTimeoutInSeconds": 6,
"enableAccounting": false, "accountingPort": 1813 }, "secondayRadiusServer": { "serverIpAddr": "1.1.1.5",
"sharedSecret": "dssdfksdnfsdf", "authenticationPort": 1812, "connectionTimeoutInSeconds": 6,
"enableAccounting": false, "accountingPort": 1813 } }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Update the Radius Configuration for the Domain

This URL updates the radius configuration for the domain.

Resource URL

PUT /domain/<domain_id>/remoteaccess/radius

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domainId	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type
inheritSettings	Inherit settings from parent	Boolean
enableRadiusCLIAuthentication	Enable radius configuration flag	Boolean
primaryRadiusServer	Primary radius server	Object
secondayRadiusServer	Seconday radius server	Object
syslogFacility	Syslog facility	String
syslogPriorityMapping	Attack severity to syslog priority mapping	Object
message	Message format	String
filter	What attacks to log	Object

Details of primaryRadiusServer and secondayRadiusServer:

Field Name	Description	Data Type
serverIpAddr	IP address	String

Field Name	Description	Data Type
`sharedSecret`	Shared secret key	String
`authenticationPort`	Authentication port	Number
`connectionTimeoutInSeconds`	Connection time out in seconds	Number
`enableAccounting`	Enable accounting flag	Boolean
`accountingPort`	Accounting port	Number

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/remoteacess/radius

Payload

```
{ "inheritSettings": false, "enableRadiusCLIAuthentication": true, "primaryRadiusServer": { "serverIpAddr":
"1.1.1.3", "sharedSecret": "adsadasl3232", "authenticationPort": 1812, "connectionTimeoutInSeconds": 6,
"enableAccounting": false, "accountingPort": 1813 }, "secondayRadiusServer": { "serverIpAddr": "1.1.1.5",
"sharedSecret": "dssdfksdnfsdf", "authenticationPort": 1812, "connectionTimeoutInSeconds": 6,
"enableAccounting": false, "accountingPort": 1813 } }
```

Response

```
{ "status": 1 }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Get the Advanced Device Configuration at Domain Level

This URL retrieves the advanced device configuration at the domain level.

Resource URL

GET /domain/<domainId>/ advanceddeviceconfiguration

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`inheritSettings`	Inherit settings from the parent domain	Boolean
`preAttackBytestoCapture`	Attack bytes to capture. Can be 128, 256	Int
`inspectTunneledTraffic`	Inspect tunneled traffic	Boolean
`cliActivityLogging`	Log CLI activity. Values allowed are: • DISABLED • DEVICE_ONLY • MANAGER_ONLY • DEVICE_AND_MANAGER	String
`showCPUUsageinCLI`	Show CPU usage in CLI	Boolean
`restrictSSHAccesstoCLI`	Restrict CLI access using SSH	Boolean
`enableSSHLogging`	Enable SSH logging	Boolean
`permittedIPv4CIDRBlocks`	The permitted IPV4 CIDR list for SSH access to CLI	Object
`permittedIPv6CIDRBlocks`	The permitted IPV6 CIDR list for SSH access to CLI	Object
`useTraditionalSnort`	Chooses either the traditional McAfee snort or the new Suricata snort	Boolean

Details of permittedIPv4CIDRBlocks:

Field Name	Description	Data Type
`id`	ID of the object	Int
`cidr`	IPV4 CIDR address	String

Field Name	Description	Data Type
action	On delete action, the value should be 'delete'	String

Details of permittedIPv6CIDRBlocks:

Field Name	Description	Data Type
id	ID of the object	Int
cidr	IPV6 CIDR address	String
action	On delete action, the value should be 'delete'	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/advanceddeviceconfiguration

Response

```
{ "inheritSettings": false, "preAttackBytestoCapture": 128, "inspectTunneledTraffic": false,
"cliActivityLogging": "DISABLED", "showCPUUsageinCLI": false, "restrictSSHAccesstoCLI": true,
"enableSSHLogging": false, "permittedIPv4CIDRBlocks": [ { "id": 1, "cidr": "1.1.1.1/32", "action": null } ],
"permittedIPv6CIDRBlocks": [ { "id": 2, "cidr": "2001:0DB9:0000:0000:0000:0000:0000:0001/128", "action":
null } ], “useTraditionalSnort”: true }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Update the Advanced Device Configuration at Domain Level

This URL is used to update the advanced device configuration at the domain level.

Resource URL

PUT /domain/<domainId>/ advanceddeviceconfiguration

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domainId	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
inheritSettings	Inherit settings from the parent domain	Boolean	Yes

Field Name	Description	Data Type	Mandatory
`preAttackBytestoCapture`	Attack bytes to capture. Can be 128, 256	Int	Yes
`inspectTunneledTraffic`	Inspect tunneled traffic	Boolean	Yes
`cliActivityLogging`	Log CLI activity. Values allowed are: • DISABLED • DEVICE_ONLY • MANAGER_ONLY • DEVICE_AND_MANAGER	String	Yes
`showCPUUsageinCLI`	Show CPU usage in CLI	Boolean	Yes
`restrictSSHAccesstoCLI`	Restrict CLI access using SSH	Boolean	Yes
`enableSSHLogging`	Enable SSH logging	Boolean	Yes
`permittedIPv4CIDRBlocks`	The permitted IPV4 CIDR list for SSH access to CLI	Object	Yes
`permittedIPv6CIDRBlocks`	The permitted IPV6 CIDR list for SSH access to CLI	Object	Yes
`useTraditionalSnort`	Chooses either the traditional McAfee snort or the new Suricata snort	Boolean	Yes

Details of permittedIPv4CIDRBlocks:

Field Name	Description	Data Type	Mandatory
`id`	ID of the object	Int	No
`cidr`	IPV4 CIDR address	String	Yes
`action`	On delete action, the value should be 'delete'	String	Yes

Details of permittedIPv6CIDRBlocks:

Field Name	Description	Data Type	Mandatory
`id`	ID of the object	Int	No
`cidr`	IPV6 CIDR address	String	Yes
`action`	On delete action, the value should be 'delete'	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`Status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/advanceddeviceconfiguration

Payload

```
{ "inheritSettings": false, "preAttackBytestoCapture": 128, "inspectTunneledTraffic": false,
"cliActivityLogging": "DISABLED", "showCPUUsageinCLI": false, "restrictSSHAccesstoCLI": true,
"enableSSHLogging": false, "permittedIPv4CIDRBlocks": [ { "id": null, "cidr": "1.1.1.1/32", "action": null } ],
"permittedIPv6CIDRBlocks": [ { "id": null, "cidr": "2001:0DB9:0000:0000:0000:0000:0000:0001/128", "action":
null } ] , “useTraditionalSnort”: true }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	1001	Pre attack packet capture bytes if provided, can only be 128 and 256
3	400	9101	Cannot inherit setting for parent domain
4	400	1701	The cidrs provided are not present in the resource :: <list>
5	400	1701	The cidrs provided for addition are already present in the resource :: <list>
6	400	1701	Invalid CIDR notation : <list>
7	400	1701	Duplicate CIDR entry : <list>
8	400	1001	IP list is required
9	500	1001	Internal server errors

Get the Advanced Device Configuration at Sensor Level

This URL is used to retrieve the advanced device configuration at the Sensor level.

Resource URL

GET /sensor/<sensorId>/ advanceddeviceconfiguration

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensorId	Sensor id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
inheritSettings	Inherit settings from the parent domain	Boolean
preAttackBytestoCapture	Attack bytes to capture. Can be 128, 256	Int
inspectTunneledTraffic	Inspect tunneled traffic	Boolean
cliActivityLogging	Log CLI activity. Values allowed are: • DISABLED • DEVICE_ONLY • MANAGER_ONLY • DEVICE_AND_MANAGER	String
showCPUUsageinCLI	Show CPU usage in CLI	Boolean
restrictSSHAccesstoCLI	Restrict CLI access using SSH	Boolean
enableSSHLogging	Enable SSH logging	Boolean
permittedIPv4CIDRBlocks	The permitted IPV4 CIDR list for SSH access to CLI	Object
permittedIPv6CIDRBlocks	The permitted IPV6 CIDR list for SSH access to CLI	Object
useTraditionalSnort	Chooses either the traditional McAfee Snort or the new Suricata snort	Boolean

Details of permittedIPv4CIDRBlocks:

Field Name	Description	Data Type
id	ID of the object	Int
cidr	IPV4 CIDR address	String
action	On delete action, the value should be 'delete'	String

Details of permittedIPv6CIDRBlocks:

Field Name	Description	Data Type
id	ID of the object	Int

Field Name	Description	Data Type
`cidr`	IPV6 CIDR address	String
`action`	On delete action, the value should be 'delete'	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/advanceddeviceconfiguration

Response

```
{ "inheritSettings": false, "preAttackBytestoCapture": 128, "inspectTunneledTraffic": false,
"cliActivityLogging": "DISABLED", "showCPUUsageinCLI": false, "restrictSSHAccesstoCLI": true,
"enableSSHLogging": false, "permittedIPv4CIDRBlocks": [ { "id": 1, "cidr": "1.1.1.1/32", "action": null } ],
"permittedIPv6CIDRBlocks": [ { "id": 2, "cidr": "2001:0DB9:0000:0000:0000:0000:0000:0001/128", "action":
null } ] , “useTraditionalSnort”: true }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1124	The Sensor is inactive

Update the Advanced Device Configuration at Sensor Level

This URL is used to update the advanced device configuration at the Sensor level.

Resource URL

PUT /sensor/<sensorId>/ advanceddeviceconfiguration

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`inheritSettings`	Inherit settings from the parent domain	Boolean	Yes
`preAttackBytestoCapture`	Attack bytes to capture. Can be 128, 256	Int	Yes
`inspectTunneledTraffic`	Inspect tunneled traffic	Boolean	Yes
`cliActivityLogging`	Log CLI activity. Values allowed are: • DISABLED	String	Yes

Field Name	Description	Data Type	Mandatory
	• DEVICE_ONLY • MANAGER_ONLY • DEVICE_AND_MANAGER		
`showCPUUsageinCLI`	Show CPU usage in CLI	Boolean	Yes
`restrictSSHAccesstoCLI`	Restrict CLI access using SSH	Boolean	Yes
`enableSSHLogging`	Enable SSH logging	Boolean	Yes
`permittedIPv4CIDRBlocks`	The permitted IPV4 CIDR list for SSH access to CLI	Object	Yes
`permittedIPv6CIDRBlocks`	The permitted IPV6 CIDR list for SSH access to CLI	Object	Yes
`useTraditionalSnort`	Chooses either the traditional McAfee Snort or the new Suricata Snort	Boolean	Yes

Details of permittedIPv4CIDRBlocks:

Field Name	Description	Data Type	Mandatory
`id`	ID of the object	Int	No
`cidr`	IPV4 CIDR address	String	Yes
`action`	On delete action, the value should be 'delete'	String	Yes

Details of permittedIPv6CIDRBlocks:

Field Name	Description	Data Type	Mandatory
`id`	ID of the object	Int	No
`cidr`	IPV6 CIDR address	String	Yes
`action`	On delete action, the value should be 'delete'	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1001/advanceddeviceconfiguration

Payload

```
{ "inheritSettings": false, "preAttackBytestoCapture": 128, "inspectTunneledTraffic": false,
"cliActivityLogging": "DISABLED", "showCPUUsageinCLI": false, "restrictSSHAccesstoCLI": true,
"enableSSHLogging": false, "permittedIPv4CIDRBlocks": [ { "id": 1, "cidr": "1.1.1.1/32", "action": null } ],
"permittedIPv6CIDRBlocks": [ { "id": 2, "cidr": "2001:0DB9:0000:0000:0000:0000:0000:0001/128", "action":
"delete" } ] , "useTraditionalSnort": true }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1124	The Sensor is inactive
3	400	1001	Pre attack packet capture bytes if provided, can only be 128 and 256
4	400	1701	The cidrs provided are not present in the resource :: <list>
5	400	1701	The cidrs provided for addition are already present in the resource :: <list>
6	400	1701	Invalid CIDR notation : <list>
7	400	1701	Duplicate CIDR entry : <list>
8	400	1001	IP list is required
9	500	1001	Internal server errors

Get All Alerts

This URL retrieves all alerts.

Resource URL

GET /alerts? domainId=<domain_id>&includeChildDomain=<true/false>&alertstate=<state>&timeperiod=<timeperiod>&starttime=<start_time>&endtime=<endBtime>&search=<search_string>&page=<page>&filter=<filterBvalue>

Request Parameters

Query Parameters:

Field Name	Description	Data Type	Mandatory
`alertstate`	Alert state, values allowed are, ANY/Acknowledged/Unacknowledged	String	No
`timeperiod`	Time period, allowed values are • LAST_5_MINUTES • Last_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_7_DAYS • LAST_14_DAYS • CUSTOM	String	No
`starttime`	Start time	String	No
`endtime`	End time	String	No
`Page`	Next/Previous	String	No
`domainId`	Domain ID. Default value is 0.	Number	Yes
`includeChildDomain`	Chooses to include child domain or not. Default value is true.	Boolean	Yes
`search`	Search	String	No
`Filter`	Filter on following column is allowed name, assignTo, application, layer7Data, result, attackCount, relevance, alertId, direction, device, domain, interface, attackSeverity, nspId, btp, attackCategory, malwarefileName,	String	No

Field Name	Description	Data Type	Mandatory
	malwarefileHash, malwareName, malwareConfidence, malwareEngine ,executableName, executableHash, executableConfidenceName, attackerIPAddress, attackerPort, attackerRisk, attackerProxyIP, attackerHostname, targetIPAddress, targetPort, targetRisk, targetProxyIP, targetHostname, botnetFamily Ex: name:Malware;direction:Inbound,Outbound;attackcount:>3,<4		

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`totalAlertsCount`	Total alerts count	Number
`retrievedAlertsCount`	Retrieved alerts count	Number
`alertsList`	List of alerts	ObjectList

Details of alerts:

Field Name	Description	Data Type
`name`	Alert name	String
`uniqueAlertId`	Unique alert id	Number
`alertState`	List of alerts	Object
`assignTo`	Assignment	String
`attackSeverity`	Attack severity	String
`event`	Event details	Object
`attack`	Attack details	Object
`attacker`	Attacker details	Object
`target`	Target details	Object
`malwareFile`	Malware file	Object
`endpointExcutable`	Endpoint executable	Object
`detection`	Detection	Object
`application`	Application string	String

Field Name	Description	Data Type
layer7Data	Layer 7 information	String

Details of event:

Field Name	Description	Data Type
time	Time	String
direction	Direction	Number
result	Result	String
attackCount	Attack count	String
relevance	Relevance	String
alertId	Alert id	Number
nspId	NSP id	String
btp	Btp	String
attackCategory	Attack category	String

Details of attacker/target:

Field Name	Description	Data Type
ipAddrs	IP address	String
port	Port	String
hostName	Host name	String
country	Country	String
os	OS	String
vmName	VM name	String
proxyIP	Proxy IP	String
user	User	String
risk	Risk	String
networkObject	Network object	String

Details of malwareFile:

Field Name	Description	Data Type
fileName	File name	String
fileHash	File hash	String
malwareName	Malware name	String

Field Name	Description	Data Type
`malwareConfidence`	Malware confidence	String
`engine`	Engine	String
`size`	Size	String

Details of EndpointExecutable:

Field Name	Description	Data Type
`name`	Name	String
`hash`	Hash	String
`malwareConfidence`	Malware confidence	String

Example

Request

GET https://<NSM_IP>/sdkapi/alerts?fromalert=1334242&page=next&timeperiod=custom&starttime=10/10/2015 12:00&endtime=01/12/2015 12:00

Response

```
"totalAlertsCount": 824917, "retrievedAlertsCount": 1000, "alertsList": [ { "name": "DNS: New Dataloc Test
Attack 8-3 (16 bytes)", "uniqueAlertId": "6245941293374082717", "alertState": "UnAcknowledged", "assignTo": "",
"attackSeverity": "Medium", "event": { "time": "Jan 04, 2016 16:24:4", "direction": "Outbound", "result":
"Inconclusive", "attackCount": 1, "relevance": "Unknown", "alertId": "1383009720294233669" }, "attack":
{ "nspId": "0x40307a00", "btp": "Low", "attackCategory": "Exploit" }, "attacker": { "ipAddrs": "1.1.1.10",
"port": 58719, "hostName": "", "country": null, "os": null, "vmName": null, "proxyIP": "", "user": null, "risk":
"Minimal Risk", "networkObject": null }, "target": { "ipAddrs": "1.1.1.9", "port": 53, "hostName": "",
"country": null, "os": null, "vmName": null, "proxyIP": "", "user": null, "risk": "Minimal Risk",
"networkObject": null }, "malwareFile": { "fileName": "", "fileHash": "", "malwareName": "",
"malwareConfidence": "", "engine": "", "size": null }, "endpointExcutable": { "name": "", "hash": "",
"malwareConfidence": "" }, "detection": { "domain": "/My Company", "device": "prabu-6050", "interface":
"5A-5B" }, "application": "DNS", "layer7Data": "" }, { "name": "DNS: New Dataloc Test Attack 8-3 (16 bytes)",
"uniqueAlertId": "6245941293374082716", "alertState": "UnAcknowledged", "assignTo": "", "attackSeverity":
"Medium", "event": { "time": "Jan 04, 2016 16:24:4", "direction": "Outbound", "result": "Inconclusive",
"attackCount": 1, "relevance": "Unknown", "alertId": "1383009720294233668" }, "attack": { "nspId": "0x40307a00",
"btp": "Low", "attackCategory": "Exploit" }, "attacker": { "ipAddrs": "1.1.1.10", "port": 58719, "hostName": "",
"country": null, "os": null, "vmName": null, "proxyIP": "", "user": null, "risk": "Minimal Risk",
"networkObject": null }, "target": { "ipAddrs": "1.1.1.9", "port": 53, "hostName": "", "country": null, "os":
null, "vmName": null, "proxyIP": "", "user": null, "risk": "Minimal Risk", "networkObject": null },
"malwareFile": { "fileName": "", "fileHash": "", "malwareName": "", "malwareConfidence": "", "engine": "",
"size": null }, "endpointExcutable": { "name": "", "hash": "", "malwareConfidence": "" }, "detection":
{ "domain": "/My Company", "device": "prabu-6050", "interface": "5A-5B" }, "application": "DNS", "layer7Data":
"" } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	3704	Invalid filter value
2	404	9803	Sensor id is required
3	404	9803	Manager name is required

Delete All Alerts

This URL is used to delete all alerts.

Resource URL

DELETE /alerts? alertstate=<state> &timeperiod==<timeperiod> &starttime==<start_time> &endtime=<end_time>&search=<search_strng>&filter=<filter_value>

Request Parameters

Query Parameters:

Field Name	Description	Data Type	Mandatory
`alertstate`	Alert state, values allowed are, ANY/Acknowledged/ Unacknowledged	String	No
`timeperiod`	Time period, allowed values are • LAST_5_MINUTES • Last_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_7_DAYS • LAST_14_DAYS • CUSTOM	String	No
`starttime`	Start time	String	No
`endtime`	End time		No
`search`	Search	String	No
`Filter`	Filter on following column is allowed name, assignTo, application, layer7Data, result, attackCount, relevance, alertId, direction, device, domain, interface, attackSeverity, nspId, btp, attackCategory, malwarefileName, malwarefileHash, malwareName, malwareConfidence, malwareEngine ,executableName, executableHash, executableConfidenceName, attackerIPAddress, attackerPort, attackerRisk, attackerProxyIP, attackerHostname, targetIPAddress, targetPort, targetRisk, targetProxyIP, targetHostname, botnetFamily Ex: name:Malware;direction:Inbound,Outbound;attackcount:>3,<4	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/alerts?fromalert=1334242&page=next&timeperiod=custom&starttime=10/10/2015 12:00&endtime=01/12/2015 12:00

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	3704	Invalid filter value
2	404	9803	Sensor id is required
3	404	9803	Manager name is required

Update All Alerts

This URL is used to retrieve all alerts.

Resource URL

UPDATE /alerts? alertstate=<state> &timeperiod==<timeperiod> &startime==<start_time> &endtime=<end_time>& search=<search_strng>&filter=<filter_value>

Request Parameters

Query Parameters:

Field Name	Description	Data Type	Mandatory
`alertstate`	Alert state, values allowed are, ANY/Acknowledged/ Unacknowledged	String	No
`timeperiod`	Time period, allowed values are • LAST_5_MINUTES • Last_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	No

Field Name	Description	Data Type	Mandatory
	• CUSTOM		
`starttime`	Start time	String	No
`endtime`	End time	String	No
`search`	Search	String	No
`Filter`	Filter on following column is allowed name, assignTo, application, layer7Data, result, attackCount, relevance, alertId, direction, device, domain, interface, attackSeverity, nspId, btp, attackCategory, malwarefileName, malwarefileHash, malwareName, malwareConfidence, malwareEngine ,executableName, executableHash, executableConfidenceName, attackerIPAddress, attackerPort, attackerRisk, attackerProxyIP, attackerHostname, targetIPAddress, targetPort, targetRisk, targetProxyIP, targetHostname, botnetFamily Ex: name:Malware;direction:Inbound,Outbound;attackcount:>3,<4	String	No

Payload parameters:

Field Name	Description	Data Type
`alertState`	Alert state	String
`assignTo`	User id	String

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

UPDATE https://<NSM_IP>/sdkapi/alerts?fromalert=1334242&page=next&timeperiod=custom&starttime=10/10/2015 12:00&endtime=01/12/2015 12:00

```
{ "alertState": "Acknowledged", "assignTo": "admin" }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	3704	Invalid filter value
2	404	9803	Sensor id is required
3	404	9803	Manager name is required

Get Alert Details

This URL is used to retrieve the alert details.

Resource URL

GET /alerts/<alert_uuid>?sensorId=<sensor_id>&manager=<manager_name>

Request Parameters

Query Parameters:

Field Name	Description	Data Type	Mandatory
Alert_uuid	Alert uuid	Number	Yes
sensorId	Sensor id	Number	Yes
manager	Name of the Manager. Required in case a multiple Managers are monitored with a single Manager.	String	No

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
name	Name	String
uniqueAlertId	Unique alert id	String
alertState	Alert state	String
summary	Summary	Object
details	Details	Object
description	Description	Object

Example

Request

GET https://<NSM_IP>/sdkapi/alerts/6245941293374080682

Response

```
{ "name": "DNS: IQUERY Buffer Overflow", "uniqueAlertId": "6806386691967877137", "alertState": "UnAcknowledged",
"assignTo": "---", "summary": { "event": { "application": "Not Available", "protocol": "telnet", "domain": "/My
Company", "manager": null, "device": "vm600-nsmapi-cc", "deviceId": "1001", "interface": "1-2", "matchedPolicy":
"Default Prevention", "zone": null, "vlan": "-10", "detection": "Application anomaly", "time": "Apr 23, 2020
22:26:13", "direction": "Inbound", "result": "Inconclusive", "attackCount": 1, "relevance": "Unknown",
"alertId": "6806386691964665876" }, "attacker": { "ipAddrs": "60.131.8.49", "port": 17561, "hostName": null,
"country": null, "os": "Microsoft Windows Server 2008", "vmName": null, "proxyIP": null, "user": "Unknown",
"risk": "N/A", "networkObject": "---" }, "target": { "ipAddrs": "0.20.209.51", "port": 58004, "hostName": null,
"country": null, "os": "Microsoft Windows Server 2003 Service Pack 1", "vmName": null, "proxyIP": null, "user":
"Unknown", "risk": "N/A", "networkObject": "---" }, "source": null, "destination": null, "zoombie": null,
"cAndcServer": null, "fastFluxAgent": null, "attackedHIPEndpoint": null, "compromisedEndpoint": null },
"details": { "matchedSignature": { "signatureName": "IQUERY-overflow-iquery.c", "signature": { "name":
"Signature#1", "conditions": [ "condition 1", " dns-request-hdr-opcode == 1 ( unsigned )", "[AND] dns-request-
answer-type == 1 ( unsigned )", "[AND] dns-request-answer-class == 1 ( unsigned )", "[AND] dns-request-answer-
rdata matches \"(\\xeb\\x6e\\x5e\\xc6\\x06\\x9a\\x31\\xc9\\x89\\x4e\\x01|\\x80\\xe8\\xd7\\xff\\xff\\xff/bin/sh)
\" ( case-sensitive )" ] } }, "layer7": null, "malwareFile": null, "hostSweep": null, "portScan": null,
"fastFlux": null, "triggeredComponentAttacks": null, "sqlInjection": null, "callbackDetectors": null,
"exceededThreshold": null, "communicationRuleMatch": null }, "description": { "definition": "BIND is used by
most UNIX DNS servers, and implements the Domain Name Service (DNS) protocol. Certain versions of BIND do not
properly bounds check a memory copy when responding to an inverse query (IQUERY) request. An improperly or
maliciously formatted inverse query in a TCP stream can crash the server or allow an attacker to execute
arbitrary code, possibly gaining root privileges.\n\nBuffer overflow vulnerabilities can be exploited to cause a
denial of service or enable the execution of arbitrary code with the privileges of the affected server or
process.\n\nThe inverse query feature is disabled by default, so only those systems that have been explicitly
configured to allow it are vulnerable. Inverse queries can be disabled with little ill effect to prevent this
attack.\n\nUpgrade to the latest applicable version of BIND as listed in CERT Advisory CA-98.05. Upgrading to
the latest version of BIND 8 is recommended. <br> <br> For SunOS 2.x, apply the necessary patch as listed in Sun
Microsystems, Inc. Security Bulletin #00180.\n\nSoftware Packages <br>Internet Software Consortium
BIND<ul><ul><li>4.9.6 to 4.9.6</li></ul><ul><li>8.1 to 8.1.1</li></ul></ul>", "btp": "Low", "rfSB": "Yes",
"protectionCategory": "[Server Protection/Name Servers]", "target": "Server", "httpResponseAttack": "No",
"priority": "High", "protocols": "dns", "attackCategory": "Exploit", "attackSubCategory": "Buffer Overflow",
"snortEngine": "---", "versionAdded": "10.8.1.6", "versionUpdated": "10.8.1.6", "reference": { "nspId":
"0x40300200", "cveId": "CVE-1999-0009", "microsoftId": "", "bugtraqId": "134", "certId": null, "arachNidsId":
"", "additionInfo": "http://www.cert.org/advisories/CA-98.05.bind_problems.html" }, "signatures": [ { "name":
"Signature#1", "conditions": [ "condition 1", " dns-request-hdr-opcode == 1 ( unsigned )", "[AND] dns-request-
answer-type == 1 ( unsigned )", "[AND] dns-request-answer-class == 1 ( unsigned )", "[AND] dns-request-answer-
rdata matches \"(\\xeb\\x6e\\x5e\\xc6\\x06\\x9a\\x31\\xc9\\x89\\x4e\\x01|\\x80\\xe8\\xd7\\xff\\xff\\xff/bin/sh)
\" ( case-sensitive )" ] }, { "name": "Signature#2", "conditions": [ "condition 1", " dns-request-hdr-opcode ==
1 ( unsigned )", "[AND] dns-request-answer-type == 1 ( unsigned )", "[AND] dns-request-answer-class == 1
( unsigned )", "[AND] dns-request-answer-rdata matches \"(\\xff\\xff\\xff/usr/bin/X11/xterm\\xff-display|\\xe8\
\xd7\\xff\\xff\\xff/tmp/hi)\" ( case-sensitive )" ] }, { "name": "Signature#3", "conditions": [ "condition 1", "
dns-request-hdr-opcode == 1 ( unsigned )", "[AND] dns-error-code == host-ip-addr-len-too-long ( unsigned )",
"[AND THEN] condition 2", "[Any Of]", " System Event Name=\"shellcode-detected-for-arch-i386\" ", "[OR] System
Event Name=\"shellcode-detected-for-arch-sparc\" ", "[OR] System Event Name=\"shellcode-detected-for-arch-
powerpc\" " ] }, { "name": "Signature#4", "conditions": [ "condition 1", " dns-request-hdr-opcode == 1
( unsigned )", "[AND] dns-error-code == iquery-overflow ( unsigned )", "[AND THEN] condition 2", "[Any Of]", "
System Event Name=\"shellcode-detected-for-arch-i386\" ", "[OR] System Event Name=\"shellcode-detected-for-arch-
sparc\" ", "[OR] System Event Name=\"shellcode-detected-for-arch-powerpc\" " ] }, { "name": "Signature#5",
"conditions": [ "condition 1", " dns-request-hdr-opcode == 1 ( unsigned )", "[AND] dns-error-code == iquery-
overflow ( unsigned )" ] } ], "componentAttacks": [], "comments": { "comments": "", "availabeToChildDomains":
true, "parentDomainComments": null } } }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	9803	Invalid alert id
2	404	9803	Sensor id is required
3	404	9803	Manager name is required

Update Alert Details

This URL is used to update a single alert.

Resource URL

UPDATE /alerts/<alert_uuid>?sensorId=<sensor_id>&manager=<manager_name>

Request Parameters

Query Parameters:

Field Name	Description	Data Type	Mandatory
`Alert_uuid`	Alert uuid	Number	Yes
`sensorId`	Sensor id	Number	Yes
`manager`	Name of the Manager. Required in case a multiple Managers are monitored with a single Manager.	String	No

Payload Parameters:

Field Name	Description	Data Type
`alertState`	Alert state	String
`assignTo`	User id	String

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
status	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

UPDATE https://<NSM_IP>/sdkapi/alerts/66692334234234

```
{ "alertState": "Acknowledged", "assignTo": "admin" }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	9803	Invalid alert id
2	404	9803	Sensor id is required
3	404	9803	Manager name is required

Delete Alert

This URL is used to delete a single alert.

Resource URL

DELETE /alerts/<alert_uuid>?sensorId=<sensor_id>&manager=<manager_name>

Request Parameters

Query Parameters:

Field Name	Description	Data Type	Mandatory
`Alert_uuid`	Alert uuid	Number	Yes
`sensorId`	Sensor id	Number	Yes
`manager`	Name of the Manager. Required in case a multiple Managers are monitored with a single Manager.	String	No

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
status	Set to 1 if the operation was successful, -1 otherwise	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/alerts/66692334234234

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	9803	Invalid alert id
2	404	9803	Sensor id is required
3	404	9803	Manager name is required

Get Component Alert Packet Log

This URL returns the packet log files related to the component alerts in a ZIP file.

Resource URL

GET /alerts/<alert_id>/triggeredpkt

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`alert_id`	Alert uuid	Number	Yes

Query Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes
`manager`	Name of the Manager. Required in case a multiple Managers are monitored with a single Manager.	String	No

Response Parameters

Returns packet log files associated with the alert in a ZIP file.

Example

Request

GET https://<NSM_IP>/sdkapi/alerts/12345678/triggeredpkt?sensorId=1001

Payload

NA

Response

<packet logs data in ZIP file>

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	9803	Invalid alert id
2	404	9803	Sensor id is required
3	404	9803	Manager name is required

Get Packet Capture of an Alert

This URL returns packet capture file data associated with the alert.

Resource URL

GET /domain/<domainId>/threatanalysis/packetlog?alertId=<alertId>&device=<deviceName>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Query Parameters:

Field Name	Description	Data Type	Mandatory
`alertId`	Alert id	Number	Yes
`device`	Name of the device required in case multiple devices are managed by a single Manager.	String	No

Response Parameters

Returns packet capture file data associated with the alert.

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/threatanalysis/packetlog?alertId=103&device=NS-9200

Payload

NA

Response

<packet capture file data>

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Get the Traffic Send/Received Statistics

This URL is used to retrieve the traffic send/received statistics for the Sensor.

Resource URL

GET /sensor/{sensorId}/port/{portId}/trafficstats/trafficrxtx

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes
`portId`	Port id belonging to the device mentioned	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`totalBytesSent`	Total bytes sent on the given port of the Sensor	String
`totalBytesReceived`	Total bytes received at the given port of the Sensor	String
`totalPacketsSent`	Total number of packets sent on the given port of the Sensor	String
`totalPacketsReceived`	Total number of packets received at the given port of the Sensor	String
`packetsUnicastSent`	Total number of unicast packets sent on the given port of the Sensor	String
`packetsUnicastReceived`	Total number of unicast packets received at the given port of the Sensor	String
`packetsBroadcastSent`	Total number of broadcast packets sent on the given port of the Sensor	String
`packetsBroadcastReceived`	Total number of broadcast packets received at the given port of the Sensor	String
`packetsMulticastSent`	Total number of multicast packets sent on the given port of the Sensor	String
`packetsMulticastReceived`	Total number of multicast packets received at the given port of the Sensor	String
`crcErrorsSent`	Total number of packets sent with crc errors on a given port of the Sensor	String

Field Name	Description	Data Type
`crcErrorsReceived`	Total number of packets sent with crc errors at a given port of the Sensor	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1009/port/124/trafficstats/trafficrxtx

Response

```
{ "totalBytesSent": "4800", "totalBytesReceived": "2374734758", "totalPacketsSent": "63",
"totalPacketsReceived": "2828977", "packetsUnicastSent": "62", "packetsUnicastReceived": "2828956",
"packetsBroadcastSent": "1", "packetsBroadcastReceived": "19", "packetsMulticastSent": "0",
"packetsMulticastReceived": "2", "crcErrorsSent": "0", "crcErrorsReceived": "0" }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404		Invalid Sensor: When the device id given is not valid
2	404		Invalid port: If the given port does not belong to the device

Get the Flows Statistics

This URL is used to retrieve the flows statistics for a Sensor.

Resource URL

GET /sensor/{sensorId}/trafficstats/flows

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`overallFlowUsage`	Shows overall flow usage for a given Sensor	String
`inboundSynCookieProtection`	Shows whether inbound SYN cookie protection is active or inactive. Can have two values: • Inactive • Active	String

Field Name	Description	Data Type
`outboundSynCookieProtection`	Shows whether outbound SYN cookie protection is active or inactive. Can have two values: • Inactive • Active	String
`totalFlowsProcessed`	Shows total number of flows processed	String
`totalFlowsActive`	Shows total number of active flows	String
`totalFlowsActiveUsingSYNcookies`	Shows total number of active flows using SYN cookies	String
`totalFlowsInSYNState`	Shows total number of flows using SYN state	String
`totalFlowsInTimeWaitState`	Shows total number of flows using wait state	String
`totalFlowsInactive`	Shows total number of inactive flows	String
`totalFlowsTimedOut`	Shows total number of flows that are timed out	String
`udpFlowsActive`	Shows total number of active UDP flows	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1009/trafficstats/flows

Response

```
{ "overallFlowUsage":0, "inboundSynCookieProtection":"Inactive", "outboundSynCookieProtection":"Inactive",
"totalFlowsProcessed":59271, "totalFlowsActive":0, "totalFlowsActiveUsingSYNcookies":0, "totalFlowsInSYNState":
0, "totalFlowsInTimeWaitState":0, "totalFlowsInactive":205, "totalFlowsTimedOut":4287, "udpFlowsActive":0 }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404		Invalid Sensor: When the device id given is not valid

Get Dropped Packets Statistics

This URL is used to retrieve the statistics for the packets dropped on a given port of a device.

Resource URL

GET /sensor/{sensorId}/port/{portId/trafficstats/droppedpackets

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensorId	Sensor id	Number	Yes
portId	Port id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
crcFailures	Packets dropped due to crc failures	String
devicePowerUp	Packets dropped during device power up	String
deviceResourceExhaustion	Packets dropped due to device resource exhaustion	String
fragementReAssemblyTimeoutIPv4	IPv4 packets dropped due to fragment reassembly timeout	String
fragementReAssemblyTimeoutIPv6	IPv6 packets dropped due to fragment reassembly timeout	String
incorrectChecksumsICMPv4	ICMPv4 packets dropped due to incorrect checksum	String
incorrectChecksumsICMPv6	ICMPv6 packets dropped due to incorrect checksum	String
incorrectChecksumsIP	IP packets dropped due to incorrect checksum	String
incorrectChecksumsTCP	TCP packets dropped due to incorrect checksum	String
incorrectChecksumsUDP	UDP packets dropped due to incorrect checksums	String
invalidConnections	Packets dropped due to invalid connections	String
offsetIndexLengthErrors	Packets dropped due to errors in offset index length	String
otherLayer2Errors	Packets dropped due to errors in layer 2	String
outOfOrderReassemblyTimeoutsTCP	TCP packets dropped due to out of order reassembly timeout	String
policyResponseActionsFirewall	Packets dropped due to firewall policy response action	String
policyResponseActionsIPS	Packets dropped due to IPS policy response action	String

Field Name	Description	Data Type
`policyResponseActionsIPv4Quarantine`	Packets dropped due to IPv4 quarantine policy response action	String
`policyResponseActionsIPv6Quarantine`	Packets dropped due to IPv6 quarantine policy response action	String
`protocolErrorsICMPv4`	ICMPv4 packets dropped due to protocol errors	String
`protocolErrorsICMPv6`	ICMPv6 packets dropped due to protocol errors	String
`protocolErrorsIPv4`	IPv4 packets dropped due to protocol errors	String
`protocolErrorsIPv6`	IPv6 packets dropped due to protocol errors	String
`protocolErrorsTCP`	TCP packets dropped due to protocol errors	String
`protocolErrorsUDP`	UDP packets dropped due to protocol errors	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1009/port/124/trafficstats/droppedpackets

Response

```
{ "crcFailures": 0, "devicePowerUp": 0, "deviceResourceExhaustion": 0, "fragementReAssemblyTimeoutIPv4": 0,
"fragementReAssemblyTimeoutIPv6": 0, "incorrectChecksumsICMPv4": 0, "incorrectChecksumsICMPv6": 0,
"incorrectChecksumsIP": 0, "incorrectChecksumsTCP": 0, "incorrectChecksumsUDP": 0, "invalidConnections": 16538,
"offsetIndexLengthErrors": 0, "otherLayer2Errors": 0, "outOfOrderReassemblyTimeoutsTCP": 63233,
"policyResponseActionsFirewall": 0, "policyResponseActionsIPS": 2, "policyResponseActionsIPv4Quarantine": 0,
"policyResponseActionsIPv6Quarantine": 0, "protocolErrorsICMPv4": 0, "protocolErrorsICMPv6": 0,
"protocolErrorsIPv4": 0, "protocolErrorsIPv6": 0, "protocolErrorsTCP": 2257, "protocolErrorsUDP": 0 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404		Invalid Sensor: When the device id given is not valid
2	404		Invalid port: If the port id given does not belong to device

Get Malware Stats Grouped by Engine

This URL is used to retrieve the malware statistics grouped by engines for a Sensor.

Resource URL

GET /sensor/{sensorId}/trafficstats/malwarestatsgroupbyengine

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`engine`	Name of the engine for which the statistics(values) is given	String
`values`	Values of traffic statistics parameters for the given engine	Object

Details of values:

Field Name	Description	Data Type
`filesSubmitted`	Number of files submitted	String
`filesIgnored`	Number of files ignored	String
`filesProcessed`	Number of files processed	String
`atdFilesDroppedUnderLoad`	Number of ATD files dropped	String
`atdStaticAnalysis`	Number of ATD static analysis	String
`atdDynamicAnalysis`	Number of ATD dynamic analysis	String
`atdCacheReferences`	Number of ATD cache references	String
`cleanFiles`	Number of clean files out of all the files submitted	String
`veryHighMalwareConfidenceMatches`	Number of files with very high malware confidence matches	String
`highMalwareConfidenceMatches`	Number of files with high malware confidence matches	String
`mediumMalwareConfidenceMatches`	Number of files with medium malware confidence matches	String
`lowMalwareConfidenceMatches`	Number of files with low malware confidence matches	String
`veryLowMalwareConfidenceMatches`	Number of files with very low malware confidence matches	String
`unknownMalwareConfidenceMatches`	Number of files with unknown malware confidence matches	String

Field Name	Description	Data Type
`alertsGenerated`	Number of alerts generated	String
`filesBlocked`	Number of files blocked	String
`connectionsReset`	Number of connection resets	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1009/trafficstats/malwarestatsgroupbyengine

Response

```
{ "mlawareEngineTrafficStats":[ { "engine":"Blocklist", "values":{ "filesSubmitted":0, "filesIgnored":0,
"filesProcessed":0, "atdFilesDroppedUnderLoad":0, "atdStaticAnalysis":0, "atdDynamicAnalysis":0,
"atdCacheReferences":0, "cleanFiles":0, "veryHighMalwareConfidenceMatches":0, "highMalwareConfidenceMatches":0,
"mediumMalwareConfidenceMatches":0, "lowMalwareConfidenceMatches":0, "veryLowMalwareConfidenceMatches":0,
"unknownMalwareConfidenceMatches":0, "alertsGenerated":0, "filesBlocked":0, "connectionsReset":0 } },
{ "engine":"GTI File Reputation", "values":{ "filesSubmitted":0, "filesIgnored":0, "filesProcessed":0,
"atdFilesDroppedUnderLoad":0, "atdStaticAnalysis":0, "atdDynamicAnalysis":0, "atdCacheReferences":0,
"cleanFiles":0, "veryHighMalwareConfidenceMatches":0, "highMalwareConfidenceMatches":0,
"mediumMalwareConfidenceMatches":0, "lowMalwareConfidenceMatches":0, "veryLowMalwareConfidenceMatches":0,
"unknownMalwareConfidenceMatches":0, "alertsGenerated":0, "filesBlocked":0, "connectionsReset":0 } },
{ "engine":"PDFEmulation", "values":{ "filesSubmitted":0, "filesIgnored":0, "filesProcessed":0,
"atdFilesDroppedUnderLoad":0, "atdStaticAnalysis":0, "atdDynamicAnalysis":0, "atdCacheReferences":0,
"cleanFiles":0, "veryHighMalwareConfidenceMatches":0, "highMalwareConfidenceMatches":0,
"mediumMalwareConfidenceMatches":0, "lowMalwareConfidenceMatches":0, "veryLowMalwareConfidenceMatches":0,
"unknownMalwareConfidenceMatches":0, "alertsGenerated":0, "filesBlocked":0, "connectionsReset":0 } },
{ "engine":"Flash Analysis Engine", "values":{ "filesSubmitted":0, "filesIgnored":0, "filesProcessed":0,
"atdFilesDroppedUnderLoad":0, "atdStaticAnalysis":0, "atdDynamicAnalysis":0, "atdCacheReferences":0,
"cleanFiles":0, "veryHighMalwareConfidenceMatches":0, "highMalwareConfidenceMatches":0,
"mediumMalwareConfidenceMatches":0, "lowMalwareConfidenceMatches":0, "veryLowMalwareConfidenceMatches":0,
"unknownMalwareConfidenceMatches":0, "alertsGenerated":0, "filesBlocked":0, "connectionsReset":0 } } ] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor: When the device id given is not valid

Get Malware Stats Grouped by File Type

This URL retrieves the malware statistics grouped by file type for a given Sensor.

Resource URL

GET /sensor/{sensorId}/trafficstats/malwarestatsgroupbyfile

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`fileType`	File type for which statistics will be given	String
`filesProcessed`	Number of files processed for a given file type	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1009/trafficstats/malwarestatsgroupbyfile

Response

```
{ "malwareEngineTrafficStatsByFile": [ { "fileType": "PE (EXE,DLL,SYS,COM,etc.) Files", "filesProcessed": 0 },
{ "fileType": "PDF Files", "filesProcessed": 0 }, { "fileType": "Flash Files", "filesProcessed": 0 },
{ "fileType": "MS Office Files", "filesProcessed": 0 }, { "fileType": "APK Files", "filesProcessed": 0 },
{ "fileType": "JAR Files", "filesProcessed": 0 }, { "fileType": "Compressed (Zip,RAR) Files", "filesProcessed":
0 } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404		Invalid Sensor: When the device id given is not valid

Get Traffic Statistics for Advance Callback Detection

This URL is used to retrieve traffic statistics for advance callback detection for a Sensor.

Resource URL

GET /sensor/{sensorId}/trafficstats/advcallbackdetectionstats

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`callbackDetectorsAlerts`	Number of alerts generated due to advanced callback detection	String
`dgaZombieDetectionAlerts`	Number of alerts due to dga zombie detection	String
`dgaCncServerDetectionAlerts`	Number of alerts due to dga cnc server detection	String

Field Name	Description	Data Type
`dgaCncServerConnectionAlerts`	Number of alerts due to dga cnc server connection	String
`fastFluxDnsDetectionAlerts`	Number of alerts due to fast flux dns detection	String
`connectionToFastFluxAgentsAlerts`	Number of alerts due to connection to fast flux agents	String
`zeroDayBotnetDetectionAlerts`	Number of alerts due to zero day botnet detection	String
`knownBotnetDetectionAlerts`	Number of known botnet detection alerts	String

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1009/trafficstats/advcallbackdetectionstats

Response

```
{ "callbackDetectorsAlerts": 39, "dgaZombieDetectionAlerts": 90, "dgaCncServerDetectionAlerts": 40,
"dgaCncServerConnectionAlerts": 30, "fastFluxDnsDetectionAlerts": 1, "connectionToFastFluxAgentsAlerts": 1,
"zeroDayBotnetDetectionAlerts": 3, "knownBotnetDetectionAlerts": 0 }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404		Invalid Sensor: When the device id given is not valid

Get the Traffic Statistics for the SSL

This URL is used to retrieve traffic statistics for SSL for a Sensor.

Resource URL

GET /sensor/{sensorId}/trafficstats/sensorsslstats

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`recycledSSLFlows`	Recycled SSL flows	Number

Field Name	Description	Data Type
`sslFlowAllocationErrors`	SSL flow allocation errors	Number
`skippedSSLFlowsDueFlowAllocationErrors`	Skipped SSL flows due to flow allocation errors	Number
`packetsReceivedFromUnknownSSLFlows`	Packets received from unknown SSL flows	Number
`sslFlowsUsingUnsupportedDiffieHellmanCipherSuite`	SSL flows using unsupported Diffie-Hellman cipher suite	Number
`sslFlowsUsingUnsupportedExportCipher`	SSL flows using unsupported export cipher	Number
`sslFlowsUsingUnsupportedOrUnknownCipher`	SSL flows using unsupported or unknown cipher	Number

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1009/trafficstats/sensorsslstats

Response

```
{ "recycledSSLFlows": 0, "sslFlowAllocationErrors": 0, "skippedSSLFlowsDueFlowAllocationErrors": 0,
"packetsReceivedFromUnknownSSLFlows": 0, "sslFlowsUsingUnsupportedDiffieHellmanCipherSuite": 0,
"sslFlowsUsingUnsupportedExportCipher": 0, "sslFlowsUsingUnsupportedOrUnknownCipher": 0 }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404		Invalid Sensor: When the device id given is not valid

Get the Traffic Statistics for Outbound SSL

This URL is used to retrieve traffic statistics for outbound SSL for a Sensor.

Resource URL

GET /sensor/{sensorId}/trafficstats/outboundsslstats

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
sslConnectionAttemptsFromClientToSensor	SSL connection attempts from the client to the Sensor	Number
sslConnectionAttemptsFromSensorToWebServer	SSL connection attempts from the Sensor to the web server	Number
endToEndSSLHandshakesInProgress	End-to-end SSL handshakes in progress	Number
endToEndSSLFlowsEstablished	End-to-end SSL flows established	Number
allowedSSLFlows	Allowed SSL flows	Number
attacksDetectedInSSLFlows	Attacks detected in SSL flows	Number
RSAFlows	RSA flows	Number
diffieHellmanFlows	Diffie-Hellman flows	Number
nonSSLFlows	Non SSL flows	Number
untrustedCertificates	Untrusted certificates	Number
sslFlowsBlockedOrSkippedFromUntrustedCertificates	SSL flows blocked or skipped due to untrusted certificates	Number
sslFlowsBlockedOrSkippedFromUnsupportedCipherSuite	SSL flows blocked or skipped due to unsupported cipher suites	Number
sslFlowsBlockedOrSkippedFromGeneralDecryptionFailures	SSL flow blocked or skipped due to general decryption failures	Number

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1009/trafficstats/outboundsslstats

Response

```
{ "sslConnectionAttemptsFromClientToSensor": 0, "sslConnectionAttemptsFromSensorToWebServer": 0,
"endToEndSSLHandshakesInProgress": 0, "endToEndSSLFlowsEstablished": 0, "allowedSSLFlows": 0,
"attacksDetectedInSSLFlows": 0, "RSAFlows": 0, "diffieHellmanFlows": 0, "nonSSLFlows": 0,
"untrustedCertificates": 0, "sslFlowsBlockedOrSkippedFromUntrustedCertificates": 0,
"sslFlowsBlockedOrSkippedFromUnsupportedCipherSuite": 0,
"sslFlowsBlockedOrSkippedFromGeneralDecryptionFailures": 0 }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404		Invalid Sensor: When the device id given is not valid

Get the Traffic Statistics for Internal Web Certificate Matches

This URL is used to retrieve traffic statistics for internal web certificate matches for a Sensor.

Resource URL

GET /sensor/{sensorId}/trafficstats/sslinternalwebcertmatches

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensorId	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
unMatchedCertificates	Count of unmatched certificates	Number
matchedCertificates	List of matched certificates	Array

Details of object in matchedCertificates:

Field Name	Description	Data Type
certificateName	Certificate name	String
flows	Number of flows	Number

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1009/trafficstats/sslinternalwebcertmatches

Response

```
{ "unMatchedCertificates": 0, "matchedCertificates": [ { “certificateName": ”: “test”, “flows”: 10 },
{ “certificateName”: “test2", “flows”: 2 } ] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404		Invalid Sensor: When the device id given is not valid

Reset SSL Counters

This URL is used to reset the SSL traffic counters for the Sensor.

Resource URL

GET /sensor/{sensorId}/trafficstats/resetsslcounters

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Returns status as 1 on pass	Number

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1009/trafficstats/resetsslcounters

Response

```
{ "status": 1 }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404		Invalid Sensor: When the device id given is not valid

Get the CLI Auditing Configuration at the Domain Level

This URL gets the CLI auditing configuration at the domain level.

Resource URL

GET /domain/<domainId>/cliauditing

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`inheritSettings`	Inherit settings from parent domain	Boolean
`enable`	CLI auditing enabled or not	Boolean

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/cliauditing

Response

```
{ "inheritSettings": false, "enable": true }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Update the CLI Auditing Configuration at Domain Level

This URL updates the CLI auditing configuration at domain level.

Resource URL

PUT /domain/<domainId>/cliauditing

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`inheritSettings`	Inherit settings from parent domain	Boolean	Yes
`enable`	Enable CLI auditing	Boolean	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/cliauditing

Payload

```
{ "inheritSettings": false, "enable": true }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	3101	Cannot inherit settings for root domain
3	500	1001	Internal server error

Get the CLI Auditing Configuration at Sensor Level

This URL gets the CLI auditing configuration at the Sensor level.

Resource URL

GET /sensor/<sensorId>/cliauditing

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`inheritSettings`	Inherit settings from parent domain	Boolean
`enable`	CLI auditing enabled or not	Boolean

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/cliauditing

Response

```
{ "inheritSettings": false, "enable": true }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1124	The Sensor is inactive

Update the CLI Auditing Configuration at the Sensor Level

This URL updates the CLI auditing configuration at the Sensor level.

Resource URL

PUT /sensor/<sensorId>/cliauditing

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`inheritSettings`	Inherit settings from parent domain	Boolean	Yes
`enable`	Enable CLI auditing	Boolean	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1001/cliauditing

Payload

```
{ "inheritSettings": false, "enable": true }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1124	The Sensor is inactive
3	500	1001	Internal server error

Get the Diagnostic Trace Files

This URL gets the diagnostics trace files.

Resource URL

GET /sensor/<sensor_id>/diagnosticstrace

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensor id`	Sensor id	Number	Yes

Payload Request Parameters: None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`files`	List of diagnostic trace file names	StringList

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/diagnosticstrace

Response

```
{ "files":[“trace_API_2950_2_Thu_Mar_03_13_58_39_IST_2016.enc”,
“trace_API_2950_2_Thu_Mar_03_14_06_15_IST_2016.enc”] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is Inactive.

Upload the Diagnostic Trace File

This URL will upload the diagnostic trace file.

Resource URL

PUT /sensor/<sensor_id>/diagnosticstrace/upload

Request Parameters

URL Parameter

Field Name	Description	Data Type	Mandatory
`sensor id`	Sensor id	Number	Yes

Payload Request Parameters: None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Status returned	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1001/diagnosticstrace/upload

Payload

None

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is Inactive
3	500	1001	Internal error message: There is another request the same as yours to Sensor in progress, Try LATER.

Get the Upload Status

This URL will get the upload status of the diagnostic trace file.

Resource URL

GET /sensor/<sensor_id>/diagnosticstrace/upload

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Payload Request Parameters: None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
updatePercentageComplete	Percentage of the upload process completed	Number
updateStatusMessage	Status of the upload process	String

Example

Request

GET https://<NSM_IP>/sensor/1001/diagnosticstrace/upload

Payload

None

Response

```
{ "updatePercentageComplete": 50, "updateStatusMessage": "IN PROGRESS:Transfer of File Segment in progress
for.... Sensor: sensor" }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive

Export the Diagnostic Trace File Captured

This URL exports the diagnostic trace file.

Resource URL

PUT /sensor/<sensor_id>/diagnosticstrace/export

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensorId	Sensor id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
fileName	Diagnostic trace file name	String	Yes

Response Parameters

Diagnostic trace file data is returned if the request parameters are correct, otherwise error details are returned.

Example

Request

PUT https://<NSM_IP>/sdkapi/sensor/1001/diagnosticstrace/export

Payload

```
{ "fileName": "trace_API_2950_2_Thu_Mar_03_13_58_39_IST_2016.enc" }
```

Response

```
<trace file data>
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is inactive

Delete the Diagnostic Trace File Captured

This URL deletes the diagnostic trace file.

Resource URL

DELETE /sensor/<sensor_id>/diagnosticstrace

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensor id	Sensor id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
fileName	Diagnostic trace file name	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
Status	Status of request,1 if successful.	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/sensor/1001/diagnosticstrace

Payload

```
{ "fileName": "trace_API_2950_2_Thu_Mar_03_13_58_39_IST_2016.enc" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1124	The Sensor is Inactive
3	400	1001	Internal error message: Trace file given is invalid. Could not be deleted

Get the Health Check

This URL gets the health check status.

Resource URL

GET /healthcheck

Request Parameters

URL Parameters: None

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`summary`	Summary feature list	ObjectList
`databaseChecks`	Database check feature list	ObjectList
`connectivityChecks`	Connectivity check feature list	ObjectList
`id`	Feature id	String
`name`	Feature name	String
`result`	Health check run result	String
`indicator`	Status of the check	String
`notes`	Heath check notes	String
`lastRun`	Health check last run time	String
`run`	If the feature check happened	Boolean

Example

Request

GET https://<NSM_IP>/sdkapi/healthcheck

Response

```
{ 'connectivityChecks': [ {'lastRun': 'Tue May 17 10:26:33 IST 2016', 'indicator': 'low', 'run': True, 'name':
'Callback Detectors Update Server Connectivity', 'notes': 'Server: download.nai.com\n Port: TCP 80 \n Response
time: 9690 ms', 'result': 'Pass', 'id': 'CallbackDetectorsUpdateServerConnectivity'}, ... , {'lastRun': 'Tue May
17 10:26:25 IST 2016', 'indicator': '', 'run': True, 'name': 'NSCM Connectivity', 'notes': 'NSCM is not in use
with this Manager', 'result': '', 'id': 'NSCMConnectivity'} ], 'databaseChecks': [ {'lastRun': 'Tue May 17
10:26:23 IST 2016', 'indicator': '', 'run': True, 'name': 'Disk Space Used by MySQL Database Backups', 'notes':
'No backup files detected', 'result': '0 MB', 'id': 'BackupFilesSpaceCheck'}, ... , {'lastRun': 'Tue May 17
10:26:25 IST 2016', 'indicator': 'low', 'run': True, 'name': 'Slow Queries', 'notes': '', 'result': '0', 'id':
'CheckForSlowQueriesInDatabase'} ], 'summary': [ {'lastRun': 'Tue May 17 10:26:23 IST 2016', 'indicator': '',
'run': True, 'name': 'Manager Software Version', 'notes': '', 'result': '8.3.7.20.8', 'id':
'GetNSMVersion'}, ... , {'lastRun': 'Tue May 17 10:26:24 IST 2016', 'indicator': '', 'run': True, 'name':
'Manager Name', 'notes': '', 'result': 'NSM', 'id': 'ManagerNameCheck'} ] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Run the Health Check

This URL runs the health check.

Resource URL

PUT /healthcheck

Request Parameters

URL Parameters: None

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`id`	Feature id list for which the health check should happen Values can be as below: • Single value “defaut”. Which will run health check only for the features which are selected by default • Single value “all”. Which will run health check for all the features • Single value “summary”. Which will run health check for summary features • Single value “databasechecks”. Which will run health check for database check features • Single value “connectivitychecks”. Which will run health check for connectivity check features • List of the feature id for which the health check should run	Array	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`summary`	Summary feature list	ObjectList
`databaseChecks`	Database check feature list	ObjectList

Field Name	Description	Data Type
connectivityChecks	Connectivity check feature list	ObjectList

Details of per feature:

Field Name	Description	Data Type
id	Feature id	String
name	Feature name	String
result	Health check run result	String
indicator	Status of the check	String
notes	Heath check notes	String
lastRun	Health check last run time	String
run	If the feature check happened	Boolean

Example

Request

PUT https://<NSM_IP>/healthcheck

Payload Examples

```
{ "id": [“all”] } { "id": [“default”] } { "id": [“summary”] } { "id":
[“CallbackDetectorsUpdateServerConnectivity”, “NSCMConnectivity”, “BackupFilesSpaceCheck”,
“CheckForSlowQueriesInDatabase”, “GetNSMVersion”, “ManagerNameCheck”] }
```

Response

```
{ 'connectivityChecks': [ {'lastRun': 'Tue May 17 10:26:33 IST 2016', 'indicator': 'low', 'run': True, 'name':
'Callback Detectors Update Server Connectivity', 'notes': 'Server: download.nai.com\n Port: TCP 80 \n Response
time: 9690 ms', 'result': 'Pass', 'id': 'CallbackDetectorsUpdateServerConnectivity'}, ... , {'lastRun': 'Tue May
17 10:26:25 IST 2016', 'indicator': '', 'run': True, 'name': 'NSCM Connectivity', 'notes': 'NSCM is not in use
with this Manager', 'result': '', 'id': 'NSCMConnectivity'} ], 'databaseChecks': [ {'lastRun': 'Tue May 17
10:26:23 IST 2016', 'indicator': '', 'run': True, 'name': 'Disk Space Used by MySQL Database Backups', 'notes':
'No backup files detected', 'result': '0 MB', 'id': 'BackupFilesSpaceCheck'}, ... , {'lastRun': 'Tue May 17
10:26:25 IST 2016', 'indicator': 'low', 'run': True, 'name': 'Slow Queries', 'notes': '', 'result': '0', 'id':
'CheckForSlowQueriesInDatabase'} ], 'summary': [ {'lastRun': 'Tue May 17 10:26:23 IST 2016', 'indicator': '',
'run': True, 'name': 'Manager Software Version', 'notes': '', 'result': '8.3.7.20.8', 'id':
'GetNSMVersion'}, ... , {'lastRun': 'Tue May 17 10:26:24 IST 2016', 'indicator': '', 'run': True, 'name':
'Manager Name', 'notes': '', 'result': 'NSM', 'id': 'ManagerNameCheck'} ] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	3702	Invalid id provided: <list of invalid ids>

Get the McAfee Cloud Integration Settings

This URL gets the McAfee cloud integration settings.

Resource URL

GET /mcafeecloudintegration

Request Parameters

URL Parameters: None

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`enable`	Is the integration enabled	Boolean
`tenantId`	Tenant id on the Manager	String
`tenantIdStatus`	Tenant id status	String
`provisioningKey`	Provisioning key of the Manager	String
`statistics`	McAfee cloud statistics	Object

Details of statistics:

Field Name	Description	Data Type
`totalFilesSubmitted`	Total files submitted to the cloud	Number
`filesSubmittedAfterDailyLimitReached`	Files submitted to the cloud after the daily file submission limit is reached	Number
`veryHighMalwareConfidenceFiles`	Number of very high malware confidence files detected	Number
`highMalwareConfidenceFiles`	Number of high malware confidence files detected	Number
`mediumMalwareConfidenceFiles`	Number of medium malware confidence files detected	Number
`lowMalwareConfidenceFiles`	Number of low malware confidence files detected	Number
`veryLowMalwareConfidenceFiles`	Number of very low malware confidence files detected	Number
`cleanMalwareConfidenceFiles`	Number of clean malware confidence files detected	Number
`lastSubmissionTime`	Time of last file submitted	String
`lastSubmissionFrom`	Initiation of last submission location	String

Field Name	Description	Data Type
`totalSubmissionErrors`	Total submission errors	Number
`lastSubmissionError`	Last submission error cause	String

Example

Request

GET https://<NSM_IP>/sdkapi/mcafeecloudintegration

Response

```
{ 'statistics': { 'veryHighMalwareConfidenceFiles': 0, 'highMalwareConfidenceFiles': 0, 'lastSubmissionTime':
'', 'lastSubmissionFrom': '', 'veryLowMalwareConfidenceFiles': 0, 'lowMalwareConfidenceFiles': 0,
'cleanMalwareConfidenceFiles': 0, 'totalSubmissionErrors': 0, 'mediumMalwareConfidenceFiles': 0,
'totalFilesSubmitted': 0, 'filesSubmittedAfterDailyLimitReached': 0, 'lastSubmissionError': '' }, 'enable':
True, 'tenantIdStatus': 'Present', 'tenantId': 'M46MS8MXle/
AVyAbtyqbxBdPwMPtXZTX1Fj2RibW0Ch68tpnCiMU3V2u1KB4nnNO', 'provisioningKey': 'Ya
+WyijMltOTWuLpzRHSbvK7bLeSewQIzxmx6LzQca0=' }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Update the McAfee Cloud Integration Settings

This URL updates the McAfee cloud integration settings.

Resource URL

PUT /mcafeecloudintegration

Request Parameters

URL Parameters: None

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`enable`	Enable McAfee cloud integration	Boolean	Yes
`tenantId`	Tenant id from ePO	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/mcafeecloudintegration

Payload

```
{ "enable": true, "tenantId": "5JT9TV3F7k9taFget0p37O5shpe0j+1FX8+ggrTZQ1/u99z8vkXzFTjRSkBD4BZu" }
```

Response

```
{ "status": 1 }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal server error

Test the Connection for McAfee Cloud Integration Settings

This URL tests the McAfee cloud integration settings.

Resource URL

PUT /mcafeecloudintegration/testconnection

Request Parameters

URL Parameters: None

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
status	1 is returned if the test connection passes else error	Number

Example

Request

PUT https://<NSM_IP>/mcafeecloudintegraton/testconnection

Response

```
{ "status": 1 }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Get the McAfee Cloud Statistics

This URL gets the McAfee cloud statistics.

Resource URL

GET /mcafeecloudinteration/statistics

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`totalFilesSubmitted`	Total files submitted to the cloud	Number
`filesSubmittedAfterDailyLimitReached`	Files submitted to the cloud after the daily file submission limit is reached	Number
`veryHighMalwareConfidenceFiles`	Number of very high malware confidence files detected	Number
`highMalwareConfidenceFiles`	Number of high malware confidence files detected	Number
`mediumMalwareConfidenceFiles`	Number of medium malware confidence files detected	Number
`lowMalwareConfidenceFiles`	Number of low malware confidence files detected	Number
`veryLowMalwareConfidenceFiles`	Number of very low malware confidence files detected	Number
`cleanMalwareConfidenceFiles`	Number of clean malware confidence files detected	Number
`lastSubmissionTime`	Time of last file submitted	String
`lastSubmissionFrom`	Initiation of last submission location.	String
`totalSubmissionErrors`	Total submission errors	Number
`lastSubmissionError`	Last submission error cause	String

Example

Request

GET https://<NSM_IP>/mcafeecloudintegration/statistics

Response

```
{ 'veryHighMalwareConfidenceFiles': 0, 'highMalwareConfidenceFiles': 0, 'lastSubmissionTime': '',
'lastSubmissionFrom': '', 'veryLowMalwareConfidenceFiles': 0, 'lowMalwareConfidenceFiles': 0,
'cleanMalwareConfidenceFiles': 0, 'totalSubmissionErrors': 0, 'mediumMalwareConfidenceFiles': 0,
'totalFilesSubmitted': 0, 'filesSubmittedAfterDailyLimitReached': 0, 'lastSubmissionError': '' }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal server error

Reset McAfee Cloud Statistics

This URL resets the McAfee cloud statistics.

Resource URL

PUT /mcafeecloudintegration/resetstatistics

Request Parameters

URL Parameters: None

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`status`	1 is returned if the reset passes else error	Number

Example

Request

PUThttps://<NSM_IP>/mcafeecloudintegraton/resetstatistics

Response

```
{ "status": 1 }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Get the Performance Monitoring Settings at the Domain Level

This URL gets the performance monitoring settings at the domain level.

Resource URL

GET /domain/<domainId>/performancemonitoring

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`inheritSettings`	Inherit settings from parent domain	Boolean
`enableMetricCollection`	Enable metric collection	Boolean
`enableThresholdAnalysis`	Enable threshold analysis	Boolean
`visibleToChildAdminDomain`	Settings visible to the child domain	Boolean
`enableCPUUtilizationMetricCollection`	Enable CPU utilization metric collection	Boolean
`enablePortThroughputUtilizationMetricCollection`	Enable port throughput utilization metric collection	Boolean
`thresholds`	List of threshold values	Array
`display`	Display values	Object

Details of object in thresholds:

Field Name	Description	Data Type
`metric`	Metric name	String
`thresholds`	List of threshold details	Array
`thresholdName`	Name of the threshold	String
`direction`	Rising/falling of threshold	String
`thresholdValue`	Threshold value	Number
`resetThresholdValue`	Reset threshold value	Number
`enableAlarm`	Alarm enabled or not	Boolean

Details of display:

Field Name	Description	Data Type
mediumMemoryUsage	Memory usage value to be shown as medium usage	Number
highMemoryUsage	Memory usage value to be shown as high usage	Number
mediumDeviceThroughputUsage	Device throughput usage value to be shown as medium usage	Number
highDeviceThroughputUsage	Device throughput usage value to be shown as high usage	Number

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/performancemonitoring

Response

```
{ "inheritSettings": false, "enableMetricCollection": true, "enableThresholdAnalysis": true,
"visibleToChildAdminDomain": true, "enableCPUUtilizationMetricCollection": true,
"enablePortThroughputUtilizationMetricCollection": true, "thresholds": [{ "metric": "CPU Usage", "thresholds":
[{ "thresholdName": "High Utilization", "direction": "Rising", "thresholdValue": 92, "resetThresholdValue": 72,
"enableAlarm": true }, { "thresholdName": "Medium Utilization", "direction": "Rising", "thresholdValue": 72,
"resetThresholdValue": 52, "enableAlarm": true }] }, { "metric": "Sensor Throughput Usage", "thresholds":
[{ "thresholdName": "High Utilization", "direction": "Rising", "thresholdValue": 91, "resetThresholdValue": 71,
"enableAlarm": false }, { "thresholdName": "Medium Utilization", "direction": "Rising", "thresholdValue": 71,
"resetThresholdValue": 51, "enableAlarm": true }, { "thresholdName": "Under Utilization", "direction":
"Falling", "thresholdValue": 6, "resetThresholdValue": 11, "enableAlarm": true }] }, { "metric": "L2 Error
Drop", "thresholds": [{ "thresholdName": "Too Many L2 Errors", "direction": "Rising", "thresholdValue": 99,
"resetThresholdValue": 51, "enableAlarm": true }] }, { "metric": "L3/L4 Error Drop", "thresholds":
[{ "thresholdName": "Too Many L3/L4 Errors", "direction": "Rising", "thresholdValue": 1001,
"resetThresholdValue": 101, "enableAlarm": true }] }, { "metric": "Memory Usage", "thresholds":
[{ "thresholdName": "High Utilization", "direction": "Rising", "thresholdValue": 91, "resetThresholdValue": 71,
"enableAlarm": false }, { "thresholdName": "Medium Utilization", "direction": "Rising", "thresholdValue": 71,
"resetThresholdValue": 51, "enableAlarm": false }] }], "display": { "mediumMemoryUsage": 76, "highMemoryUsage":
91, "mediumDeviceThroughputUsage": 76, "highDeviceThroughputUsage": 91 } }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	500	1001	Internal error

Update the Performance Monitoring Settings at the Domain Level

This URL updates the performance monitoring settings at the domain level.

Resource URL

PUT /domain/<domainId>/performancemonitoring

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`inheritSettings`	Inherit settings from parent domain	Boolean	Yes
`enableMetricCollection`	Enable metric collection	Boolean	Yes
`enableThresholdAnalysis`	Enable threshold analysis	Boolean	Yes
`visibleToChildAdminDomain`	Settings visible to the child domain	Boolean	Yes
`enableCPUUtilizationMetricCollection`	Enable CPU utilization metric collection	Boolean	Yes
`enablePortThroughputUtilizationMetricCollection`	Enable port throughput utilization metric collection	Boolean	Yes
`thresholds`	List of threshold values	Array	No
`display`	Display values	Object	No

Details of object in thresholds:

Field Name	Description	Data Type	Mandatory
`metric`	Metric name	String	Yes
`thresholds`	List of threshold details	Array	Yes
`thresholdName`	Name of the threshold	String	Yes
`thresholdValue`	Threshold value	Number	Yes
`resetThresholdValue`	Reset threshold value	Number	Yes
`enableAlarm`	Alarm enabled or not	Boolean	Yes

Details of display:

Field Name	Description	Data Type	Mandatory
`mediumMemoryUsage`	Memory usage value to be shown as medium usage	Number	Yes
`highMemoryUsage`	Memory usage value to be shown as high usage	Number	Yes
`mediumDeviceThroughputUsage`	Device throughput usage value to be shown as medium usage	Number	Yes

Field Name	Description	Data Type	Mandatory
highDeviceThroughputUsage	Device throughput usage value to be shown as high usage	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
status	Set to 1 if the operation was successful.	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/performancemonitoring

Payload

```
{ "inheritSettings": false, "enableMetricCollection": true, "enableThresholdAnalysis": true,
"visibleToChildAdminDomain": true, "enableCPUUtilizationMetricCollection": true,
"enablePortThroughputUtilizationMetricCollection": true, "thresholds": [{ "metric": "CPU Usage", "thresholds":
[{ "thresholdName": "High Utilization", "direction": "Rising", "thresholdValue": 92, "resetThresholdValue": 72,
"enableAlarm": true }, { "thresholdName": "Medium Utilization", "direction": "Rising", "thresholdValue": 72,
"resetThresholdValue": 52, "enableAlarm": true }] }, { "metric": "Sensor Throughput Usage", "thresholds":
[{ "thresholdName": "High Utilization", "direction": "Rising", "thresholdValue": 91, "resetThresholdValue": 71,
"enableAlarm": false }, { "thresholdName": "Medium Utilization", "direction": "Rising", "thresholdValue": 71,
"resetThresholdValue": 51, "enableAlarm": true }, { "thresholdName": "Under Utilization", "direction":
"Falling", "thresholdValue": 6, "resetThresholdValue": 11, "enableAlarm": true }] }, { "metric": "L2 Error
Drop", "thresholds": [{ "thresholdName": "Too Many L2 Errors", "direction": "Rising", "thresholdValue": 99,
"resetThresholdValue": 51, "enableAlarm": true }] }, { "metric": "L3/L4 Error Drop", "thresholds":
[{ "thresholdName": "Too Many L3/L4 Errors", "direction": "Rising", "thresholdValue": 1001,
"resetThresholdValue": 101, "enableAlarm": true }] }, { "metric": "Memory Usage", "thresholds":
[{ "thresholdName": "High Utilization", "direction": "Rising", "thresholdValue": 91, "resetThresholdValue": 71,
"enableAlarm": false }, { "thresholdName": "Medium Utilization", "direction": "Rising", "thresholdValue": 71,
"resetThresholdValue": 51, "enableAlarm": false }] }], "display": { "mediumMemoryUsage": 76, "highMemoryUsage":
91, "mediumDeviceThroughputUsage": 76, "highDeviceThroughputUsage": 91 } }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	1111	Cannot inherit settings for main admin domain
3	400	1111	Performance monitoring not supported
4	400	1111	Display parameters should be between 0 and 99
5	400	1111	Medium usage parameter should be greater that high usage parameter
6	400	1111	Threshold values should be greater than 0

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
7	400	1111	Threshold values should be between 1 and 100
8	400	1111	In case of rising, the reset threshold value should be less than threshold value
9	400	1111	In case of falling, the threshold value should be less than reset threshold value
10	500	1001	Internal server error

Get the Performance Monitoring Settings at the Sensor Level

This URL gets the performance monitoring settings at the Sensor level.

Resource URL

GET /sensor/<sensorId>/performancemonitoring

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`inheritSettings`	Inherit settings from the parent domain	Boolean
`enableMetricCollection`	Enable metric collection	Boolean
`enableThresholdAnalysis`	Enable threshold analysis	Boolean
`visibleToChildAdminDomain`	Settings visible to the child domain	Boolean
`enableCPUUtilizationMetricCollection`	Enable CPU utilization metric collection	Boolean
`enablePortThroughputUtilizationMetricCollection`	Enable port throughput utilization metric collection	Boolean
`thresholds`	List of threshold values	Array
`display`	Display values	Object

Details of object in thresholds:

Field Name	Description	Data Type
`metric`	Metric name	String
`thresholds`	List of threshold details	Array
`thresholdName`	Name of the threshold	String
`direction`	Rising/falling of threshold	String
`thresholdValue`	Threshold value	Number
`resetThresholdValue`	Reset threshold value	Number
`enableAlarm`	Alarm enabled or not	Boolean

Details of display:

Field Name	Description	Data Type
`mediumMemoryUsage`	Memory usage value to be shown as medium usage	Number
`highMemoryUsage`	Memory usage value to be shown as high usage	Number
`mediumDeviceThroughputUsage`	Device throughput usage value to be shown as medium usage	Number
`highDeviceThroughputUsage`	Device throughput usage value to be shown as high usage	Number

Example

Request

GET https://<NSM_IP>/sdkapi/sensor/1001/performancemonitoring

Response

```
{ "inheritSettings": false, "enableMetricCollection": true, "enableThresholdAnalysis": true,
"visibleToChildAdminDomain": true, "enableCPUUtilizationMetricCollection": true,
"enablePortThroughputUtilizationMetricCollection": true, "thresholds": [{ "metric": "CPU Usage", "thresholds":
[{ "thresholdName": "High Utilization", "direction": "Rising", "thresholdValue": 92, "resetThresholdValue": 72,
"enableAlarm": true }, { "thresholdName": "Medium Utilization", "direction": "Rising", "thresholdValue": 72,
"resetThresholdValue": 52, "enableAlarm": true }] }, { "metric": "Sensor Throughput Usage", "thresholds":
[{ "thresholdName": "High Utilization", "direction": "Rising", "thresholdValue": 91, "resetThresholdValue": 71,
"enableAlarm": false }, { "thresholdName": "Medium Utilization", "direction": "Rising", "thresholdValue": 71,
"resetThresholdValue": 51, "enableAlarm": true }, { "thresholdName": "Under Utilization", "direction":
"Falling", "thresholdValue": 6, "resetThresholdValue": 11, "enableAlarm": true }] }, { "metric": "L2 Error
Drop", "thresholds": [{ "thresholdName": "Too Many L2 Errors", "direction": "Rising", "thresholdValue": 99,
"resetThresholdValue": 51, "enableAlarm": true }] }, { "metric": "L3/L4 Error Drop", "thresholds":
[{ "thresholdName": "Too Many L3/L4 Errors", "direction": "Rising", "thresholdValue": 1001,
"resetThresholdValue": 101, "enableAlarm": true }] }, { "metric": "Memory Usage", "thresholds":
[{ "thresholdName": "High Utilization", "direction": "Rising", "thresholdValue": 91, "resetThresholdValue": 71,
"enableAlarm": false }, { "thresholdName": "Medium Utilization", "direction": "Rising", "thresholdValue": 71,
"resetThresholdValue": 51, "enableAlarm": false }] }], "display": { "mediumMemoryUsage": 76, "highMemoryUsage":
91, "mediumDeviceThroughputUsage": 76, "highDeviceThroughputUsage": 91 } }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
2	500	1001	Internal error

Update the Performance Monitoring Settings at the Sensor Level

This URL updates the performance monitoring settings at the Sensor level.

Resource URL

PUT /sensor/<sensorId>/performancemonitoring

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`sensorId`	Sensor id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`inheritSettings`	Inherit settings from parent domain	Boolean	Yes
`enableMetricCollection`	Enable metric collection	Boolean	Yes
`enableThresholdAnalysis`	Enable threshold analysis	Boolean	Yes
`visibleToChildAdminDomain`	Settings visible to the child domain	Boolean	Yes
`enableCPUUtilizationMetricCollection`	Enable CPU utilization metric collection	Boolean	Yes
`enablePortThroughputUtilizationMetricCollection`	Enable port throughput utilization metric collection	Boolean	Yes
`thresholds`	List of threshold values	Array	No
`display`	Display values	Object	No

Details of object in thresholds:

Field Name	Description	Data Type	Mandatory
`metric`	Metric name	String	Yes
`thresholds`	List of threshold details	Array	Yes
`thresholdName`	Name of the threshold	String	Yes
`thresholdValue`	Threshold value	Number	Yes
`resetThresholdValue`	Reset threshold value	Number	Yes

Field Name	Description	Data Type	Mandatory
`enableAlarm`	Alarm enabled or not	Boolean	Yes

Details of display:

Field Name	Description	Data Type	Mandatory
`mediumMemoryUsage`	Memory usage value to be shown as medium usage	Number	Yes
`highMemoryUsage`	Memory usage value to be shown as high usage	Number	Yes
`mediumDeviceThroughputUsage`	Device throughput usage value to be shown as medium usage	Number	Yes
`highDeviceThroughputUsage`	Device throughput usage value to be shown as high usage	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful.	Number

Example

Request

PUThttps://<NSM_IP>/sdkapi/sensor/1001/performancemonitoring

Payload

```
{ "inheritSettings": false, "enableMetricCollection": true, "enableThresholdAnalysis": true,
"visibleToChildAdminDomain": true, "enableCPUUtilizationMetricCollection": true,
"enablePortThroughputUtilizationMetricCollection": true, "thresholds": [{ "metric": "CPU Usage", "thresholds":
[{ "thresholdName": "High Utilization", "thresholdValue": 92, "resetThresholdValue": 72, "enableAlarm": true },
{ "thresholdName": "Medium Utilization", "thresholdValue": 72, "resetThresholdValue": 52, "enableAlarm":
true }] }, { "metric": "Sensor Throughput Usage", "thresholds": [{ "thresholdName": "High Utilization",
"thresholdValue": 91, "resetThresholdValue": 71, "enableAlarm": false }, { "thresholdName": "Medium
Utilization", "thresholdValue": 71, "resetThresholdValue": 51, "enableAlarm": true }, { "thresholdName": "Under
Utilization", "thresholdValue": 6, "resetThresholdValue": 11, "enableAlarm": true }] }, { "metric": "L2 Error
Drop", "thresholds": [{ "thresholdName": "Too Many L2 Errors", "thresholdValue": 99, "resetThresholdValue": 51,
"enableAlarm": true }] }, { "metric": "L3/L4 Error Drop", "thresholds": [{ "thresholdName": "Too Many L3/L4
Errors", "thresholdValue": 1001, "resetThresholdValue": 101, "enableAlarm": true }] }, { "metric": "Memory
Usage", "thresholds": [{ "thresholdName": "High Utilization", "thresholdValue": 91, "resetThresholdValue": 71,
"enableAlarm": false }, { "thresholdName": "Medium Utilization", "thresholdValue": 71, "resetThresholdValue":
51, "enableAlarm": false }] }], "display": { "mediumMemoryUsage": 76, "highMemoryUsage": 91,
"mediumDeviceThroughputUsage": 76, "highDeviceThroughputUsage": 91 } }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	500	1001	Internal error

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
3	400	1111	Performance monitoring not supported
4	400	1111	Display parameters should be between 0 and 99
5	400	1111	Medium usage parameter should be greater than high usage parameter
6	400	1111	Threshold values should be greater than 0
7	400	1111	Threshold values should be between 1 and 100
8	400	1111	In case of rising, the reset threshold value should be less than threshold value
9	400	1111	In case of falling, the threshold value should be less than reset threshold value

Get Attack Set Profile Configuration Details at Domain Level

This URL retrieves the attack set profile configuration details at domain level.

Resource URL

GET /domain/<domainId>/attacksetprofile/getallrules

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`AttackSetProfileList`	List of all attack set profiles	Object

Details of attack set profiles:

Field Name	Description	Data Type
`policyName`	Policy name	String
`domainId`	Domain id	Number
`domainName`	Domain name	String
`policyId`	Policy id	Number
`description`	Policy description	String
`lastModifiedTime`	Last modified time	String
`enableRfSBExpoit`	RfSB exploit configuration	Boolean
`enableRfSBMalware`	RfSB malware configuration	Boolean
`enableRfSBRecon`	RfSB recon configuration	Boolean
`enableRfSBPolicy`	RfSB policy configuration	Boolean
`isEditable`	Attack set editable configuration	Boolean

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/attacksetprofile/getallrules

Response

```
{ "AttackSetProfileList": [ { "policyName": "Master Attack Repository", "domainId": 0, "domainName": "My
Company", "policyId": -1, "description": "Default settings for all attack definitions", "lastModifiedTime":
"2017-06-20 10:47:29", "lastModifiedUser": "admin", "enableRfSBExpoit": false, "enableRfSBMalware": false,
"enableRfSBRecon": false, "enableRfSBPolicy": false, "isEditable": false, "rules": [], }, { "policyName":
"Default Detection", "domainId": 0, "domainName": "My Company", "policyId": 0, "description": "The standard
attack set (blocking disabled)", "lastModifiedTime": "2017-06-20 10:45:57", "lastModifiedUser": "admin",
"enableRfSBExpoit": false, "enableRfSBMalware": false, "enableRfSBRecon": false, "enableRfSBPolicy": false,
"isEditable": false, "rules": [], }, { "policyName": "Outside Firewall", "domainId": 0, "domainName": "My
Company", "policyId": 1, "description": "Include all except for the RECONNAISSANCE category, and excluding known
noisy signatures. ", "lastModifiedTime": "2017-06-20 10:46:04", "lastModifiedUser": "admin", "enableRfSBExpoit":
false, "enableRfSBMalware": false, "enableRfSBRecon": false, "enableRfSBPolicy": false, "isEditable": false,
"rules": [], }, ], }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Get Attack Set Profile Configuration Details using Policy ID at Domain Level

This URL retrieves the rule set configuration details at domain level.

Resource URL

GET /domain/<domainId>/ attacksetprofile/rulesetdetails/<policyId>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domainId	Domain id	Number	Yes
policyId	Policy id	Number	Yes

Response Parameters

Following fields are returned if the operation was successful, otherwise error details are returned.

Field Name	Description	Data Type
policyName	Policy name	String
domainId	Domain id	Number
domainName	Domain name	String
policyId	Policy id	Number
description	Policy description	String
lastModifiedTime	Last modified time	String
enableRfSBExpoit	RfSB exploit configuration	Boolean
enableRfSBMalware	RfSB malware configuration	Boolean
enableRfSBRecon	RfSB recon configuration	Boolean

Field Name	Description	Data Type
`enableRfSBPolicy`	RfSB policy configuration	Boolean
`isEditable`	Attack set editable configuration	Boolean
`rules`	Rules of attack set profile	Object

Details of rules:

Field Name	Description	Data Type
`action`	Inclusion/exclusion of rules	String
`comment`	Comments	String
`isSpecificAttack`	Specific attack name	Boolean
`AttackList`	List of attacks	String
`minSeverity`	Severity level	String
`maxBTP`	BTP level	String
`attackType`	Type of attack	String
`attackCategory`	Attack category	String
`application`	Application list	String
`protocol`	Protocols	String
`operatingsystem`	Operating system	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/<domainId>/attacksetprofile/rulesetdetails/<policyId>

Response

```
{ "policyName": "Outside Firewall", "domainId": 0, "domainName": "My Company", "policyId": 1, "description":
"Include all except for the RECONNAISSANCE category, and excluding known noisy signatures. ",
"lastModifiedTime": "2017-06-20 10:46:04", "lastModifiedUser": "1", "enableRfSBExpoit": false,
"enableRfSBMalware": false, "enableRfSBRecon": false, "enableRfSBPolicy": false, "isEditable": false, "rules":
[ { "action": "INCLUDE", "comment": null, "isSpecificAttack": false, "AttackList": [], "minSeverity": "LOW(2)",
"maxBTP": "MEDIUM(4)", "attackType": "ANY", "attackCategory": [ null ], "application": [ null ], "protocol":
[ null ], "operatingsystem": [ null ], }, { "action": "EXCLUDE", "comment": null, "isSpecificAttack": false,
"AttackList": [], "minSeverity": null, "maxBTP": null, "attackType": "ANY", "attackCategory":
[ "Reconnaissance" ], "application": [ null ], "protocol": [ null ], "operatingsystem": [ null ], } ], }
```

Error Information

Following error codes are returned by this URL:

No	SDK API errorId	SDK API errorMessage
1	1105	Invalid domain
2	7001	Invalid policy id

Create New Attack Set Profile at Domain Level

This URL creates new attack set profile at domain level.

Resource URL

POST /domain/<domainId>/attacksetprofile/createruleset

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`policyName`	Policy name	String	Yes
`description`	Policy description	String	Yes
`enableRfSBExpoit`	RfSB exploit configuration	Boolean	Yes
`enableRfSBMalware`	RfSB malware configuration	Boolean	Yes
`enableRfSBRecon`	RfSB recon configuration	Boolean	Yes
`enableRfSBPolicy`	RfSB policy configuration	Boolean	Yes
`isEditable`	Attack set editable configuration	Boolean	No
`action`	Inclusion/exclusion of rules Values can be: • INCLUDE • EXCLUDE	String	No
`comment`	Comments	String	No
`isSpecificAttack`	Specific attack name	Boolean	No
`AttackList`	List of attacks	String	No
`minSeverity`	Severity level values can be: • NONE • HIGH_1 • HIGH_8 • HIGH_7 • MEDIUM_6 • MEDIUM_5 • MEDIUM_4 • LOW_3 • LOW_2 • LOW_1 • INFORMATIONAL_0	String	No

Field Name	Description	Data Type	Mandatory
`maxBTP`	BTP level values can be: • NONE_0 • HIGH_7 • HIGH_6 • MEDIUM_5 • MEDIUM_4 • MEDIUM_3 • LOW_2 • LOW_1	String	No
`attackType`	Type of attack values can be: • ANY • RF_SB_ONLY	String	No
`attackCategory`	Attack category	String	No
`application`	Application list	String	No
`Protocol`	Protocols	String	No
`operatingsystem`	Operating system	String	No

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique id of the created policy	Number

Example

Request

POST https://<NSM_IP>/sdkapi/domain/<domainId>/attacksetprofile/createruleset

```
{ "policyName": "New Attackset_API", "description": "Test creation ", "enableRfSBExpoit": false,
"enableRfSBMalware": false, "enableRfSBRecon": false, "enableRfSBPolicy": false, "rules": [ { "action":
"INCLUDE", "comment": null, "isSpecificAttack": false, "AttackList": [], "minSeverity": "LOW(2)", "maxBTP":
"MEDIUM(4)", "attackType": "ANY", "attackCategory": [ null ], "application": [ null ], "protocol": [ null ],
"operatingsystem": [ null ], }, { "action": "EXCLUDE", "comment": null, "isSpecificAttack": false, "AttackList":
[], "minSeverity": null, "maxBTP": null, "attackType": "ANY", "attackCategory": [ "Reconnaissance" ],
"application": [ null ], "protocol": [ null ], "operatingsystem": [ null ], } ], }
```

Response

```
{ createdResourceId :1 }
```

Error Information

Following error codes are returned by this URL:

No	SDK API errorId	SDK API errorMessage
1	1105	Invalid domain
2	7001	Invalid policy id
3	7001	Duplicate name detected
4	7001	The first rule in the list must be an Include rule

No	SDK API errorId	SDK API errorMessage
5	7001	Invalid attack type input
6	7001	A rule cannot contain multiple items of multiple categories at the same time

Update Attack Set Profile Configuration Detail

This URL updates the attack set profile configuration details at domain level.

Resource URL

PUT /domain/<domainId>/ attacksetprofile/updateruleset/<policyId>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes
`policyId`	Policy id	Number	Yes

Payload parameters:

Field Name	Description	Data Type	Mandatory
`policyName`	Policy name	String	Yes
`description`	Policy description	String	Yes
`enableRfSBExpoit`	RfSB exploit configuration	Boolean	Yes
`enableRfSBMalware`	RfSB malware configuration	Boolean	Yes
`enableRfSBRecon`	RfSB recon configuration	Boolean	Yes
`enableRfSBPolicy`	RfSB policy configuration	Boolean	Yes
`isEditable`	AttackSet editable configuration	Boolean	No
`action`	Inclusion/exclusion of rules Values can be: • INCLUDE • EXCLUDE	String	No
`comment`	Comments	String	No
`isSpecificAttack`	Specific attack name	Boolean	No
`AttackList`	List of attacks	String	No
`minSeverity`	Severity level values can be: • NONE	String	No

Field Name	Description	Data Type	Mandatory
	• HIGH_9 • HIGH_8 • HIGH_7 • MEDIUM_6 • MEDIUM_5 • MEDIUM_4 • LOW_3 • LOW_2 • LOW_1 • INFORMATIONAL_0		
`maxBTP`	BTP level values can be: • NONE • HIGH_7 • HIGH_6 • MEDIUM_5 • MEDIUM_4 • MEDIUM_3 • LOW_2 • LOW_1	String	No
`attackType`	Type of attack values can be: • ANY • RF_SB_ONLY	String	No
`attackCategory`	Attack category	String	No
`Application`	Application list	String	No
`Protocol`	Protocols	String	No
`operatingsystem`	Operating system	String	No

Response Parameters

Following fields are returned if the operation was successful, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/<domainId>/attacksetprofile/updateruleset/<policyId>

Payload

```
{"policyName":"API new create2", "description":"Include all except for the RECONNAISSANCE\ncategory, and
excluding known noisy signatures.", "enableRfSBExpoit":false, "enableRfSBMalware":false,
"enableRfSBRecon":false, "enableRfSBPolicy":false, "rules":[{"action":"INCLUDE",
"comment":null,"isSpecificAttack":false,"AttackList":
[],"minSeverity":"LOW(2)","maxBTP":"MEDIUM(4)","attackType":"ANY","attackCategory":[null],"application":
[null],"protocol":[null],"operatingsystem":[null]}]}
```

Response

```
{ status:1 }
```

Error Information

Following error codes are returned by this URL:

No	SDK API errorId	SDK API errorMessage
1	1105	Invalid domain
2	7001	Invalid policy id
3	7001	Duplicate name detected
4	7001	The first rule in the list must be an Include rule
5	7001	Invalid attack type input
6	7001	A rule cannot contain multiple items of multiple categories at the same time

Delete Attack Set Profile

This URL deletes the created attack set profile.

Resource URL

DELETE /domain/<domainId>/ attacksetprofile/deleteruleset/<policyId>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes
`policyId`	Policy id	Number	Yes

Payload Parameters

None

Response Parameters

Following fields are returned if the operation was successful, otherwise error details are returned.

Field Name	Description	Data Type
status	Set to 1 if the operation was successful	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/domain/<domainId>/attacksetprofile/deletruleset/<policyId>

Payload

None

Response

```
{ status:1 }
```

Error Information

Following error codes are returned by this URL:

No	SDK API errorId	SDK API errorMessage
1	1105	Invalid domain
2	7001	Invalid policy id
3	7001	Rule set is used by other policies

Get the Proxy Server Configuration at Domain Level

This URL gets the proxy server configuration at domain level.

Resource URL

GET /domain/<domainId>/proxyserver

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domainId	Domain id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
useDeviceListSettings	Inherit settings from parent domain	Boolean
useProxyserver	Use proxy server configuration	Boolean
proxyServerNameOrIPAddr	Proxy server name/IP configuration	String
proxyPort	Proxy port configuration	Number
userName	Username	String
password	Password	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/proxyserver

Response

```
{ "useDeviceListSettings": false, "useProxyserver": false, "proxyServerNameOrIPAddr": 1.1.1.1, "proxyPort":
8443, "userName": null, "password": null }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

Update Proxy Server Configuration

This URL updates the proxy server configuration.

Resource URL

PUT /domain/<domainId>/proxyserver

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domainId	Domain id	Number	Yes

Payload parameters:

Field Name	Description	Data Type	Mandatory
useDeviceListSettings	Inherit managers settings	Boolean	No
useProxyserver	Use proxy server	Boolean	No
proxyServerNameOrIPAddr	Proxy server IP/name	String	Yes
proxyPort	Proxy port	Number	Yes
userName	Username	String	No
password	Password	String	No

Response Parameters

Following fields are returned if the operation was successful, otherwise error details are returned.

Field Name	Description	Data Type
status	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/<domainId>/proxyserver

Payload

```
{ "useDeviceListSettings": false, "useProxyserver": false, "proxyServerNameOrIPAddr": 1.1.1.1, "proxyPort":
8443, "userName": null, "password": null }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	SDK API errorId	SDK API errorMessage
1	4714	Listening port number should be between 1 and 65535

Get the Proxy Server Configuration at Device Level

This URL gets the proxy server configuration at device level.

Resource URL

GET /device/<device_id>/proxyserver

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
device_id	Device id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
useDeviceListSettings	Inherit settings from parent domain	Boolean
useProxyserver	Use proxy server configuration	Boolean
proxyServerNameOrIPAddr	Proxy server name/IP configuration	String
proxyPort	Proxy port configuration	Number
userName	Username	String
password	Password	String

Example

Request

GET https://<NSM_IP>/sdkapi/device/1001/proxyserver

Response

```
{ "useDeviceListSettings": false, "useProxyserver": true, "proxyServerNameOrIPAddr": 1.1.1.1, "proxyPort": 8443,
"userName": null, "password": null }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Update the Proxy Server Configuration at Device Level

This URL updates the proxy server configuration at device level.

Resource URL

PUT /device/<device_id>/proxyserver

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`device_id`	Device id	Number	Yes

Payload parameters:

Field Name	Description	Data Type	Mandatory
`useDeviceListSettings`	Inherit settings from parent domain	Boolean	Yes
`useProxyserver`	Use proxy server configuration	Boolean	Yes
`proxyServerNameOrIPAddr`	Proxy server name/IP configuration	String	Yes
`proxyPort`	Proxy port configuration	Number	Yes
`userName`	Username	String	No
`password`	Password	String	No

Response Parameters

Following fields are returned if the operation was successful, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/device/1001/proxyserver

Payload

```
{ "useDeviceListSettings": true, "useProxyserver": false, "proxyServerNameOrIPAddr": null, "proxyPort": 0,
"userName": null, "password": null }
```

Response

```
{ "status": 1 }
```

Error Information

Following error code is returned by the URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal server error

Get the Proxy Server Configuration at the Manager Level

This URL gets the proxy server configuration at the Manager level.

Resource URL

GET /domain/proxyserver

Request Parameters

URL Parameters: None

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`useProxyserver`	Use proxy server configuration	Boolean
`proxyServerNameOrIPAddr`	Proxy server name/IP configuration	String
`proxyPort`	Proxy port configuration	Number
`userName`	Username	String
`password`	Password	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/proxyserver

Response

```
{ "useProxyserver": false, "proxyServerNameOrIPAddr": 1.1.1.1, "proxyPort": 8443, "userName": null, "password":
null }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Update the Proxy Server Configuration at the Manager Level

This URL updates the proxy server configuration at the Manager level.

Resource URL

PUT /domain/proxyserver

Request Parameters

URL Parameters: None

Payload parameters:

Field Name	Description	Data Type	Mandatory
`useProxyserver`	Use proxy server configuration	Boolean	Yes
`proxyServerNameOrIPAddr`	Proxy server name/IP configuration	String	Yes
`proxyPort`	Proxy port configuration	Number	Yes
`userName`	User name	String	No

Field Name	Description	Data Type	Mandatory
`password`	Password	String	No

Response Parameters

Following fields are returned if the operation was successful, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/proxyserver

Payload

```
{ "useProxyserver": true, "proxyServerNameOrIPAddr": 1.1.1.1, "proxyPort": 8443, "userName": null, "password":
null }
```

Response

```
{ "status": 1 }
```

Error Information

Following error code is returned by the URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal server error

Get the Cluster ID Based on Name

This URL retrieves the vNSP cluster id based on name.

Resource URL

POST /cloud/getclusterid

Request Parameters

URL Parameters

None

Payload Request Parameters

Field Name	Description	Data Type	Mandatory
`name`	Cluster name	String	Yes

Response Parameters

Following fields are returned:

Field Name	Description	Data Type
`createdResourceId`	The cluster id	Number

Example

Request

POST https://<NSM_IP>/sdkapi/cloud/getclusterid

Payload

```
{ 'name' : 'clusterName' }
```

Response

```
{ 'createdResourceId' : 101 }
```

Error Information

None

Get the Controller ID Based on Name

This URL retrieves the vNSP controller ID based on name.

Resource URL

POST /cloud/getcontrollerid

Request Parameters

URL Parameters

None

Payload Request Parameters

Field Name	Description	Data Type	Mandatory
`name`	Controller name	String	Yes

Response Parameters

Following fields are returned:

Field Name	Description	Data Type
`createdResourceId`	The controller id	Number

Example

Request

POST https://<NSM_IP>/sdkapi/cloud/getcontrollerid

Payload

```
{ ‘name’ : ‘controllerName’ }
```

Response

```
{ ‘createdResourceId’ : 101 }
```

Error Information

None

Get the Virtual Probe Status

This URL retrieves the virtual probe status.

Resource URL

GET cloud/checkprobestatus/<ip_address>

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
`Ip_address`	Virtual probe IP	String	Yes

Payload Request Parameters

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned:

Field Name	Description	Data Type
`workloadVMIP`	Workload IP	String
`privateIP`	Private IP of virtual machine	String
`publicIP`	Public IP of virtual machine	String
`hostname`	Virtual machine host name	String

Field Name	Description	Data Type
`worloadOS`	OS on virtual machine	String
`probeInstalled`	Probe agent is installed on the virtual machine or not	Boolean
`probeRunning`	Probe agent is running on the virtual machine or not	Boolean
`probeVersion`	Probe agent version	String
`probeRunningSince`	Time since the probe agent has been running	String

Example

Request

GET https://<NSM_IP>/sdkapi/cloud/checkprobestatus/<ip_address>

Payload

None

Response

```
{ "workloadVMIP": "10.15.2.113", "privateIP": "10.15.2.113", "publicIP": "10.15.2.113", "hostName":
"ip-10-15-2-113", "workloadOS": "Amazon Linux AMI release 2016.09", "probeInstalled": true, "probeRunning":
true, "probeVersion": "3.5.3-8(64-bit)", "probeRunningSince": "Fri Mar 24 05:24:30 UTC 2017 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	1406	Invalid IP format

Get the vNSP Controllers Present in the Domain

This URL retrieves all the vNSP controllers from the domain.

Resource URL

GET /cloud/<domain_id>/connector

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
`Domain_id`	Domain id	Number	Yes

Payload Request Parameters

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned:

Field Name	Description	Data Type
`cloudConnector`	List of the controllers	Array

Details of fields in the objects under Controller:

Field Name	Description	Data Type
`id`	Controller id	Number
`domain`	Domain details	String
`name`	Controller name	String
`isHA`	Specifies if the controller is in high availability mode or not	Boolean
`serviceIp`	Controller service IP, if provided	String
`haTimeout`	High availability timeout in minutes	Number
`sharedSecret`	Shared secret between the Manager and controller	String
`privateCommunicationSubnet`	Private controller communication subnet CIDR	String
`lastUpdated`	Last updated time	String
`description`	Controller description	String
`members`	Controller member details. Maximum 2 members.	Array
`cloud`	Cloud access details	Object

Details of fields in members:

Field Name	Description	Data Type
`status`	Registration/connection status between controller and the Manager	String
`localIP`	Controller member private IP	String
`controllerSoftware`	Software version on controller	String
`probeSoftware`	Virtual probe agent version associated with the controller	String

Details of fields in cloud:

Field Name	Description	Data Type
`type`	Type of cloud environment. Supported value: • Amazon	String

Field Name	Description	Data Type
	• Azure	
`awsDetails`	AWS cloud details	Object
`azureDetails`	Azure cloud details	Object

Details of fields in AWS:

Field Name	Description	Data Type
`useIAMRole`	Specifies if the IAM roles in Manager machines are used to access the AWS cloud or not	Boolean
`region`	Cloud access region	String
`accessKey`	Cloud access key	String
`secretKey`	Cloud access secret key	String

Details of fields in Azure:

Field Name	Description	Data Type
`directoryId`	Azure directory id	String
`applicationKey`	Azure app application key	String
`applicationId`	Azure app application id	String
`subscription`	Azure app subscription id	String

Example

Request

GET https://<NSM_IP>/sdkapi/cloud/<domain_id>/connector

Response

```
{ "cloudConnector": [ { "id": 101, "domain": "My Company ( 0 )", "name": "Cont8_4", "isHA": true, "serviceIp":
"34.210.121.120", "haTimeout": 5, "sharedSecret": "********", "privateCommunicationSubnet": "1.1.12.0/24",
"lastUpdated": "2017-06-14 09:03:39.0 ( null )", "description": "controller in 8.4", "members": [ { "status":
"ONLINE", "localIP": "10.40.10.17", "controllerSoftware": "3.6.1 (060717a)", "probeSoftware": "3.6.1-5" },
{ "status": "ONLINE", "localIP": "10.40.10.98", "controllerSoftware": "3.6.1 (060717a)", "probeSoftware":
"3.6.1-5" } ], "cloud": { "type": "AMAZON", “awsDetails”: { “useIAMRole”: false, "region": "US West (Oregon)",
"accessKey": "AKIAJOKGKIFNHOWISXOA", "secretKey": "****************************************" }, “azureDetails”:
null } }, { "id": 103, "domain": "My Company ( 0 )", "name": "StAl", "isHA": false, "serviceIp": null,
"haTimeout": 5, "sharedSecret": "********", "privateCommunicationSubnet": "1.14.7.0/24", "lastUpdated":
"2017-06-14 09:34:29.0 ( null )", "description": "standalone controller", "members": [ { "status": "ONLINE",
"localIP": "10.40.10.210", "controllerSoftware": "3.6.1 (060717a)", "probeSoftware": "3.6.1-5" } ], "cloud":
{ "type": "AMAZON", “awsDetails”: { “useIAMRole”: false, "region": "US West (Oregon)", "accessKey":
"AKIAJOKGKIFNHOWISXOA", "secretKey": "****************************************" }, “azureDetails”: null } } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: internal server error
2	400	1105	Invalid domain

Create the vNSP Controller

This URL creates the vNSP controller.

Resource URL

POST /cloud/<domain_id>/connector

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
`Domain_Id`	Domain id	Number	Yes

Payload Parameters

Field Name	Description	Data Type	Mandatory
`name`	Controller name	String	Yes
`isHA`	Specifies if the controller is in high availability mode or not	Boolean	Yes
`serviceIp`	Controller service IP, if provided	String	No
`haTimeout`	High availability timeout in minutes	Number	No
`sharedSecret`	Shared secret between the Manager and Controller	String	Yes
`privateCommunicationSubnet`	Private controller communication subnet CIDR	String	Yes
`description`	Controller description	String	No
`cloud`	Cloud access details	Object	Yes

Details of fields in cloud:

Field Name	Description	Data Type	Mandatory
`type`	Type of cloud environment. Supported value: • Amazon • Azure	String	Yes
`awsDetails`	AWS cloud details	Object	Yes
`azureDetails`	Azure cloud details	Object	Yes

Details of fields in AWS:

Field Name	Description	Data Type	Mandatory
`useIAMRole`	Specifies if the IAM roles in Manager machines are used to access the AWS cloud or not	Boolean	Yes
`region`	Cloud access region	String	Yes
`accessKey`	Cloud access key	String	Yes
`secretKey`	Cloud access secret key	String	Yes

Details of fields in Azure:

Field Name	Description	Data Type	Mandatory
`directoryId`	Azure directory id	String	Yes
`applicationKey`	Azure app application key	String	Yes
`applicationId`	Azure app application id	String	Yes
`subscription`	Azure app subscription id	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned:

Field Name	Description	Data Type
`createdResourceId`	Created resource id	Number

Example

Request

POST https://<NSM_IP>/sdkapi/cloud/0/connector

Payload

```
{ 'privateCommunicationSubnet': '1.1.1.0/24', 'sharedSecret': 'ControllerSharedSecretKey', 'name':
'Controller1', ‘isHA’: false, "cloud":{ "azureDetails": { "directoryId": "directoryId", "applicationKey":
"appKey", "applicationId": "appId", "subscription": "subscription" }, "type": "AZURE", "awsDetails": null },
'description': 'Demo Controller' }
```

Response

```
{ "createdResourceId" : 103 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: internal server error
2	400	1105	Invalid domain
3	400	11001	Name is required

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
4	400	11001	Controller name can have alphanumeric characters and [_, -, .] special characters
5	400	11001	Cloud details are required
6	400	11001	Cloud type is required
7	400	11001	Cloud type should be one of: <list of allowed values>
8	400	11001	Cloud region should be one of: <list of allowed regions>
9	400	11001	Shared secret is required
10	400	11001	Private communication subnet is required
11	400	1701	Invalid CIDR notation
12	400	11001	Only IPv4 IP supported for server IP address
13	400	11001	HA timeout should be between 1 and 10

Get the vNSP Controller Details

This URL gets the vNSP controller details.

Resource URL

GET /cloud/connector/<id>

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
`id`	Controller id	Number	Yes

Payload Request Parameters

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned:

Field Name	Description	Data Type
`id`	Controller id	Number
`domain`	Domain details	String

Field Name	Description	Data Type
`name`	Controller name	String
`isHA`	Specifies if the controller is in high availability mode or not	Boolean
`serviceIp`	Controller service IP, if provided	String
`haTimeout`	High availability timeout in minutes	Number
`sharedSecret`	Shared secret between Manager and the controller	String
`privateCommunicationSubnet`	Private controller communication subnet CIDR	String
`lastUpdated`	Last updated time	String
`description`	Controller description	String
`members`	Controller member details. Maximum 2 members.	Array
`cloud`	Cloud access details	Object

Details of fields in members:

Field Name	Description	Data Type
`status`	Registration/connection status between controller and the Manager	String
`localIP`	Controller member private IP	String
`controllerSoftware`	Software version on controller	String
`probeSoftware`	Virtual probe agent version associated with the controller	String

Details of fields in cloud:

Field Name	Description	Data Type
`type`	Type of cloud environment. Supported Value: • Amazon • Azure	String
`awsDetails`	AWS cloud details	Object
`azureDetails`	Azure cloud details	Object

Details of fields in AWS:

Field Name	Description	Data Type
`useIAMRole`	Specifies if the IAM roles in Manager machines are used to access the AWS cloud or not	Boolean
`region`	Cloud access region	String
`accessKey`	Cloud access key	String
`secretKey`	Cloud access secret key	String

Details of fields in Azure:

Field Name	Description	Data Type
`directoryId`	Azure directory id	String
`applicationKey`	Azure app application key	String
`applicationId`	Azure app application id	String
`subscription`	Azure app subscription id	String

Example

Request

GET https://<NSM_IP>/sdkapi/cloud/conenctor/101

Response

```
{ "id": 101, "domain": "My Company ( 0 )", "name": "Cont8_4", "isHA": true, "serviceIp": "34.210.121.120",
"haTimeout": 5, "sharedSecret": "********", "privateCommunicationSubnet": "1.1.12.0/24", "lastUpdated":
"2017-06-14 09:03:39.0 ( null )", "description": "controller in 8.4", "members": [ { "status": "ONLINE",
"localIP": "10.40.10.17", "controllerSoftware": "3.6.1 (060717a)", "probeSoftware": "3.6.1-5" }, { "status":
"ONLINE", "localIP": "10.40.10.98", "controllerSoftware": "3.6.1 (060717a)", "probeSoftware": "3.6.1-5" } ],
"cloud": { "type": "AMAZON", “awsDetails”: { “useIAMRole”: false, "region": "US West (Oregon)", "accessKey":
"AKIAJOKGKIFNHOWISXOA", "secretKey": "*****************************************" }, “azureDetails”: null } }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message
2	400	11001	Invalid controller

Test Manager-Controller Connection

This URL tests the Manager-controller connection.

Resource URL

GET /cloud/connector/<id>/testcontrollerconnection

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
id	Controller id	Number	Yes

Payload Request Parameters

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned:

Field Name	Description	Data Type
status	Set to 1 if the connection was successful	Number

Example

Request

GET https://<NSM_IP>/sdkapi/cloud/connector/103/testcontrollerconnection

Payload

None

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message
2	400	11001	Invalid controller

Test Manager-Controller Cloud Connection

This URL tests the Manager-controller connection.

Resource URL

GET /cloud/connector/<id>/testcloudconnection

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
id	Controller id	Number	Yes

Payload Request Parameters

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned:

Field Name	Description	Data Type
status	Set to 1 if the connection was successful	Number

Example

Request

GET https://<NSM_IP>/sdkapi/cloud/connector/103/testcloudconnection

Payload

None

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message
2	400	11001	Invalid controller

Update the vNSP Controller

This URL updates the vNSP controller.

Resource URL

PUT /cloud/connector/<id>

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
id	Controller id	Number	Yes

Payload Request Parameters

Field Name	Description	Data Type	Mandatory
name	Controller name	String	Yes
isHA	Specifies if the controller is in high availability mode or not	Boolean	Yes
serviceIp	Controller service IP, if provided	String	No
haTimeout	High availability timeout in minutes	Number	No
sharedSecret	Shared secret between the Manager and controller	String	Yes

Field Name	Description	Data Type	Mandatory
`privateCommunicationSubnet`	Private controller communication subnet CIDR	String	Yes
`description`	Controller description	String	No
`cloud`	Cloud access details	Object	Yes

Details of fields in cloud:

Field Name	Description	Data Type	Mandatory
`type`	Type of cloud environment. Supported value: • Amazon • Azure	String	Yes
`awsDetails`	AWS cloud details	Object	Yes
`azureDetails`	Azure cloud details	Object	Yes

Details of fields in AWS:

Field Name	Description	Data Type	Mandatory
`useIAMRole`	Specifies if the IAM roles in Manager machines are used to access the AWS cloud or not	Boolean	Yes
`region`	Cloud access region	String	Yes
`accessKey`	Cloud access key	String	Yes
`secretKey`	Cloud access secret key	String	Yes

Details of fields in Azure:

Field Name	Description	Data Type	Mandatory
`directoryId`	Azure directory id	String	Yes
`applicationKey`	Azure app application key	String	Yes
`applicationId`	Azure app application id	String	Yes
`subscription`	Azure app subscription id	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned:

Field Name	Description	Data Type
`status`	Set to 1 if the update was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/cloud/connector/103

Payload

```
{ 'privateCommunicationSubnet': '1.1.1.0/24', 'sharedSecret': 'ControllerSharedSecretKey', 'cloud': { 'type':
'AMAZON', 'awsDetails': { 'secretKey': 'ControllerCloudSecretKey', 'region': 'US_WEST_2', 'accessKey':
'ControllerCloudAccessKey' } }, 'description': 'Demo Controller' }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: internal server error
2	400	1105	Invalid domain
3	400	11001	Cloud details are required
4	400	11001	Cloud type is required
5	400	11001	Cloud type should be one of: <list of allowed values>
6	400	11001	Cloud region should be one of: <list of allowed regions>
7	400	11001	Shared secret is required
8	400	11001	Private communication subnet is required
9	400	1701	Invalid CIDR notation

Delete the vNSP Controller

This URL deletes the vNSP controller.

Resource URL

DELETE /cloud/connector/<id>

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
id	Controller id	Number	Yes

Payload Parameters

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned:

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/cloud/connector/103

Payload

None

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message
2	400	11001	Invalid controller

Upgrade the vNSP Controller Software

This URL upgrades the vNSP controller software.

Resource URL

PUT /cloud/connector/<id>/upgrade

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
`id`	Controller id	Number	Yes

Payload Request Parameters

Field Name	Description	Data Type	Mandatory
`MultiPart`	Holds the body part objects	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
`BodyPart[0]`	Holds the file name detail	Application/json object	Yes

Details of object in BodyPart[0]:

Field Name	Description	Data Type	Mandatory
`fileName`	Name of the file	String	Yes

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
`BodyPart[1]`	Holds the file as input stream	Application/octet-stream	Yes

Details of .tar.gz file:

Field Name	Description	Data Type	Mandatory
`File`	Software file input stream	Byte array input stream	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned:

Field Name	Description	Data Type
`status`	Set to 1 if the update was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/cloud/connector/101/upgrade

Response

```
{ " status ": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message
2	400	5301	Invalid file type given for import: the file name does not have any extension
3	400	5301	Invalid file type given for import expected is .tar.gz while <filetype> was provided.

Get the vNSP Clusters Present in the Domain

This URL retrieves all the vNSP clusters from the domain.

Resource URL

GET /cloud/<domain_id>/cluster

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
`Domain_id`	Domain id	Number	Yes

Payload Request Parameters

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned:

Field Name	Description	Data Type
`cloudCluster`	List of the controllers	Array

Details of fields in the objects under vNSP Cluster:

Field Name	Description	Data Type
`id`	Cluster id	Number
`domain`	Domain details	String
`name`	Cluster name	String
`description`	Cluster description	String
`cloudConnector`	Controller name	String
`subscription`	Subscription id for Azure controllers	String
`sharedSecret`	Shared secret between the Manager and cluster	String
`memberSensors`	Number of member Sensors	Number
`lastUpdated`	Last updated time	String

Example

Request

GET https://<NSM_IP>/sdkapi/cloud/<domain_id>/connector

Response

```
{ "cloudCluster": [ { "id": 101, "domain": "My Company ( 0 )", "name": "test", "description": "",
"cloudConnector": "Cloud_Controller", "sharedSecret": "********", "memberSensors": 0, "lastUpdated": "2017-03-23
10:25:42.0 ( admin )" "subscription": "subscription" }, { "id": 102, "domain": "My Company ( 0 )", "name":
"Cloud_Cluster", "description": "api updated", "cloudConnector": "Cloud_Controller", "sharedSecret": "********",
"memberSensors": 0, "lastUpdated": "2017-03-23 10:38:29.0 ( admin )" } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: internal server error

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
2	400	1105	Invalid domain

Create the vNSP Cluster

This URL creates the vNSP cluster.

Resource URL

POST /cloud/<domain_id>/cluster

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
`Domain_Id`	Domain id	Number	Yes

Payload Parameters

Field Name	Description	Data Type	Mandatory
`name`	Cluster name	String	Yes
`description`	Cluster description	String	No
`cloudConnector`	Controller name	String	Yes
`subscription`	Subscription id for Azure controllers	String	No
`sharedSecret`	Shared secret between the Manager and Cluster	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned:

Field Name	Description	Data Type
`createdResourceId`	Created resource id	Number

Example

Request

POST https://<NSM_IP>/sdkapi/cloud/0/cluster

Payload

```
{ "name": "Cloud_Cluster", "description": "api updated", "cloudConnector": "Cloud_Controller", "subscription":
"subscription id", "sharedSecret": "secret" }
```

Response

```
{ " createdResourceId ": 101 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: internal server error
2	400	1105	Invalid domain
3	400	11001	Cluster name is required
4	400	11001	Cluster name can have alphanumeric characters and [_, -, .] special characters

Get the vNSP Cluster Details

This URL gets the vNSP cluster details.

Resource URL

GET /cloud/cluster/<id>

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
`id`	Cluster id	Number	Yes

Payload Request Parameters

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned:

Field Name	Description	Data Type
`id`	Cluster id	Number
`domain`	Domain details	String
`name`	Cluster name	String
`description`	Cluster description	String
`cloudConnector`	Controller name	String
`subscription`	Subscription id for Azure controllers	String
`sharedSecret`	Shared secret between the Manager and cluster	String
`memberSensors`	Number of member Sensors	Number
`lastUpdated`	Last updated time	String

Example

Request

GET https://<NSM_IP>/sdkapi/cloud/cluster/101

Response

```
{ "id": 101, "domain": "My Company ( 0 )", "name": "test", "description": "", "cloudConnector":
"Cloud_Controller", "subscription": null, "sharedSecret": "********", "memberSensors": 0, "lastUpdated":
"2017-03-23 10:25:42.0 ( admin )" }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message
2	400	11001	Get failed for id <id> : <error>

Update the vNSP Cluster

This URL updates the vNSP cluster.

Resource URL

PUT /cloud/cluster/<id>

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
id	Cluster id	Number	Yes

Payload Request Parameters

Field Name	Description	Data Type	Mandatory
description	Cluster description	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned:

Field Name	Description	Data Type
status	Set to 1 if the update was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/cloud/cluster/101

Payload

```
{ 'description': Updated }
```

Response

```
{ " status ": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: internal server error
2	400	11001	Get failed for id <id> : <error>

Delete the vNSP Cluster

This URL deletes the vNSP cluster.

Resource URL

DELETE /cloud/cluster/<id>

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
`id`	Cluster id	Number	Yes

Payload Parameters

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned:

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/cloud/cluster/101

Payload

None

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message
2	400	11001	Get failed for id <id> : <error>

Get the Protected VM Groups Present in the vNSP Cluster

This URL gets all the protected VM groups in the vNSP cluster.

Resource URL

GET /cloud/cluster/<id>/vmgroups

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
`id`	Cluster id	Number	Yes

Payload Request Parameters

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned:

Field Name	Description	Data Type
`vmgroups`	List of the protected VM groups under the Cluster	Array

Details of fields in the objects under vmgroups:

Field Name	Description	Data Type
`name`	Protected VM group name	String
`description`	Protected VM group description	String
`cloudCluster`	Cluster name	String
`cloudConnector`	Controller name	String
`vpc`	VPC where the protected VM group has been created	Array
`resourceGroup`	Resource group list in case of Azure	Array
`advancedAgentSettings`	Traffic inspection settings	Object
`protectedObjects`	List of the protected subnets	Array
`lastUpdated`	Last updated time	String

Details of fields in advancedAgentSettings:

Field Name	Description	Data Type
`trafficProcessing`	Traffic processing direction. Values can be: • Ingress • Egress	String

Field Name	Description	Data Type
	• Ingress & Egress	
`inspectionMode`	Inspection mode. Values can be : • IPS • IDS	String

Example

Request

GET https://<NSM_IP>/sdkapi/cloud/cluster/101/vmgroups

Response

```
{ "vmgroups": [ { "oldName": null, "name": "Protected_VMGroup", "description": "api update", "cloudCluster":
"Cloud_Cluster", "cloudConnector": "Cloud_Controller", "vpc": ["vpc-06b3ce61(Protected_test)"], "resourceGroup":
[], "advancedAgentSettings": { "trafficProcessing": "Ingress & Egress", "inspectionMode": "ips" },
"protectedObjects": [ "subnet-bde05df4(Secure_subnet)" ], "lastUpdated": "2017-03-23 11:02:50.0 (admin)" } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: internal server error

Create the Protected VM Group under vNSP Cluster

This URL creates the protected VM groups in the vNSP cluster.

Resource URL

POST /cloud/cluster/<id>/vmgroup

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
`id`	Cluster id	Number	Yes

Payload Request Parameters

Field Name	Description	Data Type	Mandatory
`name`	Protected VM group name	String	Yes
`description`	Protected VM group description	String	No
`vpc`	VPC where the protected VM group has been created	Array	Yes
`resourceGroup`	Resource group list in case of Azure	Array	Yes

Field Name	Description	Data Type	Mandatory
`advancedAgentSettings`	Traffic inspection settings	Object	Yes
`protectedObjects`	List of the protected subnets	Array	Yes

Details of fields in advancedAgentSettings:

Field Name	Description	Data Type	Mandatory
`trafficProcessing`	Traffic processing direction. Values can be: • Ingress • Egress • Ingress & Egress	String	Yes
`inspectionMode`	Inspection mode. Values can be: • IPS • IDS	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned:

Field Name	Description	Data Type
`createdResourceId`	Created resource id	Number

Example

Request

POST https://<NSM_IP>/sdkapi/cloud/cluster/101/vmgroup

Payload

```
{ "name": "Protected_VMGroup", "description": "api", "vpc": ["vpc-06b3ce61(Protected_test)"],
"advancedAgentSettings": { "trafficProcessing": "Ingress & Egress", "inspectionMode": "ips" },
"protectedObjects": [ "subnet-bde05df4(Secure_subnet)" ] }
```

Response

```
{ " createdResourceId ": 101 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: internal server error
2	400	11001	Protected VM group name is required
3	400	11001	Inspection mode is required
4	400	11001	Invalid inspection mode, it should be one of: <valid list>
5	400	11001	Traffic processing is required

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
6	400	11001	Invalid traffic processing, it should be one of: <list>

Get the Protected VM Group Details

This URL gets the protected VM group details.

Resource URL

PUT /cloud/cluster/<id>/getvmgroup

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
id	Cluster id	Number	Yes

Payload Request Parameters

Field Name	Description	Data Type	Mandatory
name	Protected VM group name	String	yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned:

Field Name	Description	Data Type
name	Protected VM group name	String
description	Protected VM group description	String
cloudCluster	Cluster name	String
cloudConnector	Controller name	String
vpc	VPC where the protected VM proup has been created	Array
resourceGroup	Resource group list in case of Azure	Array
advancedAgentSettings	Traffic inspection settings	Object
protectedObjects	List of the protected subnets	Array
lastUpdated	Last updated time	String

Details of fields in advancedAgentSettings:

Field Name	Description	Data Type
`trafficProcessing`	Traffic processing direction. Values can be: • Ingress • Egress • Ingress & Egress	String
`inspectionMode`	Inspection mode. Values can be : • IPS • IDS	String

Example

Request

PUT https://<NSM_IP>/sdkapi/cloud/cluster/101/getvmgroup

Payload

```
{ “name”: “Protected_VMGroup” }
```

Response

```
{ "oldName": null, "name": "Protected_VMGroup", "description": "api update", "cloudCluster": "Cloud_Cluster",
"cloudConnector": "Cloud_Controller", "vpc": ["vpc-06b3ce61(Cloud_test)"], "advancedAgentSettings":
{ "trafficProcessing": "Ingress & Egress", "inspectionMode": "ips" }, "protectedObjects": [ "subnet-
bde05df4(Secure_subnet)" ], "lastUpdated": "2017-03-23 11:02:50.0 ( admin)" }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message
2	400	11001	No VM group of <name> name in cluster

Update the Protected VM Group

This URL updates the protected VM group.

Resource URL

PUT /cloud/cluster/<id>/vmgroup

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
`id`	Cluster id	Number	Yes

Payload Request Parameters

Field Name	Description	Data Type	Mandatory
`oldName`	Protected VM group name which needs to be updated	String	Yes
`name`	New name for protected VM group	String	Yes
`description`	Protected VM group description	String	No
`vpc`	VPC where the protected VM group has been created	Array	Yes
`resourceGroup`	Resource group list in case of Azure	Array	Yes
`advancedAgentSettings`	Traffic inspection settings	Object	Yes
`protectedObjects`	List of the protected subnets	Array	Yes

Details of fields in advancedAgentSettings:

Field Name	Description	Data Type	Mandatory
`trafficProcessing`	Traffic processing direction. Values can be: • Ingress • Egress • Ingress & Egress	String	Yes
`inspectionMode`	Inspection mode. Values can be : • IPS • IDS	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned:

Field Name	Description	Data Type
`status`	Set to 1 if the update was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/cloud/cluster/101/vmgroup

Payload

```
{ "oldName": “Protected_VMGroup”, "name": "Protected_VMGroup", "description": "api", "vpc":
["vpc-06b3ce61(Protected_test)"], "advancedAgentSettings": { "trafficProcessing": "Ingress & Egress",
"inspectionMode": "ips" }, "protectedObjects": [ "subnet-bde05df4(Protected_subnet)" ] }
```

Response

```
{ " status ": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: internal server error
2	400	11001	VM group name is required
3	400	11001	Inspection mode is required
4	400	11001	Invalid Inspection mode, it should be one of: <valid list>
5	400	11001	Traffic processing is required
6	400	11001	Invalid traffic processing, it should be one of: <list>
7	400	11001	Old VM group name is required

Delete the Protected VM Group

This URL deletes the protected VM group.

Resource URL

DELETE /cloud/cluster/<id>/vmgroup

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
`id`	Cluster id	Number	Yes

Payload Request Parameters

Field Name	Description	Data Type	Mandatory
`name`	Protected VM group name	String	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned:

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/cloud/cluster/101/vmgroup

Payload

```
{ “name”: “Protected_VMGroup” }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message
2	400	11001	No VM group of <name> name in cluster

Download the Cluster Virtual Probe Agent

This URL download the cluster virtual probe agent.

Resource URL

GET /cloud/cluster/<id>/downloadagent

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
`id`	Cluster id	Number	Yes

Query Parameter

Field Name	Description	Data Type	Mandatory
`ostype`	Operating system type. Values can be: • Windows (default) • Linux	String	No

Payload Request Parameters

None

Response Parameters

Cluster virtual probe file data is returned if the request parameters are correct, otherwise error details are returned.

Example

Request

PUT https://<NSM_IP>/sdkapi/cloud/cluster/101/downloadagent?ostype=linux

Response

<probe software file data>

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: internal server error
2	400	11001	Please provide valid OS, one of [windows, linux]
3	400	11001	Get failed for id <id> : <error>

Download the Cluster Probe Agent without Login

This URL downloads the cluster probe agent without logging into the Manager.

Resource URL

GET /cloud/cluster/downloadprobeagent

Request Parameters

URL Parameters

None

Query Parameter

Field Name	Description	Data Type	Mandatory
`ostype`	Operating system type. Values can be: • Windows (default) • Linux	String	No
`name`	Cluster name for which probe needs to be downloaded	String	Yes

Payload Request Parameters

None

Response Parameters

Cluster Virtual Probe file data is returned if the request parameters are correct, otherwise error details are returned.

Example

Request

GET https://<NSM_IP>/sdkapi/cloud/cluster/downloadprobeagent?ostype=linux

Response

<probe software file data>

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: internal server error

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
2	400	11001	Please provide valid OS, one of [Windows, Linux]
3	400	11001	Get failed for id <id>: <error>

Update the vNSP Cluster Agent

This URL updates the vNSP cluster agents.

Resource URL

PUT /cloud/cluster/<id>/upgradeagents

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
`id`	Cluster id	Number	Yes

Payload Request Parameters

None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned:

Field Name	Description	Data Type
`status`	Set to 1 if the update was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/cloud/cluster/101/upgradeagents

Payload

None

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: internal server error
2	400	11001	Get failed for id <id> : <error>

Get the List of Protected VM Hosts

This URL gets the list of protected VM hosts from the Manager based on cluster.

Resource URL

GET /cloud/cluster/<id>/getProtectedVMHosts

Request Parameters

URL Parameters

Field Name	Description	Data Type	Mandatory
id	Cluster id	Number	Yes

Payload Request Parameters

Field Name	Description	Data Type	Mandatory
name	Cluster name	String	Yes

Response Parameters

Following fields are returned:

Field Name	Description	Data Type
protectedVMHosts	List of protected VM hosts with details	Object

Details of fields under objects in protected VM hosts:

Field Name	Description	Data Type
hostname	Name of the protected VM host.	String
privateIP	Private IP address of protected VM host	String
publicIP	Public IP address of protected VM host	String
operatingSystem	Operating system of protected VM host	String
probeServiceStatus	Online / offline	String
probeActiveSince	Time stamp from which the protected VM host is online. If NULL it implies VM host is offline (probe_status= false)	String
probeVersion	Version of the probe installed on protected VM host	String
clusterName	Cluster name under which this protected VM host is added.	String
controllerIP	IP address of the controle_server (zCenter)	String
domainName	Domain name of control of protected VM host	String

Field Name	Description	Data Type
awsInstanceId	Unique id generated by AWS	String

Example

Request

POST https://<NSM_IP>/sdkapi/cloud/cluster/101/getProtectedVMHosts

Payload

None

Response

```
{ "protectedVMHosts": [{ "hostname": "WIN-IPMU0PRS727", "privateIP": "10.40.20.252", "publicIP":
"52.89.154.236", "operatingSystem": "Windows Server 2012 R2 (build 9600), 64-bit", "probeServiceStatus": true,
"probeActiveSince": "2017-04-13 14:04:27", "probeVersion": "3.5.3-8(64-bit)", "clusterName": "ClusterTwo",
"controllerIP": "35.166.195.169", "domainName": "MyDomainOne", “awsInstanceId”:”amazonGeneratedID1” },
{ "hostname": "WIN-IPMU0PRS728", "privateIP": "11.40.20.252", "publicIP": "62.89.154.236", "operatingSystem":
"CentOSrelease6.8(Final)", "probeServiceStatus": true, "probeActiveSince": "8-04-1314: 04: 27", "probeVersion":
"4.5.3-8(64-bit)", "clusterName": "ClusterOne", "controllerIP": "45.166.195.169", "domainName": "MyDomainTwo",
“awsInstanceId”:” amazonGeneratedID2” } ] }
```

Error Information

None

Get Quarantine Zone Details using Quarantine Zone ID at Domain Level

This URL retrieves the details of quarantine zone at domain level.

Resource URL

GET /domain/<domainId>/quarantineZone/<quarantineZoneID>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes
`quarantineZoneID`	Quarantine zone id	Number	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`quarantineZoneId`	Quarantine zone unique id	Number
`quarantineZoneName`	Name of quarantine zone	String
`quarantineZoneDescription`	Description of quarantine zone	String
`ownerId`	Domain id	Number
`visibleToChild`	Is quarantine zone visible to child domain	Boolean
`isEditable`	Is quarantine zone editable or not	Boolean
`quarantineZoneVersion`	Quarantine zone version	Number
`lastModifiedTime`	The time quarantine zone last modified	String
`lastModifiedUser`	Last user that modified the quarantine zone	String
`rules`	List of rules	Array

Details of rules:

Field Name	Description	Data Type
`uuid`	Unique id of rule	Number
`state`	Is rule enabled or not	Boolean
`ruleDescription`	Description of rule	String

Field Name	Description	Data Type
`destObjList`	Destination rule object	Object
`serviceObjList`	Service rule object	Object
`action`	Action to be performed if the traffic matches this rule, can be "PERMIT"/ "DROP"	String
`islogging`	Is logging enabled for this rule	Boolean

Details of destObjList:

Field Name	Description	Data Type
`RuleObjectId`	Unique rule object id	String
`RuleObjectName`	Rule object name	String
`RuleObjectType`	Destination mode. Can be "IPV4_NETWORK" / "IPV4_ENDPOINT" /	String

Details of serviceObjList:

Field Name	Description	Data Type
`RuleObjectId`	Unique rule object id	String
`RuleObjectName`	Rule object name	String
`RuleObjectType`	Destination mode. Can be "SERVICE"	String
`ApplicationType`	Application type. Can be "DEFAULT" / "CUSTOM"	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/quarantineZone/220

Response

```
{ "quarantineZoneId": 220, "quarantineZoneName": "Quarantine20", "quarantineZoneDescription": "Desc:Adds a new
Quarantine Zone", "ownerId": 0, "visibleToChild": true, "isEditable": true, "quarantineZoneVersion": 0,
"lastModifiedTime": "2017-06-21 11:13:38", "lastModifiedUser": "admin", "rules": [ { "uuid": 125, "state": true,
"ruleDescription": "create a new rule", "destObjList": [], "serviceObjList": [], "action": "PERMIT",
"islogging": true }, { "uuid": 126, "state": true, "ruleDescription": "create a new rule", "destObjList":
[ { "ruleObjectId": "12", "ruleObjectName": "The 172.16.0.0/12 network", "ruleObjectType": "IPV4_NETWORK" } ],
"serviceObjList": [ { "ruleObjectId": "130", "ruleObjectName": "ssl", "ruleObjectType": "SERVICE",
"applicationType": "DEFAULT" } ], "action": "PERMIT", "islogging": true } ] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	500	1001	Invalid quarantine zone id

Get all Quarantine Zones at Domain Level

This URL retrieves details of all quarantine zones at given domain.

Resource URL

GET /domain/<domainId>/quarantineZone

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Payload Request Parameters:

None

Response Parameters

Following fields are returned if the operation was successful, otherwise error details are returned.

Field Name	Description	Data Type
`quarantineZoneList`	List of quarantine zones defined in the domain	Array

Details of quarantineZoneList:

Field Name	Description	Data Type
`quarantineZoneId`	Quarantine zone unique id	Number
`quarantineZoneName`	Name of quarantine zone	String
`quarantineZoneDescription`	Description of quarantine zone	String
`ownerId`	Domain id	Number
`visibleToChild`	Is quarantine one visible to child domain	Boolean
`isEditable`	Is quarantine zone editable or not	Boolean
`quarantineZoneVersion`	Quarantine zone version	Number
`lastModifiedTime`	The time quarantine zone last modified	String
`lastModifiedUser`	Last user that modified the quarantine zone	String
`rules`	Member rules of quarantine zone	Array

Details of rules:

Field Name	Description	Data Type
`uuid`	Unique id of rule	Number

Field Name	Description	Data Type
`state`	Is rule enabled or not	Boolean
`ruleDescription`	Description of rule	String
`destObjList`	Destination rule object	Object
`serviceObjList`	Service rule object	Object
`action`	Action to be performed if the traffic matches this rule, can be "PERMIT"/ "DROP"	String
`islogging`	Is logging enabled for this rule	Boolean

Details of destObjList:

Field Name	Description	Data Type
`RuleObjectId`	Unique rule object id	String
`RuleObjectName`	Rule object name	String
`RuleObjectType`	Destination mode. Can be "IPV4_NETWORK" / "IPV4_ENDPOINT" /	String

Details of serviceObjList:

Field Name	Description	Data Type
`RuleObjectId`	Unique rule object id	String
`RuleObjectName`	Rule object name	String
`RuleObjectType`	Destination mode. Can be "SERVICE"	String
`ApplicationType`	Application type. Can be "DEFAULT" / "CUSTOM"	String

Example

Request

GET https://<NSM_IP>/sdkapi/domain/0/quarantineZone

Payload

None

Response

```
{ "quarantineZoneList": [ { "quarantineZoneId": 201, "quarantineZoneName": "Quarantine1",
"quarantineZoneDescription": "Desc:Adds a new Quarantine Zone1", "ownerId": 0, "visibleToChild": true,
"isEditable": false, "quarantineZoneVersion": 0, "lastModifiedTime": "2017-06-21 11:13:29", "lastModifiedUser":
"admin", "rules": [ { "uuid": 101, "state": true, "ruleDescription": "create a new rule", "destObjList": [],
"serviceObjList": [], "action": "PERMIT", "islogging": true }, { "uuid": 102, "state": true, "ruleDescription":
"create a new rule", "destObjList": [], "serviceObjList": [], "action": "DROP", "islogging": true }, { "uuid":
103, "state": true, "ruleDescription": "create a new rule", "destObjList": [], "serviceObjList": [], "action":
"PERMIT", "islogging": false } ] }, { "quarantineZoneId": 51, "quarantineZoneName": "Allow Full Access",
"quarantineZoneDescription": "Default zone that provides full network access.", "ownerId": 0, "visibleToChild":
true, "isEditable": false, "quarantineZoneVersion": 0, "lastModifiedTime": "2017-06-21 10:29:54",
"lastModifiedUser": "admin", "rules": [ { "uuid": 31, "state": true, "ruleDescription": "Full Access",
"destObjList": [], "serviceObjList": [], "action": "PERMIT", "islogging": false } ] } ] }
```

Error Information

Following error code is returned by this URL:

No	SDK API errorId	SDK API errorMessage
1	1105	Invalid domain

Update Quarantine Zone

This URL updates given quarantine zone.

Resource URL

PUT /domain/<domainId>/quarantineZone/<quarantineZoneID>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes
`quarantineZoneID`	Quarantine zone id	Number	Yes

Payload parameters:

Field Name	Description	Data Type	Mandatory
`quarantineZoneName`	Name of quarantine zone	String	Yes
`quarantineZoneDescription`	Description of quarantine zone	String	Yes
`visibleToChild`	Is quarantine zone visible to child domain	Boolean	Yes
`rules`	List of rules	Array	Yes

Details of rules:

Field Name	Description	Data Type	Mandatory
`state`	Is rule enabled or not	Boolean	Yes
`ruleDescription`	Description of rule	String	No
`destObjList`	Destination rule object	Object	No
`serviceObjList`	Service rule object	Object	No
`action`	Action to be performed if the traffic matches this rule, can be "PERMIT"/ "DROP"	String	Yes
`islogging`	Is logging enabled for this rule	Boolean	Yes

Details of destObjList:

Field Name	Description	Data Type	Mandatory
RuleObjectId	Unique rule object id	String	Yes
RuleObjectName	Rule object name	String	Yes
RuleObjectType	Destination mode. Can be "IPV4_NETWORK" / "IPV4_ENDPOINT" /	String	Yes

Details of serviceObjList:

Field Name	Description	Data Type	Mandatory
RuleObjectId	Unique rule object id	String	Yes
RuleObjectName	Rule object name	String	Yes
RuleObjectType	Destination mode. Can be "SERVICE"	String	Yes
ApplicationType	Application type. Can be "DEFAULT" / "CUSTOM"	String	Yes

Response Parameters

Following fields are returned if the operation was successful, otherwise error details are returned.

Field Name	Description	Data Type
status	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domain/0/quarantineZone/220

Payload

```
{ "quarantineZoneName": "Quarantine20", "quarantineZoneDescription": "Desc:Adds a new Quarantine Zone",
"visibleToChild": true, "rules": [ { "state": true, "ruleDescription": "create a new rule", "destObjList": [ ],
"serviceObjList": [ ], "action": "PERMIT", "islogging": true }, { "state": true, "ruleDescription": "create a
new rule", "destObjList": [ { "ruleObjectId": "12", "ruleObjectName": "The 172.16.0.0/12 network",
"ruleObjectType": "IPV4_NETWORK" } ], "serviceObjList": [ { "ruleObjectId": "130", "ruleObjectName": "ssl",
"ruleObjectType": "SERVICE", "applicationType": "DEFAULT" } ], "action": "DROP", "islogging": false } ] }
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Invalid quarantine zone id
2	500	1001	Given policy cannot be updated at this domain
3	404	1105	Invalid domain

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
4	404	1720	Invalid rule object id/ rule object not visible to this domain.
5	500	1001	At least one rule is required.
6	500	1001	Quarantine zone description: field should not be empty
7	500	1001	Quarantine zone name: The maximum length for the field is 64
8	500	1001	Quarantine zone description: The maximum length for the field is 150
9	500	1001	Quarantine zone name: Field should not be empty
10	500	1001	Name must contain only letters, numerical, spaces, commas, periods, hyphens or underscores

Add Quarantine Zone

This URL adds a quarantine zone at given domain.

Resource URL

POST /domain/<domainId>/quarantineZone

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`quarantineZoneName`	Name of quarantine zone	String	Yes
`quarantineZoneDescription`	Description of quarantine zone	String	Yes
`visibleToChild`	Is quarantine zone visible to child domain	Boolean	Yes
`rules`	List of rules	Array	Yes

Details of rules:

Field Name	Description	Data Type	Mandatory
state	Is rule enabled or not	Boolean	Yes
ruleDescription	Description of rule	String	No
destObjList	Destination rule object	Object	No
serviceObjList	Service rule object	Object	No
action	Action to be performed if the traffic matches this rule, can be "PERMIT"/ "DROP"	String	Yes
islogging	Is logging enabled for this rule	Boolean	Yes

Details of destObjList:

Field Name	Description	Data Type	Mandatory
RuleObjectId	Unique rule object id	String	Yes
RuleObjectName	Rule object name	String	Yes
RuleObjectType	Destination mode. Can be "IPV4_NETWORK" / "IPV4_ENDPOINT" /	String	Yes

Details of serviceObjList:

Field Name	Description	Data Type	Mandatory
RuleObjectId	Unique rule object id	String	Yes
RuleObjectName	Rule object name	String	Yes
RuleObjectType	Destination mode. Can be "SERVICE"	String	Yes
ApplicationType	Application type. Can be "DEFAULT" / "CUSTOM"	String	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
createdResourceId	Unique id of the created quarantine zone	Number

Example

Request

POST https://<NSM_IP>/sdkapi/domain/0/quarantineZone

Payload

```
{ "quarantineZoneName": "Quarantine1", "quarantineZoneDescription": "Desc:Adds a new Quarantine Zone",
"visibleToChild": true, "rules": [ { "state": true, "ruleDescription": "create a new rule", "destObjList": [ ],
"serviceObjList": [ ], "action": "PERMIT", "islogging": true }, { "state": true, "ruleDescription": "create a
new rule", "destObjList": [ { "ruleObjectId": "12", "ruleObjectName": "The 172.16.0.0/12 network",
"ruleObjectType": "IPV4_NETWORK" } ], "serviceObjList": [ { "ruleObjectId": "130", "ruleObjectName": "ssl",
"ruleObjectType": "SERVICE", "applicationType": "DEFAULT" } ], "action": "DROP", "islogging": false } ] }
```

Response

```
{ "createdResourceId": 243 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error - Failed to add NAZ definition. A NAZ with the same name already exists.
2	404	1105	Invalid domain
3	404	1720	Invalid rule object id/ rule object not visible to this domain
4	500	1001	At least one rule is required.
5	500	1001	Quarantine zone description: field should not be empty
6	500	1001	Quarantine zone name: The maximum length for the field is 64
7	500	1001	Quarantine zone description: The maximum length for the field is 150
8	500	1001	Quarantine zone name: Field should not be empty
9	500	1001	Name must contain only letters, numerical, spaces, commas, periods, hyphens or underscores

Delete Quarantine Zone

This URL deletes a quarantine zone.

Resource URL

DELETE /domain/<domainId>/quarantineZone

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	Domain id	Number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
`quarantineZoneIdsList`	List of quarantine zone id's	Array	Yes

Response Parameters

Following fields are returned if the operation was successful, otherwise error details are returned.

Field Name	Description	Data Type
status	Set to 1 if the operation was successful	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/domain/0/quarantineZone

Payload

```
{"quarantineZoneIdsList": [216]}
```

Response

```
{ "status": 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	The following policies cannot be deleted because of dependency
2	500	1001	Following policies cannot be deleted at this domain
3	404	1105	Invalid domain
4	404	1001	Internal error

Get the GTI Private Cloud Configuration

This URL gets the GTI private cloud configuration present on the Manager.

Resource URL

GET /gticonfiguration/private

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Response Parameters

Returns the following fields.

Field Name	Description	Data Type
`enabled`	GTI private cloud is enabled or not	Boolean
`server`	Server IP	String
`certificateStatus`	GTI private cloud certificate is present or not	Boolean

Example

Request

GET https://<NSM_IP>/sdkapi/gticonfiguration/private

Payload

None

Response

```
{ "enabled":false,"server":null,"certificateStatus":false }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Update the GTI Private Cloud Configuration

This URL updates the GTI private cloud configuration present on the Manager.

Resource URL

PUT /gticonfiguration/private

Request Parameters

URL Parameters: None

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`enabled`	GTI private cloud is enabled or not	Boolean	Yes
`server`	Server IP	String	Yes

Response Parameters

Returns the following fields.

Field Name	Description	Data Type
`status`	Set to 1 if the update is successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/gticonfiguration/private

Payload

```
{ "enabled":false,"server":null,"certificateStatus":false }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	1111	Certificate should be present on the Manager
3	400	1111	Invalid IP address

Import GTI Private Cloud Certificate to the Manager

This URL imports the GTI private cloud certificate file to the Manager.

Resource URL

PUT /gticonfiguration/private/importcert

Request Parameters

URL Parameters: None

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`MultiPart`	Holds the objects of the body part	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
`BodyPart[0]`	Holds the file format object	Application/json object	Yes

Details of FileFormat:

Field Name	Description	Data Type	Mandatory
`fileName`	Name of the file	String	Yes

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
`BodyPart[1]`	Holds the license file as an input stream	Application/octet-stream	Yes

Details of certificate file:

Field Name	Description	Data Type	Mandatory
`File`	The certificate file data	ByteArrayInputStream	Yes

Response Parameters

Returns the following fields:

Field Name	Description	Data Type
`status`	Set to 1 if the update is successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/gticonfiguration/private/importcert

Payload

```
--Boundary_1_17241377_1362484380857 Content-Type: application/json {"fileName":"certificate.zip"} --
Boundary_1_17241377_1362484380857 Content-Type: application/octet-stream File data --
Boundary_1_17241377_1362484380857--
```

Response

```
{ 'status' : 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	5301	Invalid file type given for import: The file name does not have any extension

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
3	400	5301	Invalid file type given for import expected is .zip while <filetype> was provided

Get the IP Status from a GTI Private Cloud

This URL gets the IP status from GTI private cloud configured on the Manager.

Resource URL

GET /gticonfiguration/private/{ip_address}/testconnection

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`ip_address`	IP address whose status you want to know	String	Yes

Payload Request Parameters: None

Response Parameters

Returns the following fields.

Field Name	Description	Data Type
`status`	Reputation of the IP on the GTI private cloud	String
`country`	Country of the IP. If information about the country is not available, returns an empty string as the value.	String

Example

Request

GET https://<NSM_IP>/sdkapi/gticonfiguration/private/1.1.1.1/testconnection

Payload

None

Response

```
{ "status":"High","country":"" }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Get the Telemetry Configuration

This URL gets the telemetry configuration present on the Manager.

Resource URL

GET /gticonfiguration

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`alertDataDetails`	Alert data details	Object
`alertDataSummary`	Should the alert data summary be included in data send to telemetry	Boolean
`generalSetup`	Should the general setup data be included in data send to telemetry	Boolean
`featureUsage`	Should the feature usage data be included in data send to telemetry	Boolean
`systemFaults`	Should the system faults data be included in data send to telemetry	Boolean
`technicalContactInformation`	Contact details in the organization	Object

Details of fields in alertDataDetails:

Field Name	Description	Data Type
`AlertDataDetailsEnabled`	Alert data details to be sent	Boolean
`excludedIpList`	IP's excluded	Array
`alertDetaDetailsFilterLevel`	Alert data filter level	Object

Details of fields in technicalContactInformation:

Field Name	Description	Data Type
`sendContactInfo`	Send contact information	Boolean
`firstName`	First name	String
`lastName`	Last name	String
`address`	Address	String
`phone`	Phone	String
`email`	Email	String

Details of fields in alertDetaDetailsFilterLevel:

Field Name	Description	Data Type
`high`	Include high severity alerts	Boolean
`low`	Include low severity alerts	Boolean
`medium`	Include medium severity alerts	Boolean
`informational`	Include informational severity alerts	Boolean

Example

Request

GET https://<NSM_IP>/sdkapi/gticonfiguration

Payload

None

Response

```
{ "alertDataDetails":{"AlertDataDetailsEnabled":true,"excludedIpList":
["1.1.1.1/32"],"alertDetaDetailsFilterLevel":
{"high":true,"low":true,"medium":true,"informational":true}},"alertDataSummary":true,
"generalSetup":true,"featureUsage":true,"systemFaults":true,"technicalContactInformation":
{"sendContactInfo":true,"firstName":"Mcafee","lastName":"Mcafee","address":"MIC","phone":"1234567890","email":"E
IT@mcafee.com"} }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Update the Telemetry Configuration

This URL updates the telemetry configuration present on the Manager.

Resource URL

PUT /gticonfiguration

Request Parameters

URL Parameters: None

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`alertDataDetails`	Alert data details	Object	Yes
`alertDataSummary`	Should the alert data summary be included in data send to telemetry	Boolean	Yes
`generalSetup`	Should the general setup data be included in data send to telemetry	Boolean	Yes

Field Name	Description	Data Type	Mandatory
`featureUsage`	Should the feature usage data be included in data send to telemetry	Boolean	Yes
`systemFaults`	Should the system faults data be included in data send to telemetry	Boolean	Yes
`technicalContactInformation`	Contact details in the organization	Object	Yes

Details of fields in alertDataDetails:

Field Name	Description	Data Type	Mandatory
`AlertDataDetailsEnabled`	Alert data details to be sent	Boolean	Yes
`excludedIpList`	Exclude IP address information for endpoints on this list	Array	No
`alertDetaDetailsFilterLevel`	Alert data filter level	Object	Yes

Details of fields in technicalContactInformation:

Field Name	Description	Data Type	Mandatory
`sendContactInfo`	Send contact information	Boolean	Yes
`firstName`	First name	String	No
`lastName`	Last name	String	No
`address`	Address	String	No
`phone`	Phone	String	No
`email`	Email	String	No

Details of fields in alertDetaDetailsFilterLevel:

Field Name	Description	Data Type	Mandatory
`high`	Include high severity alerts	Boolean	Yes
`low`	Include low severity alerts	Boolean	Yes
`medium`	Include medium severity alerts	Boolean	Yes
`informational`	Include informational severity alerts	Boolean	Yes

Response Parameters

Returns the following fields:

Field Name	Description	Data Type
`status`	Set to 1 if the update is successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/gticonfiguration

Payload

```
{ "alertDataDetails":{"AlertDataDetailsEnabled":true,"excludedIpList":["1.1.1.1/32"],
"alertDetaDetailsFilterLevel":{"high":true,"low":true,"medium":true,"informational":true}},
"alertDataSummary":true,"generalSetup":true,"featureUsage":true,"systemFaults":true,
"technicalContactInformation":{"sendContactInfo":true,"firstName":"Mcafee",
"lastName":"Mcafee","address":"MIC","phone":"1234567890","email":"EIT@mcafee.com"} }
```

Response

```
{ "status":1 }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Get the vIPS Licenses Present on the Manager

This URL gets the vIPS licenses present on the Manager.

Resource URL

GET /license/vmips

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Response Parameters

Returns the following fields.

Field Name	Description	Data Type
`compliant`	Compliant state of the Manager	Boolean
`additionalLicensesRequired`	The number of additional licenses required	Number
`virtualSensors`	License usage status in virtual Sensors	String
`virtualProbes`	License usage status in virtual probes	String
`licenses`	List of individual VMIPS license details	Array of objects

Details of fields in VMIPSLicenseDetails:

Field Name	Description	Data Type
`Allowed`	Number of vNSP Sensors allowed	Number
`licenseCustomer`	Customer of the license	String
`key`	License key	String
`comment`	Comment	String
`addedBy`	User who added the license	String
`addedTime`	Time when the license was added	String
`licenseGrantID`	License grant id	String
`licenseExpiration`	License expiration date	String

Example

Request

GET https://<NSM_IP>/sdkapi/license/vmips

Payload

None

Response

```
{ "compliant": True, "additionalLicensesRequired": 0, "virtualSensors": "0 (of 10 allowed) in use",
"virtualProbes": "0 in use", "licenses": [ {"comment": None, "licenseCustomer": "Ingram Micro Inc.", "addedBy":
"admin", "key": "0007010100-NAI-000010", "allowed": 10, "addedTime": "Oct 23 05:11:25 2019", "licenseGrantID":
"0007010100-NAI", "licenseExpiration": "12-31-2043"} ] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Get the Proxy Licenses Present on the Manager

This URL retrieves the proxy licenses present on the Manager.

Resource URL

GET /license/proxy

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Response Parameters

Returns the following fields.

Field Name	Description	Data Type
`Licenses`	List of individual license details parameter	Array of objects

Details of fields in LicenseDetails:

Field Name	Description	Data Type
`allowanceModel`	Sensor model allowed for the license	String
`Capacity`	Sensor capacity supported by the license	String
`licenseCustomer`	Customer of the license	String
`key`	License key	String
`comment`	Comment	String
`addedBy`	User who added the license	String
`addedTime`	Time when the license was added	String
`licenseGrantID`	License grant id	String
`licenseExpiration`	License expiration date	String
`targetType`	Type of the target e.g, Sensor	String

Field Name	Description	Data Type
`targetIdAssociated`	Target id associated with the license e.g., sensorId	String
`deviceName`	Name of the device associated with the license	String
`GrantIndex`	Grant index of the license	Int
`licenseId`	License id	String

Example

Request

GET https://<NSM_IP>/sdkapi/license/proxy

Payload

None

Response

```
{ "licenses": [ "comment": None, "targetType": "SENSOR", "licenseCustomer": "McAfee Inc. - for Eval Purposes
Only", "capacity": "30 Gbps", "deviceName": "/My Company/Test Child Domain 1/denali-1", "allowanceModel": "IPS-
NS9500", "addedBy": "admin", "targetIdAssociated": "1006", "key": "80002-1", “licenseId”: ”80002”, “grantIndex”:
1, "addedTime": "Oct 22 12:20:09 2019", "licenseGrantID": "0010080", "licenseExpiration": "09-12-2020"] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Get the Capacity Licenses Present on the Manager

This URL gets the capacity licenses present on the Manager.

Resource URL

GET /license/capacity

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Response Parameters

Returns the following fields.

Field Name	Description	Data Type
`licenses`	List of individual license details parameter	Array of objects

Details of fields in LicenseDetails:

Field Name	Description	Data Type
`allowanceModel`	Sensor model allowed for the license	String
`Capacity`	Sensor capacity supported by the license	String
`licenseCustomer`	Customer of the license	String
`key`	License key	String
`comment`	Comment	String
`addedBy`	User who added the license	String
`addedTime`	Time when the license was added	String
`licenseGrantID`	License grant id	String
`licenseExpiration`	License expiration date	String
`targetType`	Type of the target e.g, Sensor	String
`targetIdAssociated`	Target id associated with the license e.g., sensorId	String
`deviceName`	Name of the device associated with the license	String
`GrantIndex`	Grant index of the license	Int
`licenseId`	License Id	String

Example

Request

GET https://<NSM_IP>/sdkapi/license/capacity

Payload

None

Response

```
{ "licenses": [ "comment": None, "targetType": "SENSOR", "licenseCustomer": "McAfee Inc. - for Eval Purposes
Only", "capacity": "20 Gbps", "deviceName": "/My Company/Test Child Domain 1/denali-1", "allowanceModel": "IPS-
NS9500", "addedBy": "admin", "targetIdAssociated": "1006", "key": "50002-1", “licenseId”: ”50002”, “grantIndex”:
1, "addedTime": "Oct 22 12:20:09 2019", "licenseGrantID": "0030080", "licenseExpiration": "09-12-2020"] }
```

Error Information

Following error code is returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Import License to the Manager

This URL imports a license file to the Manager.

Resource URL

PUT /license

Request Parameters

URL Parameters: None

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`MultiPart`	Holds the body part objects	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
`BodyPart[0]`	Holds the file format object	Application/json object	Yes

Details of file format:

Field Name	Description	Data Type	Mandatory
`fileName`	Name of the file	String	Yes
`oldLicense`	Details of the existing license that should be upgraded. **Note:** This information is required only when an upgrade license is imported.	Object	No

Details of oldLicense:

Field Name	Description	Data Type	Mandatory
`licenseId`	License id which needs to be upgraded	String	Yes
`grantIndex`	Grant Index of the license which needs to be upgraded	String	Yes

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
`BodyPart[1]`	Holds the license file as an input stream	Application/octet-stream	Yes

Details of license file:

Field Name	Description	Data Type	Mandatory
`File`	The license file data	ByteArrayInputStream	Yes

Response Parameters

Following field is returned.

Field Name	Description	Data Type
`status`	Set to 1 if the request is successful	number

Example

Request

PUT https://<NSM_IP>/sdkapi/license

Payload

```
NSM-SDK-API: QjUzNDQzMjNCNUQ2NkEzQjc4Mzc5REMxRjMxMDg0OTE6MQ== Accept: application/vnd.nsm.v1.0+json Content-
Type: multipart/form-data; boundary=Boundary_1_17241377_1362484380857 MIME-Version: 1.0 User-Agent: Java/
1.6.0_25 Host: localhost:8888 Connection: keep-alive Content-Length: 15956464 --
Boundary_1_17241377_1362484380857 Content-Type: application/json {"fileName":"VMIPSLICENCE_sdkapi.jar"} --
Boundary_1_17241377_1362484380857 Content-Type: application/octet-stream File data --
Boundary_1_17241377_1362484380857--
```

Response

```
{ 'status' : 1 }
```

Error Information

Following error codes are returned by this URL

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	500	1001	Internal error message: <message>

Assign a License

This URL assigns a license to the device.

Resource URL

PUT /license/assignlicense

Request Parameters

URL Parameters: None

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`licenseId`	License id	String	Yes
`grantIndex`	Grant Index of the license	String	Yes
`grantId`	Grant id of the license	String	Yes
`sensorId`	Sensor id to be associated with license	String	Yes

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the request is successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/assignlicense

Payload

```
{ "licenseId": "50002", "grantIndex": "3", "grantId": "0030080", "sensorId": "1006" }
```

Response

```
{ 'status' : 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	500	1001	License <licenseId> cannot be assigned to the Sensor <sensorId>

Unassign a License

This URL unassign's a license associated with the device.

Resource URL

PUT /license/unassignlicense

Request Parameters

URL Parameters: None

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`licenseId`	License id	String	Yes
`grantIndex`	Grant Index of the license	String	Yes
`grantId`	Grant id of the license	String	Yes
`sensorId`	Sensor id to be associated with license	String	No

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the unassignment is successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/unassignlicense

Payload

```
{ “licenseId”: “50002”, “grantIndex”: “3”, “grantId”: “0030080”, }
```

Response

```
{ 'status' : 1 }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Delete Licenses

This URL deletes licenses.

Resource URL

DELETE /license/delete/<licensetype>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
licensetype	License type can be one of the following: 1. Proxy 2. Capacity 3. vIPS	String	Yes

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
licenseId	List of license id's	Array of string	Yes

Response Parameters

Returns the following fields.

Field Name	Description	Data Type
status	Set to 1 if the deletion is successful	Number

Example

Request

DELETE https://<NSM_IP>/sdkapi/license/delete/proxy

Payload

```
{ 'licenseId': ['10004'] }
```

Response

```
{ "status": 1 }
```

Error Information

Following error code is returned by this URL

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

Get the Sensors for Association

This URL retrieves the Sensors which can be associated with the given license.

Resource URL

GET /license/getSensorsforassociation

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`model`	Model allowed for the license	String	Yes
`licenseId`	License id	String	Yes

Payload Request Parameters: None

Response Parameters

Returns the following fields.

Details of the fields in usage.

Field Name	Description	Data Type
`sensorDetailsList`	List of Sensor details that can be associated with license	Object

Details of fields in virtualSensors:

Field Name	Description	Data Type
`sensorId`	Sensor id	Number
`peerSensor`	Peer Sensor id	Number
`deviceName`	Device name	String

Example

Request

GET https://<NSM_IP>/license//getSensorsforassociation?model=IPS-NS9500&licenseId=00001

Payload

None

Response

```
{ "sensorDetailsList": [ {"sensorId": 1002, "peerSensor": None, "deviceName": "/My Company/Test Child Domain 1/
NS9500_2"}, {"sensorId": 1006, "peerSensor": "denali-2", "deviceName": "/My Company/Test Child Domain 1/
denali-1"}, {"sensorId": 1007, "peerSensor": "denail-1", "deviceName": "/My Company/Test Child Domain 1/
denali-2"}]}
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	500	4812	License with the given id does not exist

Get IPS Inspection Allowlist from the Manager

This URL retrieves the domain name exceptions from the Manager.

Resource URL

GET /domainnameexceptions/ipsinspectionallowlist

Request Parameters

URL Parameters: None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
dneDetail	List of domains from the IPS Inspection allowlist	ObjectList

Details of dneDetail :

Field Name	Description	Data Type
id	Domain name exception id	Number
state	State of the domain name exception (Enabled/Disabled)	String
domainName	Name of the domain	String
comment	Description of the exception	String
domainType	Type of the domain (Custom/Default)	String
lastUpdated	Details of the time and username under which the domain name exception was added	String

Example

Request

GET https://<NSM_IP>/sdkapi/domainnameexceptions/ipsinspectionallowlist

Response

```
{ 'dneDetail': [{ 'id': 10118, ‘state’: ‘E’, 'domainName':'www.google.com', ‘comment’: ‘Google’ ‘domainType’:
‘C’, 'lastUpdated': 'Jan 13 6:35 (admin)' }, { 'id': 10119, ‘state’: ‘E’, 'domainName':'www.abc.com', ‘comment’:
‘abc domain’ ‘domainType’: ‘C’, 'lastUpdated': 'Jan 13 6:39 (admin)' }, { 'id': 10120, ‘state’: ‘D’,
'domainName':'www.yahoo.com', ‘comment’: ‘ ’ ‘domainType’: ‘C’, 'lastUpdated': 'Jan 13 6:45 (admin)' }] }
```

Error Information

None

Get Details of a Domain Name from IPS Inspection Allowlist

This URL retrieves the details of the domain name exception from the IPS inspection allowlist.

Resource URL

GET /domainnameexceptions/ipsinspectionallowlist/IPSDNEDetail/<domainName>

Request Parameters

URL Parameters:

Field Name	Description	Data Type
`domainName`	Name of the domain	String

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`dneDetail`	List of domains from the IPS inspection allowlist	ObjectList

Details of dneDetail :

Field Name	Description	Data Type
`id`	Domain name exception id	Number
`state`	State of the domain name exception (Enabled/Disabled)	String
`domainName`	Name of the domain	String
`comment`	Description of the exception	String
`domainType`	Type of the domain (Custom/Default)	String
`lastUpdated`	Details of the time and username under which the domain name exception was added	String

Example

Request

GET https://<NSM_IP>/domainnameexceptions/ipsinspectionallowlist/IPSDNEDetail/www.google.com

Response

```
{ 'dneDetail': [{ 'id': 10118, ‘state’: ‘E’, 'domainName':'www.google.com', ‘comment’: ‘Google’ ‘domainType’:
‘C’, 'lastUpdated': 'Jan 13 6:35 (admin)' }, }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: Internal server error
2	500	1001	Internal error message: Domain name not found

Add Domain Name to IPS Inspection Allowlist

This URL adds domain name to IPS inspection allowlist.

Resource URL

POST /domainnameexceptions/ipsinspectionallowlist

Request Parameters

URL Parameters: None

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`domainName`	Name of the new domain	String	Yes
`State`	State of the domain. Can either be "E" or "D".	String	No
`comment`	Description of the execution	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Unique Id of created IPS inspection allowlist	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/domainnameexceptions/ipsinspectionallowlist

Payload

```
{ “state”: “E”, "domainName": "www.google1.com", "comment": "updated domain" }
```

Error Information

Response

```
{ "createdResourceId": 10010 }
```

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: Internal server error
2	500	1001	Internal error message: Domain name field is required
3	500	1001	Invalid domain name. The length should be a maximum of 67 characters.
4	500	1001	Invalid domain name

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
5	500	1001	Duplicate domain name

Import the Domain Name Exceptions to the Manager

This URL imports the domain names from the IPS inspection allowlist to the Manager.

Resource URL

POST /domainnameexceptions/ipsinspectionallowlist/import

Request Parameters

URL Parameters: None

Payload Request Parameters

Field Name	Description	Data Type	Mandatory
`MultiPart`	Holds the body part objects	Object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
`BodyPart[0]`	Holds the DNE file element object	Application/json object	Yes

Details of DNEFileElement:

Field Name	Description	Data Type	Mandatory
`fileName`	Name of the file with the extension	String	Yes
`fileType`	File type should be .csv	String	No

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
`BodyPart[1]`	Holds the input stream	Application/json object	Yes

Details of .csv file:

Field Name	Description	Data Type	Mandatory
`File`	Domain name exceptions input stream	ByteArrayInput stream	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Request

POST https://%3CNSM_IP%3E/sdkapi/domainnameexceptions/ipsinspectionallowlist/import

Payload

```
----Boundary_1_12424925_1353496814940 Content-Type: application/json {"fileType": null, "fileName": "dne.csv"}
----Boundary_1_12424925_1353496814940 Content-Type: application/octet-stream www.google.com, www.yahoo.com,
www.abc.com, www.test1.com, www.test2.com ----Boundary_1_12424925_1353496814940--
```

Error Information

Response

```
{ "status":1 }
```

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	2202	Input stream read error
2	500	1001	Invalid file format. Import supported for CSV files only
3	500	1001	One or more invalid domain detected in the file.

Export the Domain Name Exceptions from the Manager

This URL exports all custom domain name exceptions from the IPS inspection allowlist.

Resource URL

GET /domainnameexceptions/ipsinspectionallowlist/export

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`byteStream`	Byte stream of the exported file	String

Example

Request

GET https://%3CNSM_IP%3E/sdkapi/domainnameexceptions/ipsinspectionallowlist/export

Response

```
{ byteStream": "www.google.com,\nwww.yahoo.com,\nwww.abc.com,\nwww.test1.com,\nwww.test2.com" }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: Internal server error

Update the Details of Domain Name Exceptions

This URL updates the details of the domain name exception from the IPS inspection allowlist.

Resource URL

PUT /domainnameexceptions/ipsinspectionallowlist

Request Parameters

URL Parameters: None

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`oldDomainName`	Name of the old domain	String	Yes
`domainName`	Name of the nee domain	String	Yes
`state`	State of the domain. Either "E" or "D".	String	No
`comment`	Description of the exception	String	No

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://%3CNSM_IP%3E/sdkapi/domainnameexceptions/ipsinspectionallowlist

Payload

```
{ "state": "E", "oldDomainName": "www.google2.com", "domainName": "www.google3.com", "comment": "updated
domain" }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: Internal server error

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
2	500	1001	Internal error message: Domain name is not found <domainName>
3	500	1001	Invalid domain name. The length should be a maximum of 67 characters.
4	500	1001	Invalid domain name
5	500	1001	Duplicate domain name

Delete Domain Name Exceptions from the IPS Inspection Allowlist

This URL deletes the domain name exceptions specified in the string list.

Resource URL

DELETE /domainnameexceptions/ipsinspectionallowlist

Request Parameters

URL Parameters: None

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`domainName`	List of domain names	StringList	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

DELETE https://%3CNSM_IP%3E/sdkapi/domainnameexceptions/ipsinspectionallowlist

Payload

```
{ "domainName": ["www.google.com", "www.abc.com", "www.test.com"] }
```

Response

```
{ "status":1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: Internal server error
2	500	1001	Internal error message: no domain name is given to delete.
3	500	1001	Deletion failed: Domain name <domainName> does not exist.
4	500	1001	One or more of the selected domain name is a default domain, which cannot be deleted.
5	500	1001	Duplicate domain name

Delete all Domain Names from IPS Inspection Allowlist

This URL deletes all domain name exceptions.

Resource URL

DELETE /domainnameexceptions/ipsinspectionallowlist/all

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

DELETE https://%3CNSM_IP%3E/sdkapi/domainnameexceptions/ipsinspectionallowlist/all

Payload

None

Response

```
{ “status”:1 }
```

Error Information

Following error code is returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Error while deleting all DNEs

Update Status of Domain Name Exceptions from IPS Inspection Allowlist

This URL updates the status of domain name exceptions specified in the integer list.

Resource URL

PUT /domainnameexceptions/ipsinspectionallowlist/bulkUpdate

Request Parameters

URL Parameters: None

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
`state`	State of the domain names. Either "E" or "D".	String	Yes
`entryIDs`	List of entry id's of domain names to be updated	IntegerList	Yes

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

PUT https://<NSM_IP>/sdkapi/domainnameexceptions/ipsinspectionallowlist/bulkUpdate

Payload

```
{ "state": “D” “entryIDs”: [10118,10119] }
```

Response

```
{ “status”:1 }
```

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error message: Internal server error
2	500	1001	Internal error message: Error while bulk update

Get all the SSL Outbound Exception Rules

This URL gets all the outbound exception rules at domain level.

Resource URL

GET /domain/<domainId>/outboundsslexceptions

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	The id of the domain	Number	Yes

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`rules`	List of outbound exception rules	Array

Details of object in rules:

Field Name	Description	Data Type
`id`	Id of the outbound SSL	Number
`state`	State of the rule (Enabled/Disabled)	String
`name`	Name of the rule	String
`resource`	List of resources on which the rule has to be assigned	Array
`attacker`	List of the objects in the source network rule	Object
`target`	List of the objects in the destination network rule	Object
`targetHostName`	List of the objects in the target host names rule	Array
`targetUrlCategories`	List of URL categories	Array
`lastUpdatedByTime`	Time of the last update	String
`lastUpdatedByUserName`	User under which the last update occurred	String
`comment`	Comment	String
`ownerDomain`	Domain	String

Details of object in resource:

Field Name	Description	Data Type
`resourceId`	ID of the resource	Number
`resourceName`	Name of the resource	String
`resourceType`	Indicates the type of interface on which the Ignore Rule is created. The possible values include: • 0: The resource type is domain (for rules defined at the domain level) • 1: The resource type is Sensor (for rules defined that the Sensor level) • 2: The resource type is Vids (for rules defined at the interface and the sub-interface level) • 3: The resource type is NTBA_ZONE (for rules defined at NTBA inside and outside zones) • 4: The resource type is NTBA_SENSOR (for rules defined at NTBA level) • 5: The resource type is NTBA_DOMAIN	Number
`sensorId`	Id of the Sensor	Number

Details of the attacker:

Field Name	Description	Data Type
`AttackerEndPoint`	Attacker rule objects on which the ignore rules will be applied.	Array of string

Details of the target:

Field Name	Description	Data Type
`TargetEndPoint`	Target rule objects on which the ignore rules will be applied.	Array of string

Request

GET https://<NSM_IP>/sdkapi/domain/0/outboundsslexceptions

Response

```
{ "rules":[{"id":176,"state":"ENABLED","name":"test","attack":null,"resource":[],"attacker":{"AttackerEndPoint":
["FireWall_IPv4_Dst_15_1_7_251"], "AttackerPort":"ANY","AttackerPortNumber":null},"target":{"TargetEndPoint":
["FireWall_IPv4_Dst_15_1_7_251"],"TargetPort":"ANY", "TargetPortNumber":null},"targetHostName":
[],"targetUrlCategories":["Entertainment"],"lastUpdatedByTime":1519627703000,
"lastUpdatedByUserName":"admin","comment":"test","ownerDomain":"My Company"}] }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
2	500	1001	Internal error

Get Single Outbound Exception Rule

This URL gets a single outbound exception rule.

Resource URL

GET /domain/<domainId>/outboundsslexceptions/<ruleId>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	The id of the domain	Number	Yes
`ruleId`	The id of the rule	Number	Yes

Payload Request Parameters: None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`id`	ID of the outbound SSL	Number
`state`	State of the rule (Enabled/Disabled)	String
`name`	Name of the rule	String
`resource`	List of resources on which the rule has to be assigned	Array
`attacker`	List of the objects in the source network rule	Object
`target`	List of the objects in the destination network rule	Object
`targetHostName`	List of the objects in the target host names rule	Array
`targetUrlCategories`	List of URL categories	Array
`lastUpdatedByTime`	Time of the last update	String
`lastUpdatedByUserName`	User under which the last update occurred	String
`comment`	Comment	String
`ownerDomain`	Domain	String

Details of object in resource:

Field Name	Description	Data Type
`resourceId`	ID of the resource	Number
`resourceName`	Name of the resource	String
`resourceType`	Indicates the type of interface on which the Ignore Rule is created. The possible values include: • 0: The resource type is domain (for rules defined at the domain level) • 1: The resource type is Sensor (for rules defined that the Sensor level) • 2: The resource type is Vids (for rules defined at the interface and the sub-interface level) • 3: The resource type is NTBA_ZONE (for rules defined at NTBA inside and outside zones) • 4: The resource type is NTBA_SENSOR (for rules defined at NTBA level) • 5: The resource type is NTBA_DOMAIN	Number
`sensorId`	Id of the Sensor	Number

Details of the attacker:

Field Name	Description	Data Type
`AttackerEndPoint`	Attacker rule objects on which the ignore rules will be applied.	Array of string

Details of the target:

Field Name	Description	Data Type
`TargetEndPoint`	Target rule objects on which the ignore rules will be applied.	Array of string

Payload

None

Request

GET https://%3CNSM_IP%3E/sdkapi/domain/0/outboundsslexceptons/101

Response

```
{ "id":101,"state":"ENABLED","name":"test","attack":null,"resource":[],"attacker":{"AttackerEndPoint":
["FireWall_IPv4_Dst_15_1_7_251"], "AttackerPort":"ANY","AttackerPortNumber":""},"target":{"TargetEndPoint":
["FireWall_IPv4_Dst_15_1_7_251"],"TargetPort":"ANY", "TargetPortNumber":""},"targetHostName":
[],"targetUrlCategories":["Entertainment"],"lastUpdatedByTime":1519627703000,
"lastUpdatedByUserName":"admin","comment":"test","ownerDomain":"My Company" }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal server error
2	404	1408	Invalid rule id or provided rule id is not visible to this domain

Create an Outbound Exception Rule

This URL creates an outbound exception rule.

Resource URL

POST /domain/<domainId>/outboundsslexceptions

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	The id of the domain	Number	Yes

Payload Request Parameters:

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type	Mandatory
`state`	State of the rule (Enabled/ Disabled)	String	Yes
`name`	Name of the rule	String	Yes
`resource`	List of resources on which the rule has to be assigned	Array	No
`attacker`	List of the objects in the source network rule	Object	Yes
`target`	List of the objects in the destination network rule	Object	Yes
`targetHostName`	List of the objects in the target host names rule	Array	Yes
`targetUrlCategories`	List of URL categories	Array	Yes
`comment`	Comment	String	No

Details of object in resource:

Field Name	Description	Data Type	Mandatory
`resourceName`	Name of the resource	String	Yes

Details of the attacker:

Field Name	Description	Data Type	Mandatory
`AttackerEndPoint`	Attacker rule objects on which the ignore rules will be applied.	Array of string	Yes

Details of the target:

Field Name	Description	Data Type	Mandatory
`TargetEndPoint`	Target rule objects on which the ignore rules will be applied.	Array of string	Yes

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`createdResourceId`	Set to the ID of the rule if the operation was successful	Number

Example

Request

POST https://%3CNSM_IP%3E/sdkapi/domain/0/outboundsslexceptions

Payload

```
{ "state": "ENABLED", "name": "test1", "attack": null, "resource": [], "attacker": { "AttackerEndPoint":
[ "FireWall_IPv4_Dst_15_1_7_251" ] }, "target": { "TargetEndPoint": [ "FireWall_IPv4_Dst_15_1_7_251" ] },
"targetHostName": [], "targetUrlCategories": [ "Entertainment" ], "comment": "test" }
```

Response

```
{ "createdResourceId": 101 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal server error
2	400	1720	Invalid rule object/rule object is not visible in this domain
3	400	2513	Name must only contain letters, numerical, spaces, commas, periods, hyphen, or an underscore
4	400	1437	Rule name should not be longer than 64 characters
5	400	1433	This rule is invalid because it matches all alerts. Please specify at least one alert criterion.

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
6	400	1422	Resource is not visible in this domain
7	400	1001	Ignore Rule with the same name already exists
8	400	1435	The same combination of IPv4 and IPv6 should be used in the attacker and the target endpoints.
9	400	1408	The following URLs are invalid: <url_list>

Update an Outbound Exception Rule

This URL updates an outbound exception rule.

Resource URL

PUT /domain/<domainId>/outboundsslexceptions/<ruleId>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	The id of the domain	Number	Yes
`ruleId`	The id of the rule	Number	Yes

Payload Request Parameters: None

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type	Mandatory
`state`	State of the rule (Enabled/ Disabled)	String	Yes
`name`	Name of the rule	String	Yes
`resource`	List of resources on which the rule has to be assigned	Array	No
`attacker`	List of the objects in the source network rule	Object	Yes
`target`	List of the objects in the destination network rule	Object	Yes
`targetHostName`	List of the objects in the target host names rule	Array	Yes
`targetUrlCategories`	List of URL categories	Array	Yes

Field Name	Description	Data Type	Mandatory
`comment`	Comment	String	No

Details of object in resource:

Field Name	Description	Data Type	Mandatory
`resourceName`	Name of the resource	String	Yes

Details of the attacker:

Field Name	Description	Data Type	Mandatory
`AttackerEndPoint`	Attacker rule objects on which the ignore rules will be applied.	Array of string	Yes

Details of the target:

Field Name	Description	Data Type	Mandatory
`TargetEndPoint`	Target rule objects on which the ignore rules will be applied.	Array of string	Yes

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Request

PUT https://%3CNSM_IP%3E/sdkapi/domain/0/outboundsslexceptions/101

Payload

```
{ "state": "ENABLED", "name": "test2", "attack": null, "resource": [], "attacker": { "AttackerEndPoint":
[ "FireWall_IPv4_Dst_15_1_7_251" ] }, "target": { "TargetEndPoint": [ "FireWall_IPv4_Dst_15_1_7_251" ] },
"targetHostName": [], "targetUrlCategories": [ "Entertainment" ], "comment": "test" }
```

Response

```
{ “status”:1 }
```

Error Information

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal server error
2	400	1720	Invalid rule object/rule object is not visible in this domain
3	400	2513	Name must only contain letters, numerical, spaces,

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
			commas, periods, hyphen, or an underscore
4	400	1437	Rule name should not be longer than 64 characters
5	400	1433	This rule is invalid because it matches all alerts. Please specify at least one alert criterion.
6	400	1422	Resource is not visible in this domain
7	400	1001	Ignore Rule with the same name already exists
8	400	1435	The same combination of IPv4 and IPv6 should be used in the attacker and the target endpoints.
9	400	1408	The following URLs are invalid: <url_list>

Delete an Outbound Exception Rule

This URL deletes an outbound exception rule.

Resource URL

DELETE /domain/<domainId>/outboundsslexceptions/<ruleId>

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`domainId`	The idof the domain	Number	Yes
`ruleId`	The id of the rule	Number	Yes

Payload Request Parameters: None

Response Parameters

Following fields are returned if the request parameters are correct, otherwise error details are returned.

Field Name	Description	Data Type
`status`	Set to 1 if the operation was successful	Number

Example

Request

DELETE https://%3CNSM_IP%3E/sdkapi/domain/0/outboundsslexceptions/101

Error Information

Response

```
{ "status": 1 }
```

Following error codes are returned by this URL:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal server error
2	404	1408	Invalid rule id or provided rule id is not visible to this domain

Get Top Active Botnets

This URL retrieves the top active botnets.

Resource URL

GET /alerts/TopN/active_botnets >

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Query Parameters:

Field Name	Description	Data Type	Mandatory
`duration`	Indicates the start time for the alerts. The default value is LAST_14_DAYS. Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	No

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`TopActiveBotnetsList`	List of top active botnets	Array

Details of fields in TopActiveBotnetsList:

Field Name	Description	Data Type
Botnet	Name of the botnet	String
eventCount	The event count	Number

Example

Request

GET https://<NSM_IP>/sdkapi/alerts/TopN/active_botnets?duration=LAST_14_DAYS

Payload

None

Response

```
{ "TopActiveBotnetsList": [{ "botnet": "Carberp", "eventCount": 0 }, { "botnet": "Darkness", "eventCount": 0 },
{ "botnet": "Yzf", "eventCount": 0 }] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	3601	Invalid duration

Get Top Attack Applications

This URL retrieves the attack applications.

Resource URL

GET /alerts/TopN/attack_applications

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Query Parameters:

Field Name	Description	Data Type	Mandatory
`duration`	Indicates the start time for the alerts. The default value is LAST_14_DAYS. Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	No

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`TopAttackApplicationsList`	List of the top attack applications	Array

Details of fields in TopAttackApplicationsList:

Field Name	Description	Data Type
applicationName	The name of the application	String
attackCount	Count of the attack	Number

Example

Request

GET https://<NSM_IP>/sdkapi/alerts/TopN/attack_applications?duration=LAST_14_DAYS

Payload

None

Response

```
{ "TopAttackApplicationsList": [{ "applicationName": "PostgreSQL", "attackCount": 2 }] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	3601	Invalid duration

Get Top Attack Subcategories

This URL retrieves the top attack subcategories.

Resource URL

GET /alerts/TopN/attack_subcategories

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Query Parameters:

Field Name	Description	Data Type	Mandatory
duration	Indicates the start time for the alerts. The default value is LAST_14_DAYS. Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	No

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
TopAttackSubCategoriesList	List of top attack subcategories	Array

Details of fields in TopAttackSubCategoriesList:

Field Name	Description	Data Type
attackSubcategory	Subcategory of the attack	String
attackCount	Count of the attack	Number

Example

Request

GET https://<NSM_IP>/sdkapi/alerts/TopN/attack_subcategories?duration=LAST_14_DAYS

Payload

None

Response

```
{ "TopAttackSubCategoriesList": [{ "attackSubcategory":"restricted-application","attackCount":214910},
{"attackSubcategory":"protocol-violation","attackCount":151135}, {"attackSubcategory":"dos","attackCount":
99870}, {"attackSubcategory":"audit","attackCount":62959}, {"attackSubcategory":"write-exposure","attackCount":
40540}, {"attackSubcategory":"pup","attackCount":37059}, {"attackSubcategory":"botnet","attackCount":35194},
{"attackSubcategory":"privileged-access","attackCount":30411}, {"attackSubcategory":"code-
execution","attackCount":30263}, {"attackSubcategory":"buffer-overflow","attackCount":24166 }] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	3601	Invalid duration

Get Top Attacker Countries

This URL retrieves the countries of the top attackers.

Resource URL

GET /alerts/TopN/attacker_countries

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Query Parameters:

Field Name	Description	Data Type	Mandatory
`duration`	Indicates the start time for the alerts. The default value is LAST_14_DAYS. Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS	String	No

Field Name	Description	Data Type	Mandatory
	• LAST_7_DAYS • LAST_14_DAYS		

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`TopAttackerCountriesList`	List of the countries of the top attackers	Array

Details of fields in TopAttackerCountriesList:

Field Name	Description	Data Type
countryName	Name of the country	String
attackCount	Count of the attack	Number

Example

Request

GET https://<NSM_IP>/sdkapi/alerts/TopN/attacker_countries?duration=LAST_14_DAYS

Payload

None

Response

```
{ "TopAttackerCountriesList": [{ "countryName":"Japan","attackCount":231486.0}, {"countryName":"United
States","attackCount":126461.0}, {"countryName":"France","attackCount":48914.0},
{"countryName":"China","attackCount":29678.0}, {"countryName":"Australia","attackCount":25757.0},
{"countryName":"Bosnia and Herzegovina","attackCount":6395.0}, {"countryName":"Spain","attackCount":6276.0},
{"countryName":"Taiwan","attackCount":6107.0}, {"countryName":"Canada","attackCount":3204.0 }] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	3601	Invalid duration

Get Top Attackers

This URL retrieves the top attackers.

Resource URL

GET /alerts/TopN/attackers

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Query Parameters:

Field Name	Description	Data Type	Mandatory
`duration`	Indicates the start time for the alerts. The default value is LAST_14_DAYS. Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	No

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`TopAttackersList`	List of top attackers	Array

Details of fields in TopAttackersList:

Field Name	Description	Data Type
attackerIP	The attacker's IP address	String
DNSName	The DNS name	String
attackCount	Count of the attack	Number

Example

Request

GET https://<NSM_IP>/sdkapi/alerts/TopN/attackers?duration=LAST_14_DAYS

Payload

None

Response

```
{ {"TopAttackersList": [{"attackerIP":"88.174.38.117","DNSName":"loy01-1-88-174-38-117.fbx.proxad.net.",
"attackCount":35176},{"attackerIP":"172.16.230.71","DNSName":"---","attackCount":25852},
{"attackerIP":"1.1.1.9","DNSName":"---","attackCount":18876},
{"attackerIP":"172.16.195.37","DNSName":"---","attackCount":18354},
{"attackerIP":"133.35.136.9","DNSName":"nu-133-35-136-9.niigata-u.ac.jp.", "attackCount":14345},
{"attackerIP":"192.168.1.92","DNSName":"---","attackCount":12860},
{"attackerIP":"114.149.38.168","DNSName":"---","attackCount":11817},
{"attackerIP":"133.35.72.14","DNSName":"nu-133-35-072.14.niigata-u.ac.jp.", "attackCount":11065},
{"attackerIP":"2.2.88.8","DNSName":"---","attackCount":10337},
{"attackerIP":"134.154.168.205","DNSName":"---","attackCount":10105}]} }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
2	400	3601	Invalid duration

Get Top Attacks

This URL retrieves the top attacks.

Resource URL

GET /alerts/TopN/attacks

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Query Parameters:

Field Name	Description	Data Type	Mandatory
duration	Indicates the start time for the alerts. The default value is LAST_14_DAYS. Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	No

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
TopAttacksList	List of top attacks	Array

Details of fields in TopAttacksList:

Field Name	Description	Data Type
attackName	Name of the attack	String
attackCount	Count of the attack	Number

Example

Request

GET https://<NSM_IP>/sdkapi/alerts/TopN/attacks?duration=LAST_14_DAYS

Payload

None

Response

```
{ "TopAttacksList":[{"attackName":"NETBIOS-SS: Microsoft Windows SMB Client Race Condition
Vulnerability","attackCount":84637.0}, {"attackName":"HTTP: KeepAlive Request Detected","attackCount":62959.0},
{"attackName":"SSL: Client-Initiated Key Renegotiation Detected","attackCount":56981.0}, {"attackName":"P2P:
BitTorrent Meta-Info Retrieving","attackCount":52976.0}, {"attackName":"P2P: Ares/Warez-Gnutella Traffic
Detected","attackCount":52540.0}, {"attackName":"SSL: Server-Initiated Key Renegotiation
Detected","attackCount":41306.0}, {"attackName":"IPv4: TCP Session Hijacking Attempt Detected","attackCount":
40540.0}, {"attackName":"HTTP: Carberp Trojan Traffic Detected","attackCount":32008.0}, {"attackName":"P2P:
BitTorrent File Transfer HandShaking","attackCount":21072.0}, {"attackName":"HTTP: IIS root.exe Execute
Command","attackCount":20739.0}] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	3601	Invalid duration

Get Top Highrisk Hosts

This URL retrieves the top highrisk hosts.

Resource URL

GET /alerts/TopN/highrisk_hosts

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Query Parameters:

Field Name	Description	Data Type	Mandatory
duration	Indicates the start time for the alerts. The default value is LAST_14_DAYS. Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	No

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
TopHighRiskHostsList	List of top highrisk hosts	Array

Details of fields in TopHighRiskHostsList:

Field Name	Description	Data Type
hostIP	The host's IP address	String
hostRisk	The risk level of the host	Number
DNSName	The DNS name	String
RiskName	The risk's name	String

Example

Request

GET https://<NSM_IP>/sdkapi/alerts/TopN/highrisk_hosts?duration=LAST_14_DAYS

Payload

None

Response

```
{ "TopHighRiskHostsList":[] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	3601	Invalid duration

Get Top Malware Downloads

This URL retrieves the top malware downloads.

Resource URL

GET /alerts/TopN/malware_downloads

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Query Parameters:

Field Name	Description	Data Type	Mandatory
`duration`	Indicates the start time for the alerts. The default value is LAST_14_DAYS. Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS	String	No

Field Name	Description	Data Type	Mandatory
	- LAST_14_DAYS		

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`TopMalwareDownloadsList`	List of the top malware downloads	Array

Details of fields in TopMalwareDownloadsList:

Field Name	Description	Data Type
fileHash	The malware file hash	String
attackCount	Count of the attack	Number

Example

Request

GET https://<NSM_IP>/sdkapi/alerts/TopN/malware_downloads?duration=LAST_14_DAYS

Payload

None

Response

```
{ "TopMalwareDownloadsList":[] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	3601	Invalid duration

Get Top Target Countries

This URL retrieves the top countries that are targeted.

Resource URL

GET /alerts/TopN/target_countries

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Query Parameters:

Field Name	Description	Data Type	Mandatory
`duration`	Indicates the start time for the alerts. The default value is	String	No

Field Name	Description	Data Type	Mandatory
	LAST_14_DAYS. Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS		

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`TopTargetCountriesList`	List of top countries that are targeted	Array

Details of fields in TopTargetCountriesList:

Field Name	Description	Data Type
countryName	Name of the country	String
attackCount	Count of the attack	Number

Example

Request

GET https://<NSM_IP>/sdkapi/alerts/TopN/target_countries?duration=LAST_14_DAYS

Response

```
{ "TopTargetCountriesList": [{ "countryName":"Japan","attackCount":174039}, {"countryName":"United
States","attackCount":168318}, {"countryName":"China","attackCount":37652},
{"countryName":"Australia","attackCount":25651}, {"countryName":"India","attackCount":22705},
{"countryName":"Germany","attackCount":9211}, {"countryName":"Venezuela","attackCount":6884},
{"countryName":"Russia","attackCount":6720}, {"countryName":"Bosnia and Herzegovina","attackCount":6478},
{"countryName":"Netherlands","attackCount":6109 }] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	3601	Invalid duration

Get Top Targets

This URL retrieves the top targets.

Resource URL

GET /alerts/TopN/targets

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Query Parameters:

Field Name	Description	Data Type	Mandatory
`duration`	Indicates the start time for the alerts. The default value is LAST_14_DAYS. Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	No

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`TopTargetsList`	List of top targets	Array

Details of fields in TopTargetsList:

Field Name	Description	Data Type
targetIP	Target's IP address	String
DNSName	Name of the DNS	String
attackCount	Count of the attack	Number

Example

Request

GET https://<NSM_IP>/sdkapi/alerts/TopN/targets?duration=LAST_14_DAYS

Response

```
{  "TopTargetsList":[{"targetIP":"203.191.225.34","DNSName":"---","attackCount":36187},
{"targetIP":"192.168.3.2","DNSName":"---","attackCount":35780},{"targetIP":"203.191.225.54",
"DNSName":"---","attackCount":27252},{"targetIP":"203.191.225.56", "DNSName":"---","attackCount":24170},
{"targetIP":"203.191.225.50","DNSName":"---", "attackCount":18491},
{"targetIP":"1.1.1.10","DNSName":"---","attackCount":16578},
{"targetIP":"203.191.225.59","DNSName":"---","attackCount":15097},{"targetIP":"172.16.195.24",
"DNSName":"---","attackCount":14687},{"targetIP":"134.154.170.251","DNSName":"---", "attackCount":14556},
{"targetIP":"1.1.55.79","DNSName":"---","attackCount":13238}] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
2	400	3601	Invalid duration

Get Top Unblocked Malware Downloads

This URL retrieves the top unblocked malware downloads.

Resource URL

GET /alerts/TopN/unblocked_malware_downloads

Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
`duration`	Indicates the start time for the alerts. The default value is LAST_14_DAYS. Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	No

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`TopUnblockedMalwareDownloadsList`	List of top unblocked malware downloads	Array

Details of fields in TopUnblockedMalwareDownloadsList:

Field Name	Description	Data Type
fileHash	The malware file hash	String
attackCount	Count of the attack	Number

Example

Request

GET https://<NSM_IP>/sdkapi/alerts/TopN/unblocked_malware_downloads?duration=LAST_14_DAYS

Payload

None

Response

```
{ "TopUnblockedMalwareDownloadsList":[] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	3601	Invalid duration

Get Top Endpoint Executables

This URL retrieves the top endpoint executables.

Resource URL

GET /alerts/TopN/endpoint_executables

Request Parameters

URL Parameters: None

Payload Request Parameters: None

Query Parameters:

Field Name	Description	Data Type	Mandatory
`duration`	Indicates the start time for the alerts. The default value is LAST_14_DAYS. Duration can be: • LAST_5_MINUTES • LAST_1_HOUR • LAST_6_HOURS • LAST_12_HOURS • LAST_24_HOURS • LAST_48_HOURS • LAST_7_DAYS • LAST_14_DAYS	String	No
`counttype`	Allowed values are: • attackCount • endpointcount Default value is endpointcount.	String	No
`confidencetype`	Confidence type can be: • malwareConfAny • malwareConfHigh Default value is malwareConfHigh.	String	No
`classificationtype`	Allowed values are: • any • block	String	No

Field Name	Description	Data Type	Mandatory
	• allow • unclassified Default value is any.		

Response Parameters

Following fields are returned.

Field Name	Description	Data Type
`TopEndExecutablesList`	List of the top endpoint executables	Array

Details of fields in TopEndpointExecutablesList:

Field Name	Description	Data Type
name	Executable name	String
fileHash	File hash	String
count	Endpoint count	Number

Example

Request

GET https://<NSM_IP>/sdkapi/alerts/TopN/endpoint_executables?duration=LAST_14_DAYS

Response

None

Response

```
{ "TopEndpointExecutablesList":[] }
```

Error Information

Following error codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	3601	Invalid duration

HTTP Error Codes Reference

S.No	HTTP Error Code	HTTP Error Message
1	400	Bad request
2	404	Not found
3	409	Conflict
4	500	Internal server error

COPYRIGHT