



Revision A

# McAfee Network Security Platform 10.1

(Manager API Reference Guide)

## **COPYRIGHT**

Copyright © 2019 McAfee, LLC

## **TRADEMARK ATTRIBUTIONS**

McAfee and the McAfee logo, McAfee Active Protection, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundstone, McAfee LiveSafe, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, True Key, TrustedSource, VirusScan are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

## **LICENSE INFORMATION**

### **License Agreement**

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

# Contents

	<b>Preface</b>	<b>19</b>
	About this guide . . . . .	19
	Audience . . . . .	19
	Conventions . . . . .	19
	What's in this guide . . . . .	20
	Find product documentation . . . . .	20
<b>1</b>	<b>Overview</b>	<b>21</b>
	SDK API access . . . . .	21
	SDK Authentication/Validation . . . . .	26
	Version Support . . . . .	26
<b>2</b>	<b>Resources</b>	<b>29</b>
	Session . . . . .	31
	Heartbeat . . . . .	31
	Domain . . . . .	31
	Dashboard Monitors . . . . .	31
	Sensor . . . . .	32
	Interface . . . . .	33
	Port . . . . .	34
	Attacks . . . . .	34
	IPS Policies . . . . .	34
	Attack Filters . . . . .	34
	Rule Objects . . . . .	35
	Firewall Policies . . . . .	36
	Scanning Exception . . . . .	36
	IPS Quarantine . . . . .	37
	Connection Limiting Policies . . . . .	37
	Non Standard Ports . . . . .	38
	SSL Key . . . . .	38
	Rate Limiting Profiles . . . . .	39
	QoS Policy . . . . .	40
	Advanced Malware Policy . . . . .	40
	File Reputation . . . . .	41
	Alert Relevance . . . . .	41
	Manage Import . . . . .	41
	Malware Archive . . . . .	42
	Passive Device Profiling . . . . .	42
	Alert Exception . . . . .	42
	Global Auto Acknowledgment . . . . .	42
	Name Resolution Resource . . . . .	43
	Device Resource . . . . .	43
	NTBA Monitors . . . . .	43
	Endpoint Executables Resource . . . . .	46
	NMS IP Resource . . . . .	46

NMS Users Resource . . . . .	46
Policy Export Import Resource . . . . .	47
TCP Settings Resource . . . . .	47
IP Settings Resource . . . . .	48
Firewall Logging Resource . . . . .	48
IPS Alerting Resource . . . . .	48
Failover Resource . . . . .	48
Syslog Firewall Resource . . . . .	48
Syslog Faults Notification Resource . . . . .	49
Tacacs Resource . . . . .	49
Active Botnets Resource . . . . .	49
Automatic Update Configuration Resource . . . . .	49
Malware Downloads Resource . . . . .	50
Nessus scan report Resource . . . . .	50
ATD Configuration Resource . . . . .	50
Sensor Configuration Export Import Resource . . . . .	50
Denial Of Services Resource . . . . .	51
Domain Name Exceptions Resource . . . . .	51
EPO Integration Resource . . . . .	51
Packet Capture Resource . . . . .	52
Policy Group Resource . . . . .	52
Policy Assignments Resource . . . . .	52
Ignore Rules/NTBA Ignore Rules . . . . .	53
Inspection Options Policy Resource . . . . .	53
DXL Integration Resource . . . . .	53
Threat Explorer Resource . . . . .	54
Network forensics . . . . .	55
Gateway Anti-Malware Engine Update Resource . . . . .	56
Users . . . . .	56
Alert Pruning . . . . .	56
Custom Role . . . . .	56
Direct Syslog Resource . . . . .	56
Radius Resource . . . . .	57
Advanced Device Configuration Resource . . . . .	57
Attack Log Rest API . . . . .	58
Traffic Statistics . . . . .	58
CLI Auditing Resource . . . . .	59
Diagnostics Trace Resource . . . . .	59
Health Check Resource . . . . .	59
McAfee Cloud Integration Resource . . . . .	59
Performance Monitoring Resource . . . . .	60
Attack Set Profile . . . . .	60
Proxy Server . . . . .	60
Cloud Resource . . . . .	61
Quarantine Zone Resource . . . . .	62
GTI and Telemetry Resource . . . . .	62
License Resource . . . . .	62
IPS Inspection Whitelist Resource . . . . .	63
SSL Exception Rules . . . . .	63
<b>3 Error Information</b>	<b>65</b>
<b>4 Session Resource</b>	<b>67</b>
Login . . . . .	67
Logout . . . . .	68

<b>5</b>	<b>Heartbeat Resource</b>	<b>69</b>
	Get Manager availability Information . . . . .	69
<b>6</b>	<b>Domain Resource</b>	<b>71</b>
	Create a new Domain . . . . .	71
	Update a Domain . . . . .	73
	Get a Domain . . . . .	76
	Delete a Domain . . . . .	78
	Get Default Recon Policies . . . . .	79
	Get All Admin Domains . . . . .	80
	Get All Child Domains in a Admin Domain . . . . .	81
<b>7</b>	<b>Sensor Resource</b>	<b>83</b>
	Get all Sensors in a Domain . . . . .	83
	Get Sensor Details . . . . .	85
	Update Sensor Configuration . . . . .	95
	Get Configuration Update Status . . . . .	97
	Is Sensor Config Modified . . . . .	98
	Get Sensor Performance Stats . . . . .	99
	Reboot Sensor . . . . .	101
	Set IPv6 . . . . .	102
	Get IPv6 Setting . . . . .	103
	Get Sensor Status . . . . .	104
	Get Application Identification . . . . .	104
	Update Application Identification . . . . .	105
	Get NTBA Integration Configuration . . . . .	106
	Update NTBA Integration Configuration . . . . .	108
	Get Device Softwares Deployed and Available . . . . .	109
	Upgrade the Software on Device . . . . .	110
	Get the Upgrade Software Status . . . . .	111
<b>8</b>	<b>Interface Resource</b>	<b>113</b>
	Get Interface/Sub Interface details . . . . .	113
	Update Interface/Sub Interface details . . . . .	115
	Add Sub Interface . . . . .	118
	Delete a Sub Interface . . . . .	120
	Add/Assign VLAN . . . . .	121
	Delete/revoke VLAN . . . . .	123
	Get available interfaces to allocate . . . . .	124
	Get list of interfaces allocated to a sensor inside a domain . . . . .	127
	Get list of CIDR allocated to an interface . . . . .	128
	Allocate an interface to a sensor in child domain . . . . .	129
	Delete/Revoke an interface from a sensor in child domain . . . . .	130
	Adds/Assign CIDR . . . . .	131
	Delete CIDR . . . . .	132
<b>9</b>	<b>Port Resource</b>	<b>135</b>
	Get Port Configuration Details . . . . .	135
<b>10</b>	<b>Attack Resource</b>	<b>137</b>
	Get all Attacks . . . . .	137
	Get Attack Details . . . . .	138
<b>11</b>	<b>IPS Policies Resource</b>	<b>141</b>
	Get IPS Policies in a domain . . . . .	141
	Get IPS Policy details . . . . .	143

	Create/Update Light Weight Policy . . . . .	149
	Get Light Weight Policy details . . . . .	158
	Delete Light Weight Policy . . . . .	166
	Create new IPS Policy . . . . .	167
	Update IPS policy . . . . .	168
	Delete IPS Policy . . . . .	177
<b>12</b>	<b>Attack Filters Resource</b>	<b>179</b>
	Add a new Attack Filter . . . . .	179
	Update Attack Filter . . . . .	181
	Delete Attack Filter . . . . .	184
	Get a Attack Filter . . . . .	185
	Get Attack Filters defined in a domain . . . . .	187
	Assign a Attack Filter to a domain and attack . . . . .	188
	Get Attack Filters assigned to a domain and attack . . . . .	189
	Unassign Attack Filters assigned to a domain and attack . . . . .	190
	Assign a Attack Filter to a sensor and attack . . . . .	191
	Get Attack Filters assigned to a sensor and attack . . . . .	193
	Unassign Attack Filter to a sensor and attack . . . . .	194
	Assign a Attack Filter to an Interface/SubInterface and attack . . . . .	195
	Get Attack Filters assigned to an Interface/SubInterface and attack . . . . .	197
	Unassign Attack Filters to an Interface/SubInterface . . . . .	198
	Get Attack Filters assignments . . . . .	199
<b>13</b>	<b>Rule Objects Resource</b>	<b>201</b>
	Add Rule Object . . . . .	201
	Update Rule Object . . . . .	206
	Delete Rule Object . . . . .	211
	Get Rule Object . . . . .	212
	Get Rule Object Associations . . . . .	216
	Get Rule Objects in a Domain . . . . .	217
	Get User Rule Objects . . . . .	224
	Get User Group . . . . .	226
<b>14</b>	<b>Firewall Policies Resource</b>	<b>229</b>
	Add Firewall Policy . . . . .	229
	Update Firewall Policy . . . . .	234
	Delete Firewall Policy . . . . .	238
	Get Firewall Policy . . . . .	239
	Get Firewall Policies in a Domain . . . . .	242
<b>15</b>	<b>Scanning Exception Resource</b>	<b>245</b>
	Create a new Scanning Exception at sensor . . . . .	245
	Get Scanning Exception details on a sensor . . . . .	248
	Delete Scanning Exception on a sensor . . . . .	250
	Enable/Disable Scanning Exception on a sensor . . . . .	251
	Get Scanning Exception status on a sensor . . . . .	252
<b>16</b>	<b>IPS Quarantine Resource</b>	<b>255</b>
	Quarantine Host . . . . .	255
	Update IPS Quarantine duration for a Host . . . . .	256
	Release Quarantined Host . . . . .	257
	Get Quarantined Hosts . . . . .	258
	Get Quarantined Host Details . . . . .	259

<b>17</b>	<b>Connection Limiting Policies Resource</b>	<b>261</b>
	Add a new connection limiting policy . . . . .	261
	Update a connection limiting policy . . . . .	263
	Get a connection limiting policy . . . . .	266
	Delete a connection limiting policy . . . . .	268
	Get the list of available country . . . . .	268
	Get Connection Limiting Policies in a domain . . . . .	272
<b>18</b>	<b>Non Standard Ports Resource</b>	<b>275</b>
	Add a Non Standard Port at Domain level . . . . .	275
	Add a Non Standard Port at Sensor level . . . . .	276
	Get Non Standard Ports at Domain level . . . . .	278
	Get Non Standard Ports at Sensor level . . . . .	279
	Delete a Non Standard Port at Domain level . . . . .	280
	Delete a Non Standard Port at Sensor level . . . . .	281
<b>19</b>	<b>SSL Key Resource</b>	<b>283</b>
	Import SSL Key to the Manager . . . . .	283
	Delete SSL Key . . . . .	285
	Get SSL Keys . . . . .	286
	Get the SSL configuration . . . . .	287
	Update the SSL configuration . . . . .	288
	Get the SSL configuration at the domain level . . . . .	289
	Update the SSL configuration at the domain level . . . . .	291
	Get the Resign Certificates on the Manager . . . . .	293
	Regenerate the default re-sign certificate . . . . .	294
	Export the public key of the active re-sign certificate . . . . .	295
	Import a custom re-sign certificate . . . . .	296
	Get all the trusted CA certificates on the Manager . . . . .	297
	Get a single trusted CA certificate on the Manager . . . . .	299
	Enable or Disable multiple trusted CA certificates . . . . .	300
	Update the default trusted CA certificates . . . . .	301
	Import a custom trusted CA certificate . . . . .	302
	Delete multiple trusted CA certificates . . . . .	303
	Get all the internal Web Server certificates . . . . .	304
	Import custom internal Web Server certificate . . . . .	306
	Delete multiple internal Web Server certificates . . . . .	308
	Get all Inbound Proxy Rules . . . . .	309
	Get Inbound Proxy Rule Details . . . . .	310
	Add Inbound Proxy Rule . . . . .	311
	Update Inbound Proxy Rule . . . . .	313
	Delete multiple Inbound Proxy Rules . . . . .	314
	Get the SSL configuration at the Sensor level . . . . .	315
	Update the SSL configuration at the Sensor level . . . . .	317
<b>20</b>	<b>Rate Limiting Profiles Resource</b>	<b>321</b>
	Add Rate Limiting Profile . . . . .	321
	Update Rate Limiting Profile . . . . .	323
	Delete Rate Limiting Profile . . . . .	326
	Get Rate Limiting Profile . . . . .	326
	Get Rate Limiting Profiles in a Domain . . . . .	328
<b>21</b>	<b>QoS Policy Resource</b>	<b>331</b>
	Add QoS Policy . . . . .	331
	Update QoS Policy . . . . .	336
	Delete QoS Policy . . . . .	342

	Get QoS Policy . . . . .	343
	Get QoS Policies in a Domain . . . . .	347
<b>22</b>	<b>Advanced Malware Policy Resource</b>	<b>349</b>
	Add Advanced Malware Policy . . . . .	349
	Update Malware Policy . . . . .	355
	Delete Malware Policy . . . . .	360
	Get Malware Policy . . . . .	361
	Get Malware Policies in a Domain . . . . .	365
	Get Default Protocol List . . . . .	367
	Get Default Scanning Option Configuration List . . . . .	367
	Get Blacklisted Hashes . . . . .	370
	Get Whitelisted Hashes . . . . .	372
	Action on Blacklisted Hash . . . . .	372
	Action on Whitelisted Hash . . . . .	373
	Action on Multiple Blacklisted Hashes . . . . .	374
	Action on Multiple Whitelisted Hashes . . . . .	375
	Remove All Blacklisted Hashes . . . . .	376
	Remove All Whitelisted Hash . . . . .	377
	Add FileHash to Blacklist or Whitelist . . . . .	377
	Update Details of file hash . . . . .	379
	Delete some file hashes from Blacklist or Whitelist . . . . .	380
<b>23</b>	<b>File Reputation Resource</b>	<b>383</b>
	Import GTI Configuration . . . . .	383
	Import Whitelisted Fingerprints . . . . .	384
	Delete Whitelisted Fingerprints . . . . .	385
	Import Custom Fingerprints . . . . .	386
	Delete Custom Fingerprints . . . . .	387
	Manage Blacklist File Types . . . . .	388
	Number of Fingerprints in use . . . . .	390
	Get Blacklist File Types . . . . .	391
	Get GTI File Types . . . . .	393
	Get Severity for GTI . . . . .	394
<b>24</b>	<b>Alert Relevance Resource</b>	<b>395</b>
	Update Alert Relevance . . . . .	395
	Get Alert Relevance . . . . .	396
<b>25</b>	<b>Manage Import Resource</b>	<b>397</b>
	Automatic Botnet File Download to Manager . . . . .	397
	Manual Botnet File Import to Manager . . . . .	398
	Manual Signature Set Import to Manager . . . . .	399
	Manual Device Software Import to Manager . . . . .	401
	Get the Device Softwares Available in the Server . . . . .	402
	Manual Gateway Anti-Malware File Import to Manager . . . . .	404
	Download the Device Software from the Server . . . . .	405
	Get all the Device Software Available in the Server . . . . .	406
<b>26</b>	<b>IP Reputation Resource</b>	<b>409</b>
	Update IP Reputation setting at Domain Level . . . . .	409
	Get IP Reputation setting at Domain Level . . . . .	411
<b>27</b>	<b>Malware Archive Resource</b>	<b>415</b>
	Whitelist Malware Archive File . . . . .	415
	Download Malware File . . . . .	416



	Get List of Archived Malware Files . . . . .	417
	Delete Malware Archive File . . . . .	418
<b>28</b>	<b>Passive Device Profiling</b>	<b>421</b>
	Get Passive Device Profiling setting at the domain level . . . . .	421
	Update Passive Device Profiling setting at domain level . . . . .	422
	Get Passive Device Profiling setting at sensor level . . . . .	424
	Update Passive Device Profiling setting at sensor level . . . . .	427
<b>29</b>	<b>Alert Exception</b>	<b>431</b>
	Add Alert Exception . . . . .	431
	Get Alert Exception . . . . .	432
	Get All Alert Exception . . . . .	433
	Delete Alert Exception . . . . .	434
<b>30</b>	<b>Global Auto Acknowledgment</b>	<b>437</b>
	Configure Global Auto Ack Setting . . . . .	437
	Get Global Auto Ack Setting . . . . .	438
	Get attacks for rules configuration . . . . .	439
	Get Global Auto Ack Rules . . . . .	440
	Get Global Auto Ack Rule . . . . .	441
	Create Global Auto Ack Rules . . . . .	442
	Update Global Auto Ack Rules . . . . .	443
<b>31</b>	<b>Name Resolution Resource</b>	<b>445</b>
	Update Name Resolution settings at domain level . . . . .	445
	Get Name Resolution Configuration at Domain level . . . . .	446
	Update Name Resolution settings at sensor level . . . . .	447
	Get Name Resolution Configuration at Sensor level . . . . .	449
<b>32</b>	<b>Device Resource</b>	<b>451</b>
	Add Device . . . . .	451
	Get Device . . . . .	453
	Update Device . . . . .	455
	Delete Device . . . . .	457
	Get All Device . . . . .	458
<b>33</b>	<b>NTBA Resource</b>	<b>461</b>
	Get NTBA Monitors . . . . .	461
	Get Hosts Threat Factor . . . . .	462
	Get Top URLs . . . . .	464
	Get Top Zone URLs . . . . .	465
	Get Top Host URLs . . . . .	467
	Get Top URLs by Reputations . . . . .	468
	Get URL Activity . . . . .	470
	Get URLs by Category . . . . .	471
	Get URLs for Category . . . . .	473
	Get Top files . . . . .	474
	Get Top zone files . . . . .	476
	Get Top Host files . . . . .	477
	Get File Activity . . . . .	477
	Get External Hosts by Reputation . . . . .	478
	Get New Hosts . . . . .	480
	Get Active Hosts . . . . .	481
	Get Top Hosts Traffic . . . . .	482
	Get Application Traffic . . . . .	484

	Get Application Profile . . . . .	485
	Get Throughput Traffic . . . . .	486
	Get Bandwidth Utilization . . . . .	488
	Get Zone Traffic . . . . .	489
	Get Active Services . . . . .	490
	Get Host Active Services . . . . .	492
	Get New Services . . . . .	493
	Get Active Applications . . . . .	494
	Get New Applications . . . . .	496
	Get Host Active Applications . . . . .	497
	Get Host Ports . . . . .	498
<b>34</b>	<b>Endpoint Executables Resource</b>	<b>501</b>
	Get Endpoint Intelligence . . . . .	501
	Get Executable Information . . . . .	503
	Get Endpoints . . . . .	505
	Get Applications . . . . .	506
	Get Events . . . . .	507
	Action on Hash . . . . .	509
<b>35</b>	<b>NMS IP Resource</b>	<b>511</b>
	Get NMS IPs at Domain . . . . .	511
	Create NMS IP at Domain . . . . .	512
	Delete the NMS IP at Domain . . . . .	514
	Get NMS IPs at Sensor . . . . .	515
	Get available NMS IPs at Sensor . . . . .	516
	Create NMS IP at Sensor . . . . .	517
	Allocate NMS IP to Sensor . . . . .	518
	Delete the NMS IP at Sensor . . . . .	519
<b>36</b>	<b>NMS Users Resource</b>	<b>523</b>
	Get NMS Users at Domain . . . . .	523
	Create NMS User at Domain . . . . .	524
	Update NMS User at Domain . . . . .	526
	Get the NMS User Details at Domain . . . . .	527
	Delete the NMS User at Domain . . . . .	528
	Get NMS Users at Sensor . . . . .	529
	Get available NMS Users at Sensor . . . . .	530
	Create NMS User at Sensor . . . . .	532
	Allocate NMS User to Sensor . . . . .	533
	Update NMS User at Sensor . . . . .	534
	Get the NMS User Details at Sensor . . . . .	536
	Delete the NMS User at Sensor . . . . .	537
<b>37</b>	<b>Policy Export Import Resource</b>	<b>539</b>
	Get the list of importable IPS and Reconnaissance policies . . . . .	539
	Import the IPS and Reconnaissance policies . . . . .	542
	Import the Malware policies . . . . .	544
	Import the Firewall policies . . . . .	546
	Import the Exceptions . . . . .	548
	Gets the exportable IPS Reconnaissance policies from the Manager . . . . .	550
	Export the IPS Reconnaissance policies . . . . .	551
	Gets the exportable Malware policies from the Manager . . . . .	553
	Export the Malware policies . . . . .	554
	Gets the exportable Firewall policies from the Manager . . . . .	556
	Export the Firewall policies . . . . .	557

	Gets the exportable Exceptions from the Manager . . . . .	559
	Export the Exceptions . . . . .	560
<b>38</b>	<b>TCP Settings</b>	<b>563</b>
	Get TCP Settings Configuration at Sensor level . . . . .	563
	Update the TCP Settings on Sensor . . . . .	565
<b>39</b>	<b>IP Settings</b>	<b>569</b>
	Update IP Settings Configuration at Sensor level . . . . .	569
	Get IP Settings Configuration at Sensor level . . . . .	571
<b>40</b>	<b>Firewall Logging Resource</b>	<b>575</b>
	Update the Firewall Logging . . . . .	575
	Get the Firewall Logging . . . . .	576
<b>41</b>	<b>IPS Alerting Resource</b>	<b>579</b>
	Get the Alert Suppression . . . . .	579
	Update the Alert Suppression . . . . .	580
<b>42</b>	<b>Failover Resource</b>	<b>583</b>
	Add Failover . . . . .	583
	Get the Failover Pair . . . . .	585
	Get the Failover Pair list . . . . .	586
<b>43</b>	<b>Syslog Firewall Notification Resource</b>	<b>589</b>
	Get Syslog Configuration . . . . .	589
	Create/Update Syslog Configuration . . . . .	590
<b>44</b>	<b>Syslog Faults Notification Resource</b>	<b>593</b>
	Get Syslog Configuration . . . . .	593
	Create/Update Syslog Configuration . . . . .	594
<b>45</b>	<b>Tacacs Resource</b>	<b>597</b>
	Get Tacacs on Domain . . . . .	597
	Update Tacacs on Domain . . . . .	598
	Get Tacacs on Sensor . . . . .	599
	Update Tacacs on Sensor . . . . .	600
<b>46</b>	<b>Active Botnets Resource</b>	<b>603</b>
	Get the list of active botnets . . . . .	603
	Get the List of zombies for an active botnet . . . . .	604
<b>47</b>	<b>Automatic Update Configuration Resource</b>	<b>607</b>
	Get the Signature Set Automatic Update Configuration . . . . .	607
	Get the Botnet Automatic Update Configuration . . . . .	608
	Update the Signature Set Automatic Download Configuration . . . . .	610
	Update the Botnet Automatic Download Configuration . . . . .	611
	Update the Signature Set Automatic Deployment Configuration . . . . .	613
	Update the Botnet Automatic Deployment Configuration . . . . .	614
<b>48</b>	<b>Malware Downloads Resource</b>	<b>617</b>
	Get Malware Downloads . . . . .	617
	Get Malware Alerts . . . . .	619
<b>49</b>	<b>Nessus Scan Report Resource</b>	<b>623</b>
	Nessus Scan Report Import . . . . .	623

<b>50</b>	<b>ATD Configuration Resource</b>	<b>625</b>
	Get ATD Integration in Domain . . . . .	625
	Update ATD Integration Configuration in Domain . . . . .	626
	Get ATD Integration in sensor . . . . .	627
	Update ATD Integration Configuration in Sensor . . . . .	628
<b>51</b>	<b>Sensor Configuration Export Import Resource</b>	<b>631</b>
	Export the Sensor Configuration . . . . .	631
	Import the Sensor Configuration . . . . .	632
<b>52</b>	<b>Denial Of Service Resource</b>	<b>635</b>
	Get the DoS profiles on the manager for Sensors . . . . .	635
	Update the DoS learning mode on the Sensor . . . . .	636
	Get the DoS packet forwarding . . . . .	637
	Upload the DoS Profile from the Sensor . . . . .	638
	Restore the DoS Profile to the Sensor . . . . .	638
	Delete the DoS Profile . . . . .	640
	Export the DoS Profile to the Manager client . . . . .	641
<b>53</b>	<b>Domain Name Exceptions Resource</b>	<b>643</b>
	Get the Domain Name Exceptions from the Manager . . . . .	643
	Import the Domain Name Exceptions to the Manager . . . . .	644
	Export the Domain Name Exceptions from the Manager . . . . .	645
	Update a Domain Name exception's comment . . . . .	646
	Delete some Domain Name Exceptions . . . . .	647
	Delete all Domain Name Exceptions . . . . .	648
	Add domain name to callback detector whitelist . . . . .	649
	Update the details of Domain Name Exception . . . . .	650
<b>54</b>	<b>Direct Syslog Resource</b>	<b>653</b>
	Get the Direct Syslog Configuration for the domain . . . . .	653
	Update the Direct Syslog Configuration for the domain . . . . .	655
	Get the Direct Syslog Configuration for the Sensor . . . . .	659
	Update the Direct Syslog Configuration for the Sensor . . . . .	661
	Test the Direct Syslog Configuration for domain . . . . .	664
	Test the Direct Syslog Configuration for the Sensor . . . . .	668
<b>55</b>	<b>Packet Capture Resource</b>	<b>673</b>
	Get the packet capture settings . . . . .	673
	Update the packet capture settings . . . . .	676
	Update the packet capturing status . . . . .	679
	Get the list/a particular rule template . . . . .	680
	Add a packet capture rule template . . . . .	682
	Get the list of PCAP files captured . . . . .	684
	Export the PCAP file captured . . . . .	685
	Delete the PCAP file captured . . . . .	686
	Get the list/a particular rule template . . . . .	687
	Add a packet capture rule template . . . . .	688
	Update a packet capture rule template . . . . .	690
	Delete a packet capture rule template . . . . .	692
<b>56</b>	<b>Policy Group Resource</b>	<b>695</b>
	Get All Policy Group . . . . .	695
	Create Policy Group . . . . .	696
	Get Policy Group . . . . .	697
	Update Policy Group . . . . .	699

	Delete Policy Group . . . . .	700
<b>57</b>	<b>Policy Assignments Resource</b>	<b>703</b>
	Get All Policy Assignments Interface . . . . .	703
	Get Policy Assignments Interface . . . . .	704
	Get All Policy Assignments Device . . . . .	706
	Get Policy Assignments Device . . . . .	707
	Update Policy Assignments Interface . . . . .	708
	Update Policy Assignments Device . . . . .	709
<b>58</b>	<b>Ignore Rules/NTBA Ignore Rules</b>	<b>711</b>
	Get the Ignore Rules . . . . .	711
	Create an Ignore Rule . . . . .	715
	Update an Ignore Rule . . . . .	719
	Delete an Ignore Rule . . . . .	724
<b>59</b>	<b>Inspection Options policy resource</b>	<b>727</b>
	Get all Inspection Options policy . . . . .	727
	Get Inspection Options policy . . . . .	728
	Create Inspection Options policy . . . . .	732
	Update Inspection Options policy . . . . .	736
	Delete Inspection Options policy . . . . .	740
<b>60</b>	<b>DXL Integration Resource</b>	<b>741</b>
	Get the DXL Integration Configuration for domain . . . . .	741
	Update the DXL Integration Configuration for domain . . . . .	742
	Get the DXL Integration Configuration for Sensor . . . . .	743
	Update the DXL Integration Configuration for Sensor . . . . .	744
<b>61</b>	<b>Threat Explorer Resource</b>	<b>747</b>
	Get the Threat explorer data . . . . .	747
	Get the List of top attackers . . . . .	751
	Get the List of top attacks . . . . .	754
	Get the List of top targets . . . . .	757
	Get the List of top attack applications . . . . .	760
	Get the List of top malwares . . . . .	763
	Get the list of top executables . . . . .	766
<b>62</b>	<b>Network Forensics</b>	<b>771</b>
	Get Host Summary . . . . .	771
	Get Top Suspicious Flows . . . . .	773
<b>63</b>	<b>Gateway Anti-Malware Update Resource</b>	<b>777</b>
	Get the Gateway Anti-Malware Updating Configuration for domain . . . . .	777
	Update the Gateway Anti-Malware Updating Configuration for domain . . . . .	778
	Get the Gateway Anti-Malware Updating Configuration for sensor . . . . .	779
	Update the Gateway Anti-Malwares Updating Configuration for sensor . . . . .	780
<b>64</b>	<b>User Resource</b>	<b>783</b>
	Get the User Details . . . . .	783
	Create a user . . . . .	785
	Update a User . . . . .	787
	Delete a User . . . . .	790
<b>65</b>	<b>Alert Pruning Resource</b>	<b>793</b>
	Configure Alert Pruning settings . . . . .	793

<b>66</b>	<b>Custom Role Resource</b>	<b>795</b>
	Get the Details of Custom roles . . . . .	795
	Create a Role . . . . .	796
	Delete a Role . . . . .	798
<b>67</b>	<b>Direct Syslog Resource</b>	<b>799</b>
	Get the Direct Syslog Configuration for the domain . . . . .	799
	Update the Direct Syslog Configuration for the domain . . . . .	801
	Get the Direct Syslog Configuration for the Sensor . . . . .	805
	Update the Direct Syslog Configuration for the Sensor . . . . .	807
	Test the Direct Syslog Configuration for domain . . . . .	810
	Test the Direct Syslog Configuration for the Sensor . . . . .	814
<b>68</b>	<b>Radius Resource</b>	<b>819</b>
	Get the Radius Configuration for domain . . . . .	819
	Update the Radius Configuration for the domain . . . . .	820
<b>69</b>	<b>Advanced Device Configuration Resource</b>	<b>823</b>
	Get the Advanced Device Configuration at domain level . . . . .	823
	Update the Advanced Device Configuration at domain level . . . . .	825
	Get the Advanced Device Configuration at Sensor level . . . . .	827
	Update the Advanced Device Configuration at Sensor level . . . . .	829
<b>70</b>	<b>Attack Log Resource</b>	<b>833</b>
	Get All Alerts . . . . .	833
	Delete All Alerts . . . . .	838
	Update All Alerts . . . . .	839
	Get Alert Details . . . . .	840
	Update Alert Details . . . . .	843
	Delete Alert . . . . .	844
	Get Component Alert Packet Log . . . . .	845
	Get Packet Capture of an Alert . . . . .	846
<b>71</b>	<b>Traffic Statistics</b>	<b>849</b>
	Get the Traffic Send/Received statistics . . . . .	849
	Get the Flows statistics . . . . .	850
	Get dropped packets statistics . . . . .	852
	Get Malware stats grouped by engine . . . . .	854
	Get Malware stats grouped by file type . . . . .	856
	Get traffic statistics for Advance callback detection . . . . .	857
	Get the traffic statistics for the SSL . . . . .	858
	Get the traffic statistics for internal web certificate matches . . . . .	859
	Reset SSL counters . . . . .	860
<b>72</b>	<b>CLI Auditing Resource</b>	<b>861</b>
	Get the CLI Auditing Configuration at the domain level . . . . .	861
	Update the CLI Auditing Configuration at domain level . . . . .	862
	Get the CLI Auditing Configuration at Sensor level . . . . .	863
	Update the CLI Auditing Configuration at the Sensor level . . . . .	864
<b>73</b>	<b>Diagnostics Trace Resource</b>	<b>865</b>
	Get the diagnostic trace files . . . . .	865
	Upload the diagnostic trace file . . . . .	866
	Get the upload status . . . . .	867
	Export the Diagnostic Trace file captured . . . . .	868
	Delete the Diagnostic Trace file captured . . . . .	869

<b>74</b>	<b>Health Check Resource</b>	<b>871</b>
	Get the Health Check . . . . .	871
	Run the Health Check . . . . .	872
<b>75</b>	<b>McAfee Cloud Integration Resource</b>	<b>875</b>
	Get the McAfee Cloud integration settings . . . . .	875
	Update the McAfee Cloud Integration Settings . . . . .	876
	Test the connection for McAfee Cloud integration settings . . . . .	877
	Get the McAfee Cloud Statistics . . . . .	878
	Reset McAfee cloud statistics . . . . .	879
<b>76</b>	<b>Performance Monitoring Resource</b>	<b>881</b>
	Get the Performance Monitoring settings at the domain level . . . . .	881
	Update the performance monitoring settings at the domain level . . . . .	884
	Get the Performance monitoring settings at the Sensor level . . . . .	887
	Update the Performance monitoring settings at the Sensor level . . . . .	889
<b>77</b>	<b>Attack Set Profile</b>	<b>893</b>
	Get attack set profile configuration details at domain level . . . . .	893
	Get attack set profile configuration details using Policy ID at domain level . . . . .	895
	Create new attack set profile at domain level . . . . .	897
	Update attack set profile configuration detail . . . . .	899
	Delete attack set profile . . . . .	901
<b>78</b>	<b>Proxy Server</b>	<b>903</b>
	Get the proxy server configuration at domain level . . . . .	903
	Update Proxy Server configuration . . . . .	904
	Get the proxy server configuration at device level . . . . .	905
	Update the proxy server configuration at device level . . . . .	906
	Get the proxy server configuration at the Manager level . . . . .	907
	Update the proxy server configuration at the Manager level . . . . .	908
<b>79</b>	<b>Cloud Resource</b>	<b>911</b>
	Get the Cluster ID based on name . . . . .	911
	Get the Controller ID based on name . . . . .	912
	Get the Virtual Probe status . . . . .	913
	Get the vNSP Controllers present in the domain . . . . .	914
	Create the vNSP Controller . . . . .	917
	Get the vNSP Controller details . . . . .	919
	Test Manager-Controller connection . . . . .	922
	Test Manager-Controller Cloud connection . . . . .	923
	Update the vNSP Controller . . . . .	924
	Delete the vNSP Controller . . . . .	926
	Upgrade the vNSP Controller software . . . . .	927
	Get the vNSP Clusters present in the domain . . . . .	928
	Create the vNSP Cluster . . . . .	930
	Get the vNSP Cluster details . . . . .	931
	Update the vNSP Cluster . . . . .	932
	Delete the vNSP Cluster . . . . .	933
	Get the Protected VM Groups present in the vNSP Cluster . . . . .	934
	Create the Protected VM Group under vNSP Cluster . . . . .	936
	Get the Protected VM Group details . . . . .	937
	Update the Protected VM Group . . . . .	939
	Delete the Protected VM Group . . . . .	940
	Download the Cluster Virtual Probe agent . . . . .	941
	Download the Cluster probe agent without login . . . . .	942

	Update the vNSP Cluster agent . . . . .	943
	Get the list of Protected VM Hosts . . . . .	944
<b>80</b>	<b>Quarantine zone resource</b>	<b>947</b>
	Get quarantine zone Details using QuarantineZone ID at domain level . . . . .	947
	Get all quarantine zones at domain level . . . . .	949
	Update quarantine zone . . . . .	952
	Add quarantine zone . . . . .	954
	Delete quarantine zone . . . . .	956
<b>81</b>	<b>GTI and Telemetry Resource</b>	<b>959</b>
	Get the GTI private cloud configuration . . . . .	959
	Update the GTI private cloud configuration . . . . .	960
	Import GTI private cloud certificate to the Manager . . . . .	961
	Get the IP status from a GTI private cloud . . . . .	962
	Get the Telemetry configuration . . . . .	963
	Update the Telemetry configuration . . . . .	965
<b>82</b>	<b>License Resource</b>	<b>967</b>
	Get the vIPS licenses present on the Manager . . . . .	967
	Get the Proxy licenses present on the Manager . . . . .	968
	Get the Capacity licenses present on the Manager . . . . .	969
	Import license to the Manager . . . . .	971
	Assign a license . . . . .	972
	Unassign a license . . . . .	973
	Delete licenses . . . . .	974
	Get the Sensors for association . . . . .	975
<b>83</b>	<b>IPS Inspection Whitelist Resource</b>	<b>977</b>
	Get IPS Inspection whitelist from the Manager . . . . .	977
	Get Details of a domain name from IPS Inspection Whitelist . . . . .	978
	Add domain name to IPS Inspection whitelist . . . . .	979
	Import the Domain Name Exceptions to the Manager . . . . .	980
	Export the Domain Name Exceptions from the Manager . . . . .	982
	Update the details of Domain Name Exceptions . . . . .	983
	Delete Domain Name Exceptions from the IPS Inspection Whitelist . . . . .	984
	Delete all Domain Names from IPS Inspection Whitelist . . . . .	985
	Update status of Domain Name Exceptions from IPS Inspection Whitelist . . . . .	986
<b>84</b>	<b>SSL Exception Rules</b>	<b>989</b>
	Get all the SSL Outbound Exception Rules . . . . .	989
	Get single Outbound Exception Rule . . . . .	991
	Create an Outbound Exception Rule . . . . .	993
	Update an Outbound Exception Rule . . . . .	995
	Delete an Outbound Exception Rule . . . . .	997
<b>85</b>	<b>Dashboard Monitors</b>	<b>999</b>
	Get top active botnets . . . . .	999
	Get top attack applications . . . . .	1000
	Get top attack subcategories . . . . .	1002
	Get top attacker countries . . . . .	1003
	Get top attackers . . . . .	1004
	Get top attacks . . . . .	1006
	Get top highrisk hosts . . . . .	1007
	Get top malware downloads . . . . .	1008
	Get top target countries . . . . .	1010



Get top targets . . . . .	1011
Get top unblocked malware downloads . . . . .	1012
Get top endpoint executables . . . . .	1013
<b>86 HTTP Error Codes Reference</b>	<b>1017</b>
<b>Index</b>	<b>1019</b>



# Preface

This guide provides the information you need to configure, use, and maintain your McAfee product.

## Contents

- ▶ [About this guide](#)
- ▶ [Find product documentation](#)

---

## About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

## Audience





McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

## Conventions

This guide uses these typographical conventions and icons.

<i>Italic</i>	Title of a book, chapter, or topic; a new term; emphasis
<b>Bold</b>	Text that is emphasized
Monospace	Commands and other text that the user types; a code sample; a displayed message
<b>Narrow Bold</b>	Words from the product interface like options, menus, buttons, and dialog boxes
Hypertext blue	A link to a topic or to an external website
	<b>Note:</b> Extra information to emphasize a point, remind the reader of something, or provide an alternative method
	<b>Tip:</b> Best practice information
	<b>Caution:</b> Important advice to protect your computer system, software installation, network, business, or data
	<b>Warning:</b> Critical advice to prevent bodily harm when using a hardware product

## What's in this guide

This guide contains information related to an Application Programming Interface (API) framework provided by the McAfee® Network Security Manager (NSM) for external applications to access core Network Security Platform (NSP) functionalities through the REST protocol.

---

## Find product documentation

Network Security Platform Documentation can be accessed using one of the two options listed below:

- 1 **McAfee Documentation Portal:** To view the documents, perform the following steps:
  - a Go to the **McAfee Documentation Portal** at <https://docs.mcafee.com/>.
  - b In the **Browse Documentation Library**, select **Network Security Platform**.
  - c Under the **Product** filter in the left pane, select the version to display a list of documents.
- 2 **McAfee Download Server:** PDF versions of the product documentation provided alongside this release.
  - a Go to the **McAfee Download Server** at <https://secure.mcafee.com/apps/downloads/my-products/login.aspx>.
  - b Enter the **Grant Number** and **Email Address**.
  - c Click **Submit**.
  - d Under the **Filters** in the left pane, select **Network Security**.
  - e Click on the product name for the version of your choice.
  - f Under the **Filters** in the left pane, select **DOCUMENTATION**.
  - g Download the .ZIP file that contains the documentation for the product.

# 1

## 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.).

### Contents

- ▶ *SDK API access*
- ▶ *SDK Authentication/Validation*
- ▶ *Version Support*

## 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).

Method  
GET

Request URL

SEND

Parameters

Headers Authorization Variables Actions

Toggle source mode Insert headers set

Header name Header value

ADD HEADER

Headers are valid

Headers size: bytes

- 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:



For more headers, select **ADD HEADER**.

Header Name	Header Value
NSM-SDK-API	<base64 encoded value of Manager credentials, that is username:userpassword>
	Base 64 encoded values can be generated at <a href="https://www.base64encode.org/">https://www.base64encode.org/</a> . For example, the base 64 encoded value of admin:admin123 is YWRtaW46YWRtaW4zMjM=
	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


For few resource URLs, the Accept and Content-Type values 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 the Domain Name Exceptions to the Manager	POST /domainnameexceptions/ipsinspectionwhitelist/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>	

Resource	Resource URL	Method	Content-type value	Accept value
Import Custom Fingerprints	PUT /domain/<domain_id>/filereputation/customfingerprints	PUT	multipart/form-data; boundary=<x>	
Import Whitelisted Fingerprints	PUT /domain/<domain_id>/filereputation/whitelistedfingerprints	PUT	multipart/form-data; boundary=<x>	
Import GTI private cloud certificate to the Manager	PUT /gticonfiguration/private/importcert	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>	
Get the licenses present on the Manager	PUT /license	PUT	multipart/form-data; boundary=<x>	
Upgrade the vNSP Controller software	/sdkapi/cloud/connector/<id>/upgrade	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>/diagnostictrace/export	PUT		application/octet-stream



Resource	Resource URL	Method	Content-type value	Accept value
Download the Cluster Virtual Probe agent	GET/cloud/cluster/<id>/downloadagent	GET		application/octet-stream
Download the Cluster probe agent without login	GET/cloud/cluster/downloadprobeagent	GET		application/octet-stream



This resource does not require a "session resource URL" for a user to authenticate with the Manager as it can download the cluster probe agent without logging in.

Method: GET Request URL: https://10.208. /sdkapi/session SEND

Parameters

Headers Authorization Variables Actions

Toggle source mode + Insert headers set

Header name	Header value	
NSM-SDK-API	YWRtaW46YWRtaW4xMjM=	×
Header name	Header value	
Accept	application/vnd.nsm.v1.0+json	× ?
Header name	Header value	
Content-Type	application/json	× ?

ADD HEADER

## 8 Click **Send**.

### Response

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

- 9 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==

- 10 To obtain the response of other resource URLs, in **Request URL** replace `https://<nsm_ip>/sdkapi/session` with `https://<nsm_ip>/sdkapi/<resource URL>` and NSM-SDK-API with the base 64 encoded value obtained.

For example consider heartbeat resource, in **Request URL** give `https://<nsm_ip>/sdkapi/heartbeat` and NSM-SDK-API with `QUJDM0FDOUFCMz1FRtMyMkMyNjFCNzMzMjcYRkM0OUY6MQ==`

The screenshot shows a REST client interface. The Method is GET and the Request URL is `https://10.208. /sdkapi/heartbeat`. The Headers tab is selected, showing a table with the following headers:

Header name	Header value
NSM-SDK-API	<code>QUJDM0FDOUFCMz1FRtMyMkMyNjFCNzMzMjcYRkM0OUY6MQ==</code>
Accept	<code>application/vnd.nsm.v1.0+json</code>
Content-Type	<code>application/json</code>

Below the table is an "ADD HEADER" button.

- 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.



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.



# 2

## Resources

The operation to be performed in a Resource is mentioned as a HTTP verb (GET/POST/PUT/DELETE).

The following are the URIs and actions performed on requesting them.

### Contents

- ▶ *Session*
- ▶ *Heartbeat*
- ▶ *Domain*
- ▶ *Dashboard Monitors*
- ▶ *Sensor*
- ▶ *Interface*
- ▶ *Port*
- ▶ *Attacks*
- ▶ *IPS Policies*
- ▶ *Attack Filters*
- ▶ *Rule Objects*
- ▶ *Firewall Policies*
- ▶ *Scanning Exception*
- ▶ *IPS Quarantine*
- ▶ *Connection Limiting Policies*
- ▶ *Non Standard Ports*
- ▶ *SSL Key*
- ▶ *Rate Limiting Profiles*
- ▶ *QoS Policy*
- ▶ *Advanced Malware Policy*
- ▶ *File Reputation*
- ▶ *Alert Relevance*
- ▶ *Manage Import*
- ▶ *Malware Archive*
- ▶ *Passive Device Profiling*
- ▶ *Alert Exception*
- ▶ *Global Auto Acknowledgment*
- ▶ *Name Resolution Resource*
- ▶ *Device Resource*
- ▶ *NTBA Monitors*
- ▶ *Endpoint Executables Resource*
- ▶ *NMS IP Resource*
- ▶ *NMS Users Resource*
- ▶ *Policy Export Import Resource*
- ▶ *TCP Settings Resource*
- ▶ *IP Settings Resource*
- ▶ *Firewall Logging Resource*

- ▶ *IPS Alerting Resource*
- ▶ *Failover Resource*
- ▶ *Syslog Firewall Resource*
- ▶ *Syslog Faults Notification Resource*
- ▶ *Tacacs Resource*
- ▶ *Active Botnets Resource*
- ▶ *Automatic Update Configuration Resource*
- ▶ *Malware Downloads Resource*
- ▶ *Nessus scan report Resource*
- ▶ *ATD Configuration Resource*
- ▶ *Sensor Configuration Export Import Resource*
- ▶ *Denial Of Services Resource*
- ▶ *Domain Name Exceptions Resource*
- ▶ *EPO Integration Resource*
- ▶ *Packet Capture Resource*
- ▶ *Policy Group Resource*
- ▶ *Policy Assignments Resource*
- ▶ *Ignore Rules/NTBA Ignore Rules*
- ▶ *Inspection Options Policy Resource*
- ▶ *DXL Integration Resource*
- ▶ *Threat Explorer Resource*
- ▶ *Network forensics*
- ▶ *Gateway Anti-Malware Engine Update Resource*
- ▶ *Users*
- ▶ *Alert Pruning*
- ▶ *Custom Role*
- ▶ *Direct Syslog Resource*
- ▶ *Radius Resource*
- ▶ *Advanced Device Configuration Resource*
- ▶ *Attack Log Rest API*
- ▶ *Traffic Statistics*
- ▶ *CLI Auditing Resource*
- ▶ *Diagnostics Trace Resource*
- ▶ *Health Check Resource*
- ▶ *McAfee Cloud Integration Resource*
- ▶ *Performance Monitoring Resource*
- ▶ *Attack Set Profile*
- ▶ *Proxy Server*
- ▶ *Cloud Resource*
- ▶ *Quarantine Zone Resource*
- ▶ *GTI and Telemetry Resource*
- ▶ *License Resource*
- ▶ *IPS Inspection Whitelist Resource*
- ▶ *SSL Exception Rules*

## 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	Provides NSM availability information with basic details like MDR configuration

## 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 reconpoilcy in the domain
6	/domain	GET	Get details of all Admin Domains in NSM - starting from root AD and all 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


S.No	Request URI	Actions Allowed	Actions Performed
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 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 config has been changed and configuration update is pending to the sensor. The configuration change details are provided as well.
6	/sensor/<sensor_id>/performancestats?metric=<metric>&portId=<port_id>	GET	Provides Performance stats for the specified sensor, metric and portId
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
15	sensor/<sensor_id>/deploydevicesoftware	GET	Get device softwares 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 a interface_id is mentioned, the 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.  <div>  multiple comma separated vlans can be provided for this operation. </div>
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.
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 NSM
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>/ipsolicies	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>/ipsolicies/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

S.No	Request URI	Actions Allowed	Actions Performed
6	/domain/< domain_id>/attackfilter	POST	Assign the specified attack filters to a particular domain and attack
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 SubInterface 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 SubInterface 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 SubInterface 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
5	/ruleobject/<ruleobject_id>/assignments	GET	Get the associations of rule objects in all the modules where it is being used

S.No	Request URI	Actions Allowed	Actions Performed
6	/domain/<domain_id>/ruleobject?type=<ruleobject_type>	GET	Get the list of Rule Objects defined in a particular domain Query Parameter: ?type= <ul style="list-style-type: none"> <li>• application</li> <li>• applicationgroup</li> <li>• applicationoncustomport</li> <li>• country</li> <li>• finitetimeperiod</li> <li>• hostdnsname</li> <li>• hostipv4</li> <li>• hostipv6</li> <li>• ipv4addressrange</li> <li>• ipv6addressrange</li> <li>• networkipv4</li> <li>• networkipv6</li> <li>• networkgroup</li> <li>• recurringtimeperiod</li> <li>• recurringtimeperiodgroup</li> <li>• service</li> <li>• servicerange</li> <li>• servicegroup</li> </ul>
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 usergroup 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
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

S.No	Request URI	Actions Allowed	Actions Performed
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
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
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

S.No	Request URI	Actions Allowed	Actions Performed
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
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 ruleId
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
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/blacklistedhashes?search=<search_string>	GET	Get the list of blacklisted hashes
9	/advancedmalware/whitelistedhashes?search=<search_string>	GET	Get the list of whitelisted hashes
10	/advancedmalware/blacklistedhashes /<hash>/takeaction/<action>	PUT	Move the hashes from blacklist to whitelist
11	/advancedmalware /whitelistedhashes/ <hash>/takeaction/<action>	PUT	Move the hashes from whitelist to blacklist
12	/advancedmalware/blacklistedhashes/multipleHash/takeaction/whitelist	PUT	Moves multiple hashes from blacklist to whitelist
13	/advancedmalware/whitelistedhashes/multipleHash/takeaction/blacklist	PUT	Moves multiple hashes from whitelist to blacklist
14	/advancedmalware/blacklistedhashes/takeaction/removeall	PUT	Removes all the blacklisted hashes
15	/advancedmalware /whitelistedhashes/takeaction/removeall	PUT	Removes all the whitelisted hashes
16	/advancedmalware?type=<hashtype>	POST	Add a hash file to either a blacklist or a whitelist
17	/advancedmalware?type=<hashtype>	PUT	Update the details of filehash
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/whitelistedfingerprints	PUT	Import the list of Whitelisted Fingerprints to NSM
3	/domain/<domain_id>/filereputation/whitelistedfingerprints	DELETE	Delete the Whitelisted Fingerprints imported in NSM
4	/domain/<domain_id>/filereputation/customfingerprints	PUT	Import the list of Blacklisted Fingerprints to NSM
5	/domain/<domain_id>/filereputation/customfingerprints	DELETE	Delete the Custom Fingerprints imported in NSM
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 Whitelisted 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
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 softwares 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 White 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

S.No	Request URI	Actions Allowed	Actions Performed
5	/globalautoack/rules/<rule_id>	POST	Get Global Auto Ack Rule
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
2	/ntbamonitors/{ntbald}/hoststhreatfactor?TopN=<TopN> &timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>	GET	Retrieves the list of Hosts Threat Factors details
3	/ntbamonitors/{ntbald}/topurls?TopN=<TopN> &timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>	GET	Retrieves the list of Top URLs details

S.No	Request URI	Actions Allowed	Actions Performed
4	/ntbamonitors/{ntbald}/topzoneurls/<zoneid>	GET	Retrieves the list of Top Zone URLs details
5	/ntbamonitors/{ntbald}/tophosturls/<hostId >	GET	GRetrieveset the list of Top Host URLs details
6	/ntbamonitors/{ntbald}/topurlsbyreputation? TopN=<TopN> &timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>	GET	Retrieves the list of Top URLs by Reputation details
7	/ntbamonitors/{ntbald}/showurlactivity/{urlid}? TopN=<TopN> &timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>	GET	Retrieves the list of URL activity details
8	/ntbamonitors/{ntbald}/ topurlsbycategory? TopN=<TopN> &timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>	GET	Retrieves the list of Top URLs category details
9	/ntbamonitors/{ntbald}/ topurlsbycategory/ <category_id>? TopN=<TopN> &timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>	GET	Retrieves the details of Top URLs Detail by category ID
10	/ntbamonitors/{ntbald}/topfiles? TopN=<TopN> &timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>	GET	Retrieves the list of Top File details
11	/ntbamonitors/{ntbald}/topzonefiles/<zone_id	GET	Retrieves the list of Top Zone File details
12	/ntbamonitors/{ntbald}/tophostfiles/<host_id	GET	Retrieves the detail of Top host files by Id
13	/ntbamonitors/{ntbald}/ fileactivity/{fileid}? TopN=<TopN> &timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>	GET	Retrieves the list of File Activity details
14	/ntbamonitors/{ntbald}/topexthostsbyreputation? TopN=<TopN> &timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>	GET	Retrieves the list of Top External host by reputation details
15	/ntbamonitors/{ntbald}/newhosts? TopN=<TopN>	GET	Retrieves the details of new hosts
16	/ntbamonitors/{ntbald}/activehosts? TopN=<TopN> &timePeriod=<timePeriod>&startTime=<startTime>&endTime=<endTime>	GET	Retrieves the list of Active hosts details
17	/ntbamonitors/{ntbald}/tophoststraffic? TopN=<TopN> &startTime=<startTime>&endTime=<endTime>&direction=<direction>	GET	Retrieves the list of Top Hosts traffic details

S.No	Request URI	Actions Allowed	Actions Performed
18	/ntbamonitors/{ntbald}/applicationtraffic? TopN=<TopN> &startTime=<startTime>&endTime= <endTime>&direction=<direction>&frequency=<frequency>	GET	Retrieves the list of application on Traffic details
19	/ntbamonitors/{ntbald}/ applicationtraffic/ profile/{appld}? startTime=<startTime>&endTime= <endTime>	GET	Retrieves the list of application on Traffic details for App ID
20	/ntbamonitors/{ntbald}/throughputtraffic? TopN=<TopN> &startTime=<startTime>&endTime= <endTime>&frequency=<frequency>	GET	Retrieves the list of Through put traffic details list
21	/ntbamonitors/{ntbald}/bandwidthutilization? TopN=<TopN>	GET	Retrieves the list of Bandwidth utilization by Retrieves
22	/ntbamonitors/{ntbald}/zonetraffic? TopN=<TopN> &direction=<direction>&frequency= <frequency>	GET	Retrieves the list of zone traffic details
23	/ntbamonitors/{ntbald}/activeservices? TopN=<TopN> &timePeriod=<timePeriod>&startTime= <startTime>&endTime=<endTime>	GET	Retrieves the list of Active Users
24	/ntbamonitors/{ntbald}/tophostactiveservices/<host_id>? TopN=<TopN> &timePeriod=<timePeriod>&startTime= <startTime>&endTime=<endTime>	GET	Retrieves the list of Top host active users
25	/ntbamonitors/{ntbald}/newservices? TopN=<TopN>	GET	Retrieves the list of new services
26	/ntbamonitors/{ntbald}/activeapplications? TopN=<TopN> &timePeriod=<timePeriod>&startTime= <startTime>&endTime=<endTime>	GET	Retrieves the list of active applications
27	/ntbamonitors/{ntbald}/newapplications? TopN=<TopN>	GET	Retrieves the list of new applications
28	/ntbamonitors/{ntbald}/tophostactiveapplications/<host_id>? TopN=<TopN> &timePeriod=<timePeriod>&startTime= <startTime>&endTime=<endTime>	GET	Retrieves the list of Top host active applications
29	/ntbamonitors/{ntbald}/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
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 whitelist/balcklist/ 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

S.No	Request URI	Actions Allowed	Actions Performed
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
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 Setting 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 Setting 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
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>/dosprofilesmanager	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 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 whitelist
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
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

S.No	Request URI	Actions Allowed	Actions Performed
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
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

S.No	Request URI	Actions Allowed	Actions Performed
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>? starttime=<start_time>&& duration=<duration>&& ntba=<ntb a_id>	GET	Retrieves the host summary for given IP address. URL Parameter 1: <b>ipaddress</b> Query Parameter1: <b>starttime</b> = Date in the format yyyy-MMM-dd HH:mm Query Parameter 2: <b>duration</b> = <ul style="list-style-type: none"> <li>• NEXT_60_SECONDS</li> <li>• NEXT_5_MINUTES</li> <li>• NEXT_60_MINUTES</li> <li>• NEXT_30_MINUTES</li> </ul> Query Parameter 3: <b>ntba id</b>
2	/networkforensics/<ipaddress>/ suspiciousflows ? starttime=<start_time> &&duration=<duration>&& ntba=<ntba_id>	GET	Retrieves the top suspicious flows for the given IP address. URL Parameter 1: <b>ipaddress</b> Query Parameter1: <b>starttime</b> = Date in the format yyyy-MMM-dd HH:mm Query Parameter 2: <b>duration</b> = <ul style="list-style-type: none"> <li>• NEXT_60_SECONDS</li> <li>• NEXT_5_MINUTES</li> <li>• NEXT_60_MINUTES</li> <li>• NEXT_30_MINUTES</li> </ul> Query Parameter 3: <b>ntba id</b>

## 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
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



S.No	Request URI	Actions Allowed	Actions Performed
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 Rest API

Priority	Request URI	Actions Allowed	Actions Performed
1	/alerts? domainId=<domain_id>&includeChildDomain=<true/false>&alertstate=<state>&timeperiod=<timeperiod> &starttime=<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> &starttime==<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> &starttime==<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 critria 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/Unacknowledge and to update assignTo.
6	/alerts/<alert_uuid>? sensorId=<sensor_id>&manager=<manager_name>	DELETE	Delete the single alert.
7	/alerts/<alert_id>/triggeredpkt	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/trafficrx	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
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

S.No	Request URI	Actions Allowed	Actions Performed
8	/sensor/{sensorId}/trafficstats/sslinternalwebcertmatches	GET	Gets the details of the inter web certificates matched
9	/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.

S.No	Request URI	Actions Allowed	Actions Performed
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
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

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

## IPS Inspection Whitelist Resource

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

## SSL Exception Rules

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





# 3

## 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



# 4

## Session Resource

### Contents

- [Login](#)
- [Logout](#)

### 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 NSM 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



The default SDK API session inactivity timeout is 24 hours

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/session](https://<NSM_IP>/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 NSM. 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://<NSM\\_IP>/sdkapi/session](https://<NSM_IP>/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 NSM Details

# 5

## Heartbeat Resource

### 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://<NSM\\_IP>/sdkapi/heartbeat](https://<NSM_IP>/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 Manager Details

# 6

## Domain Resource

### Contents

- *Create a new Domain*
- *Update a Domain*
- *Get a Domain*
- *Delete a Domain*
- *Get Default Recon Policies*
- *Get All Admin Domains*
- *Get All Child Domains in a Admin Domain*

---

### 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

Field Name	Description	Data Type	Mandatory
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://<NSM\\_IP>/sdkapi/domain](https://<NSM_IP>/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
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/&lt;domain\_id&gt;

**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
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://<NSM\\_IP>/sdkapi/domain/101](https://<NSM_IP>/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
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)

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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
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://<NSM\\_IP>/sdkapi/domain/101](https://<NSM_IP>/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://<NSM\\_IP>/sdkapi/domain/105](https://<NSM_IP>/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://<NSM\\_IP>/sdkapi/domain/101/defaultreconpolicies](https://<NSM_IP>/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 NSM 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 DomainDescriptor object	array

### Example

#### Request

GET [https://<nsm\\_ip>/sdkapi/domain](https://<nsm_ip>/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 NSM Details

## Get All Child Domains in a Admin Domain

This API gets details of all Child Admin Domains in NSM 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 DomainDescriptor object	array

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/domain/101](https://<NSM_IP>/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

# 7

## Sensor Resource

### Contents

- ▶ *Get all Sensors in a Domain*
- ▶ *Get Sensor Details*
- ▶ *Update Sensor Configuration*
- ▶ *Get Configuration Update Status*
- ▶ *Is Sensor Config Modified*
- ▶ *Get Sensor Performance Stats*
- ▶ *Reboot Sensor*
- ▶ *Set IPv6*
- ▶ *Get IPv6 Setting*
- ▶ *Get Sensor Status*
- ▶ *Get Application Identification*
- ▶ *Update Application Identification*
- ▶ *Get NTBA Integration Configuration*
- ▶ *Update NTBA Integration Configuration*
- ▶ *Get Device Softwares Deployed and Available*
- ▶ *Upgrade the Software on Device*
- ▶ *Get the Upgrade Software Status*

---

### 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
nsmVersion	NSM Version	string
MemberSensors	Member sensors in case of fail over and load balancer	array

Details of object in MemberSensors :

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://<NSM\\_IP>/sdkapi/sensors](https://<NSM_IP>/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": "MCAFEES-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": "MCAFEES-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": "MCAFEES-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

Field Name	Description	Data Type
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	SubInterface 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

Field Name	Description	Data Type
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
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://<NSM\\_IP>/sdkapi/sensor/1001](https://<NSM_IP>/sdkapi/sensor/1001)



**Response**

```
{
  "SensorInfo": {
    "SensorDescriptor": {
      "sensorId": 1001,
      "name": "NS7100",
      "model": "IPS-NS7100",
      "Description": "MCAFFEE-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"
      }],
      "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	Gam 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://<NSM\\_IP>/sdkapi/sensor/1001/action/update\\_sensor\\_config](https://<NSM_IP>/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 NSM
13	400	1149	SSL key decryption not enabled on Sensor
14	400	1150	No Configuration changes to push



S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
15	400	1151	No SSL decryption key existed
16	400	1152	Botnet is not enabled/supported for this sensor
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
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://<NSM\_IP>/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
lastUpdateTime	Last updated Timestamp of the Config Push	string
pendingChanges	Configuration changes details	object
isGAMUpdateRequired	GAM 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://<NSM\\_IP>/sdkapi/sensor/1001/ action/update\\_sensor\\_config](https://<NSM_IP>/sdkapi/sensor/1001/ action/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
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](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](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://<NSM\\_IP>/sdkapi/sensor/1001/ipv6](https://<NSM_IP>/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://<NSM\\_IP>/sdkapi/sensor/1001/ipv6](https://<NSM_IP>/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://<NSM\\_IP>/sdkapi/sensor/1001/status](https://<NSM_IP>/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](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](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 for	string
targetNTBA	NTBA Name	string
flowCollectionIPAddr	Destination IP	string
flowCollectionUDPPort	Destination UDP Port	number
portUsedToExportTraffic	FlowSource	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	networkMask	string
defaultGateway	defaultGateway	string
VLANId	VLANId	number

#### Details of Monitoring Ports

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

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/sensor/0/ntbaintegration](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 for	string
targetNTBA	NTBA Name	string
flowCollectionIPAddr	Destination IP	string
flowCollectionUDPPort	Destination UDP Port	number
portUsedToExportTraffic	FlowSource	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	networkMask	string
defaultGateway	defaultGateway	string
VLANId	VLANId	number

Details of Monitoring Ports

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

Possible values for portNTBADirection

- 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](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 Softwares Deployed and Available

This URL retrieves the device softwares 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](https://<NSM_IP>/sdkapi/sensor/1001/deploydevicesoftware)

### Response

```
{
  " runningSoftwareVersion ": '8.2.3.12',
  " softwaresReadyForInstallation ": [ "8.2.7.1","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
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/8.2.3.12](https://<NSM_IP>/sdkapi/sensor/1001/deploydevicesoftware/8.2.3.12)

### 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
updateStatusMessage	Update message	string

## Example

### Request

PUT [https://<NSM\\_IP>/sdkapi/sensor/1001/deploydevicesoftware/1337547887180](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



# 8

## Interface Resource

### Contents

- ▶ *Get Interface/Sub Interface details*
- ▶ *Update Interface/Sub Interface details*
- ▶ *Add Sub Interface*
- ▶ *Delete a Sub Interface*
- ▶ *Add/Assign VLAN*
- ▶ *Delete/revoke VLAN*
- ▶ *Get available interfaces to allocate*
- ▶ *Get list of interfaces allocated to a sensor inside a domain*
- ▶ *Get list of CIDR allocated to an interface*
- ▶ *Allocate an interface to a sensor in child domain*
- ▶ *Delete/Revoke an interface from a sensor in child domain*
- ▶ *Adds/Assign CIDR*
- ▶ *Delete CIDR*

---

## 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/SubInterface	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 / 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	SubInterface 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 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://<NSM\_IP>/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/SubInterface	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 / 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	SubInterface 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 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

Field Name	Description	Data Type
InterfaceType	Traffic type. VLAN, CIDR, or BridgeVlan	string
IPSPolicyId	IPS policy applied on interface	number
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://<NSM\\_IP>/sdkapi/sensor/1001/interface/105](https://<NSM_IP>/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

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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
12	400	1111	Cannot create dedicated type subinterface
13	400	1160	Subinterface 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 of Interface/SubInterface	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

Field Name	Description	Data Type	Mandatory
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 SubInterface	number

## Example

### Request

POST [https://<NSM\\_IP>/sdkapi/sensor/1001/interface/105](https://<NSM_IP>/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 subinterface
5	400	1160	Subinterface 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
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 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
Status	Status returned by deletion	number

## Example

### Request

DELETE [https://<NSM\\_IP>/sdkapi/sensor/1001/interface/124](https://<NSM_IP>/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
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://<NSM\\_IP>/sdkapi/sensor/1001/interface/105/vlan](https://<NSM_IP>/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:

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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://<NSM\\_IP>/sdkapi/sensor/1001/interface/127/vlan/17,18,19](https://<NSM_IP>/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 InterfaceInf	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 InterfaceInf	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://<NSM\\_IP>/sdkapi/domain/103/sensor/1002/availableinterfaces](https://<NSM_IP>/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"
      ]
    }
  },
  {
    "interfaceId": 114,
    "name": "3A",
    "interfacetype": {
      "Dedicated": {
      }
    }
  },
  {
    "interfaceId": 113,
    "name": "4A-4B",
    "interfacetype": {
      "Dedicated": {
      }
    }
  },
  {
    "interfaceId": 112,
    "name": "5A-5B",
    "interfacetype": {
      "Dedicated": {
      }
    }
  },
  {
    "interfaceId": 111,
    "name": "6A-6B",
    "interfacetype": {
      "Dedicated": {
      }
    }
  },
  {
    "interfaceId": 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 AllocatedInterfaceElem	array

Details of fields in AllocatedInterfaceElem :

Field Name	Description	Data Type
interfaceId	Interface id	number
interfaceName	Interface name	string
interfaceType	Interface Type	string

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/domain/103/sensor/1001/allocatedinterfaces](https://<NSM_IP>/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://<NSM\\_IP>/sdkapi/sensor/1002/interface/110/allocatedcidrlist](https://<NSM_IP>/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://<NSM\\_IP>/sdkapi/domain/103/sensor/1002/allocateinterfaces](https://<NSM_IP>/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://<NSM\\_IP>/sdkapi/domain/103/sensor/1002/interface/124/revokeinterface?value=8](https://<NSM_IP>/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](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.
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](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.
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.



# 9

## Port Resource

### 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://<NSM\\_IP>/sdkapi/sensor/1001/port/101](https://<NSM_IP>/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



# 10 Attack Resource

## Contents

- [Get all Attacks](#)
- [Get Attack Details](#)

## Get all Attacks

This URL gets all available attack definitions in NSM

### 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 ID	string
name	Attack name	string
DosDirection	Attack direction, Can be "INBOUND" / "OUTBOUND" / "BOTH"	string
Severity	Attack severity, number between 0 & 9	number
UiCategory	Attack category, can be "Exploit" / "Malware" / "Reconnaissance Signature Attack" / "Policy Violation" / "Reconnaissance Correlation Attack" / "DOS Threshold Attack" / "DOS Learning Attack"	string
industryIds	Reference IDs for the attack	object

Details of object in industryIds:

Field Name	Description	Data Type
CERT	CERT ID list	string
CVE	CVE ID list	string
archNIDS	ArchNIDS list	string
microsoft	Microsoft ID list	string
bugtraq	BugTraq ID list	string

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/attacks](https://<NSM_IP>/sdkapi/attacks)

### Response

```
{
  "AttackDescriptorDetailsList": [
    ...
    {
      'industryIds': {
        'CERT': 'CA-2003-09',
        'CVE': 'CVE-2003-0109,CVE-2000-0561,CVE-1999-0744,CVE-2000-0043,CVE-2000-0395,CVE-2000-0484,CVE-2000-0571',
        'archNIDS': 'IDS258',
        'microsoft': 'MS03-007',
        'bugtraq': '1365,906,905,1213,1355,1423'},
      'Severity': 1,
      'attackId': '0x40208200',
      'UiCategory': 'Exploit',
      'DosDirection': None,
      'name': 'HTTP: URITooLong'
    }
    ...
  ]
}
```

## 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 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 & 9	number
UiCategory	Attack category, can be "Exploit" / "Malware" / "Reconnaissance Signature Attack" / "Policy Violation" / "Reconnaissance Correlation Attack" / "DOS Threshold Attack" / "DOS Learning Attack"	string
industryIds	Reference IDs for the attack	object

Details of object in industryIds:

Field Name	Description	Data Type
CERT	CERT ID list	string
CVE	CVE ID list	string
archNIDS	ArchNIDS list	string
microsoft	Microsoft ID list	string
bugtraq	BugTraq ID list	string

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/attacks/0x48804b00](https://<NSM_IP>/sdkapi/attacks/0x48804b00)

### Response

```
{
  "AttackDescriptor":
  {
    'industryIds': {
      'CERT': 'CA-2003-09',
      'CVE':
      'CVE-2003-0109,CVE-2000-0561,CVE-1999-0744,CVE-2000-0043,CVE-2000-0395,CVE-2000-0484,CVE-2000-0571',
      'archNIDS': 'IDS258',
      'microsoft': 'MS03-007',
      'bugtraq': '1365,906,905,1213,1355,1423'},
    'Severity': 1,
    'attackId': '0x40208200',
    'UiCategory': 'Exploit',
    'DosDirection': None,
  }
}
```

```
{  
  'name': 'HTTP: URITooLong'  
}
```

### 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

# 11

## IPS Policies Resource

### Contents

- *Get IPS Policies in a domain*
- *Get IPS Policy details*
- *Create/Update Light Weight Policy*
- *Get Light Weight Policy details*
- *Delete Light Weight Policy*
- *Create new IPS Policy*
- *Update IPS policy*
- *Delete IPS Policy*

---

### 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

Field Name	Description	Data Type
policyId	Policy ID	number
name	Policy Name	string

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/domain/0/ipspolicies](https://<NSM_IP>/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 Codes are 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
IsLightWeightPolicy	Is Light Weight Policy configured	boolean

Details of object in AttackCategory

Field Name	Description	Data Type
ExploitAttackList	List of Exploit Attacks	array

Details of object in ExploitAttackList:

Field Name	Description	Data Type
attackName	Attack Name	string
nspId	NSP ID of the attack	string
severity	Attack Severity, number between 0 & 9	number

Field Name	Description	Data Type
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
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	Customize 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



Field Name	Description	Data Type
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
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	TimeStamp	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	TimeStamp	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
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	TimeStamp	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://<NSM\\_IP>/sdkapi/ipspolicy/0](https://<NSM_IP>/sdkapi/ipspolicy/0)

## Response

```
{
  "PolicyDescriptor":
  {
    "PolicyName": "IpsPolicy",
    "Description": "To test the IPS policy",
    "IsVisibleToChildren": true,
    "InboundRuleSet": "TestIPS",
    "OutboundRuleSet": "Null",
    "AttackCategory":
    {
      "ExploitAttackList":
      [
        {
          "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

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 / subInterface 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
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
ExploitAttackList	List of Exploit Attacks	array	Yes

## Details of object in ExploitAttackList:

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
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

Field Name	Description	Data Type	Mandatory
isBlockingOptionCustomized	Is Blocking option customized	boolean	Yes
isCapturedPrior	Should application data be captured prior to attack	boolean	Yes
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	Customize 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	Timestamp	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	TimeStamp	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	TimeStamp	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



Field Name	Description	Data Type	Mandatory
isSeverityCustomized	Is attack severity customized	boolean	Yes
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	TimeStamp	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
ThresholdDuration	Threshold Interval (seconds)	number	Yes
mcAfeeNACNotification	Configured NAC notification that can be "DISABLED" / "ALL_HOSTS" / "MCAFFEE_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

Field Name	Description	Data Type	Mandatory
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://<NSM\\_IP>/sdkapi/sensor/1001/interface/105/localipspolicy](https://<NSM_IP>/sdkapi/sensor/1001/interface/105/localipspolicy)

Payload:

```
{
  "PolicyDescriptor":
  {
    "IsVisibleToChildren": true,
    "InboundRuleSet": "testRuleSet",
    "OutboundRuleSet": "Null",
    "AttackCategory":
    {
      "ExploitAttackList":
      [
        {
          "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-
MultipleResetsfromSMTPPreceiver',
'ThresholdDuration': 0,
>alertSuppressionTimer': 0,
'isAlertSuppressionTimerCustomized': False,
'isAttackCustomized': False,
'isMcAfeeNACNotificationEnabled': False,
'isThresholdValueCustomized': False,
'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
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>/localipolicy

### 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
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
ExploitAttackList	List of Exploit Attacks	array

Details of object in ExploitAttackList:

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
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

Field Name	Description	Data Type
flow	Customize 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	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
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



Field Name	Description	Data Type
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	TimeStamp	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	TimeStamp	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
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	TimeStamp	string
Notification	Notification to be sent	object

Field Name	Description	Data Type
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
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" / "MCAFFEE_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://<NSM\\_IP>/sdkapi/sensor/1001/interface/105/localipspolicy](https://<NSM_IP>/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":
{
  "ExploitAttackList":
  [
    {
      "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-
MultipleResetsfromSMTPPreceiver',

```

```

        '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
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

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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 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 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
Status	Status returned by deletion	number

### Example

#### Request

DELETE [https://<NSM\\_IP>/sdkapi/sensor/1001/interface/105/localipspolicy](https://<NSM_IP>/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

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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: <ul style="list-style-type: none"><li>• 0</li><li>• 1</li></ul>	number	Yes

Field Name	Description	Data Type	Mandatory
isEditable	Is policy editable after creation	boolean	No
direction	Consider inbound/outbound direction values can be: <ul style="list-style-type: none"> <li>• 0</li> <li>• 1</li> </ul>	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](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

This URL updates IPS policy.



**Resource URL**

PUT /ipspolicy/&lt;policyid&gt;

**Request Parameters**

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
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
ReconPolicy	Reconnaissance policy attack list	Object	No
AttackCategory	Attack category	Object	No
OutboundAttackCategory	Outbound attack category	Object	No
DosPolicy	DOS Policy	Object	No
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

Details of object in AttackCategory:

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

Details of object in ExploitAttackList:

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
isRecommendedForSmartBlocking	Is attack recommended for smart blocking	Boolean	No
AttackResponse	Attack response	Object	No
notification	Notifications configured	Object	No

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 <ul style="list-style-type: none"> <li>• Disabled source</li> <li>• Disabled destination</li> <li>• Both</li> </ul>	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 <ul style="list-style-type: none"> <li>• Disabled</li> <li>• All hosts</li> <li>• McAfee NAC unmanaged hosts</li> </ul>	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 <ul style="list-style-type: none"> <li>• Disable</li> <li>• Enable</li> <li>• Enable smart blocking</li> </ul>	String	No
isBlockingOptionCustomized	Is blocking option customized	Boolean	No
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 <ul style="list-style-type: none"> <li>• Do nothing</li> <li>• Send alert and log packets</li> <li>• Send alert only</li> </ul>	String	No
isLogCustomized	Is Logging customized	Boolean	No

Field Name	Description	Data Type	Mandatory
flow	Customize flow, can be <ul style="list-style-type: none"><li>• Single flow</li><li>• Forensic analysis</li></ul>	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
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 <ul style="list-style-type: none"><li>• Seconds</li><li>• Minutes</li><li>• Hours</li><li>• Days</li></ul>	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

Field Name	Description	Data Type	Mandatory
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
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 id 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	String	No
direction	Attack direction can be: <ul style="list-style-type: none"> <li>• Inbound</li> <li>• Outbound</li> <li>• Inbound and outbound</li> </ul>	String	No
notification	Notification to be sent via	Object	No

Details of object in ThresholdAttack:

Field Name	Description	Data Type	Mandatory
attackName	Attack name	String	No
nspId	Network Security Platform id of the attack	String	No
isSeverityCustomized	Is the attack severity customized	Boolean	No
severity	Attack severity between 0 and 9	Number	No

Field Name	Description	Data Type	Mandatory
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	String	No
notification	Notification to be sent via	Object	No
direction	Attack direction can be: <ul style="list-style-type: none"><li>• Inbound</li><li>• Outbound</li><li>• Inbound and outbound</li></ul>	String	No

Details of object in ReconAttack List:

Field Name	Description	Data Type	Mandatory
isAlertCustomized	Is alert customized	String	No
nspId	Network Security Platform id 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
isAlertCustomized	Is alert customized	Boolean	No
isSendAlertToManager	Is alert notification to be sent to the Manager configured	String	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 <ul style="list-style-type: none"><li>• Disabled</li><li>• All hosts</li><li>• McAfee NAC unmanaged hosts</li></ul>	String	No
notification	Notification to be sent via	Object	No
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**

POST [https://<NSM\\_IP>/sdkapi/ipspolicy/<policyid>](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": {
    "ExploitAttackList": [
        {
            "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": {
                    "CaptureNBytes": {
```

```

        "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": {
  "ExploitAttackList": [
    {
      "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
}
```



# 12 Attack Filters Resource

## Contents

- ▶ *Add a new Attack Filter*
- ▶ *Update Attack Filter*
- ▶ *Delete Attack Filter*
- ▶ *Get a Attack Filter*
- ▶ *Get Attack Filters defined in a domain*
- ▶ *Assign a Attack Filter to a domain and attack*
- ▶ *Get Attack Filters assigned to a domain and attack*
- ▶ *Unassign Attack Filters assigned to a domain and attack*
- ▶ *Assign a Attack Filter to a sensor and attack*
- ▶ *Get Attack Filters assigned to a sensor and attack*
- ▶ *Unassign Attack Filter to a sensor and attack*
- ▶ *Assign a Attack Filter to an Interface/SubInterface and attack*
- ▶ *Get Attack Filters assigned to an Interface/SubInterface and attack*
- ▶ *Unassign Attack Filters to an Interface/SubInterface*
- ▶ *Get Attack Filters assignments*

---

## 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
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://<NSM\\_IP>/sdkapi/attackfilter](https://<NSM_IP>/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
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" / "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

Field Name	Description	Data Type	Mandatory
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://<NSM\\_IP>/sdkapi/attackfilter/419](https://<NSM_IP>/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
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://<NSM\\_IP>/sdkapi/attackfilter/419](https://<NSM_IP>/sdkapi/attackfilter/419)

#### 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	1408	Invalid attack filter id

## Get a 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://<NSM\\_IP>/sdkapi/attackfilter/420](https://<NSM_IP>/sdkapi/attackfilter/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 Codes are returned 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://<NSM\\_IP>/sdkapi/attackfilters?domain=0](https://<NSM_IP>/sdkapi/attackfilters?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 a Attack Filter to a domain and attack

This URL assigns the specified attack filters to a particular domain and 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 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	Assignment Status	number

### Example

#### Request

POST [https://<NSM\\_IP>/sdkapi/domain/0/attackfilter](https://<NSM_IP>/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
3	404	1403	Invalid attack direction
4	404	1408	Invalid attack filter id

## Get Attack Filters assigned to a domain and 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 Timestamp	string
filterId	Attack Filter ID	number
name	Attack Filter Name	string

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/domain/0/attackfilter/0x40503900](https://<NSM_IP>/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 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://<NSM\_IP>/sdkapi/domain/0/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	1105	Invalid domain
2	404	1402	Invalid attack id
3	404	1403	Invalid attack direction

---

## Assign a Attack Filter to a sensor and attack

This URL assigns the specified attack filters to a particular sensor and 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 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	Assignment Status	number

## Example

### Request

POST [https://<NSM\\_IP>/sdkapi/sensor/1001/attackfilter](https://<NSM_IP>/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 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
LastModTs	Last Modified Timestamp	string
filterId	Attack Filter ID	number
name	Attack Filter Name	string

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/sensor/1001/attackfilter/0x40503900](https://<NSM_IP>/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://<NSM\\_IP>/sdkapi/sensor/1001/attackfilter /0x40503900 ?direction=INBOUND](https://<NSM_IP>/sdkapi/sensor/1001/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	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
Direction	Attack Direction, can be "INBOUND" / "OUTBOUND" / "BOTH" / "UNKNOWN"	string	Yes
Overwrite	Overwrite Filter	boolean	Yes
FilterId	List of Attack Filter 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://<NSM\\_IP>/sdkapi/sensor/1001/interface/105/attackfilter](https://<NSM_IP>/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 Timestamp	string
filterId	Attack Filter ID	number
name	Attack Filter Name	string

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/sensor/1001/interface/105/attackfilter/0x40503900](https://<NSM_IP>/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

Field Name	Description	Data Type	Mandatory
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://<NSM\\_IP>/sdkapi/sensor/1001/interface/105/attackfilter/0x40503900?direction=INBOUND](https://<NSM_IP>/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://<NSM\\_IP>/sdkapi/attackfilter/<attackfilter\\_id>/assignments](https://<NSM_IP>/sdkapi/attackfilter/<attackfilter_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



# 13 Rule Objects Resource

## Contents

- [Add Rule Object](#)
- [Update Rule Object](#)
- [Delete Rule Object](#)
- [Get Rule Object](#)
- [Get Rule Object Associations](#)
- [Get Rule Objects in a Domain](#)
- [Get User Rule Objects](#)
- [Get User Group](#)

## 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

Field Name	Description	Data Type	Mandatory
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 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
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 recurringTimePeriod Rule Object IDs	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
createdResourceId	Unique ID of the created Rule Object	number

## Example

### Request

POST [https://<NSM\\_IP>/sdkapi/ruleobject](https://<NSM_IP>/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 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

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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 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

Field Name	Description	Data Type	Mandatory
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 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
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 recurringTimePeriod Rule Object IDs	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://<NSM\\_IP>/sdkapi/ruleobject/121](https://<NSM_IP>/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
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

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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://<NSM\\_IP>/sdkapi/ruleobject/121](https://<NSM_IP>/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 Type	string
name	Rule Object Name	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
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 recurringTimePeriod Rule Object IDs	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://<NSM\_IP>/sdkapi/ruleobject/<ruleobject\_id >

### 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://<NSM\\_IP>/sdkapi/ruleobject/121/assignments](https://<NSM_IP>/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 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 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 Type	string
name	Rule Object Name	string
description	Description	string

Field Name	Description	Data Type
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
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
until	To Time	string

Details of RecurringTimePeriodGroup

Field Name	Description	Data Type
recurringTimePeriodsId	List of recurringTimePeriod Rule Object IDs	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://<NSM\_IP>/sdkapi/domain/0/ruleobject?type=  
Application,ApplicationGroup,ApplicationOnCustomPort,Country,FiniteTimePeriod,HostDNSName,HostIpv4,IPv4  
AddressRange,Network,NetworkGroup,RecurringTimePeriod,RecurringTimePeriodGroup,Service,ServiceGroup

**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

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



## Response Parameters

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://<NSM\\_IP>/sdkapi/ruleobject/user?filter=user&max\\_count=10](https://<NSM_IP>/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://<NSM\\_IP>/sdkapi/ruleobject/usergroup](https://<NSM_IP>/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



# 14

## Firewall Policies Resource

### Contents

- [Add Firewall Policy](#)
- [Update Firewall Policy](#)
- [Delete Firewall Policy](#)
- [Get Firewall Policy](#)
- [Get Firewall Policies in a Domain](#)

### 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	Lastest 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
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
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
createdResourceId	Unique ID of the created SubInterface	integer

## Example

### Request

POST [https://<NSM\\_IP>/sdkapi/firewallpolicy](https://<NSM_IP>/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" : "applicaiionOncutomPort",
      "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" : "recurringTimePeriod",
    "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 objectlist of an Advanced Firewall/QoS Policy
5	400	1805	Multiple Rule objects in a single Source/Destination objectlist 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 objectlist is not applicable for Classic Firewall Policy
9	400	1809	Application objectlist is not applicable for Classic Firewall Policy



S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
10	400	1810	Multiple Rule objects in a single Service objectlist 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
13	400	1813	Source/Destination objectlist is not provided
14	400	1814	Service/Application objectlist is not provided
15	400	1815	Time objectlist is not provided
16	400	1816	Firewall Policy Name is required
17	400	1817	For Stateless Action, Application objectlist 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	Islogging should not enabled for Stateless Action
21	400	1821	Either Application or Service objectlist can be defined in a MemberRule for an Advanced Firewall Policy
22	400	1822	Composite Rule object(Multiple items in a RuleObject) is allowed for Advanced Firewall Policy only
23	400	1824	SourceUser objectlist is not applicable for Classic Firewall Policy
24	400	1825	SourceAddress objectlist is not applicable for Classic Firewall Policy
25	400	1826	DestinationAddress objectlist is not applicable for Classic Firewall Policy
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	SourceAddress and DestinationAddress objectlist 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 SourceUser objectlist 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	SourceUser objectlist is not provided
36	400	1838	Time objectlist can contain one Finite time period
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

Field Name	Description	Data Type	Mandatory
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
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://<NSM\\_IP>/sdkapi/firewallpolicy/120](https://<NSM_IP>/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" : "recurringTimePeriod",
        "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 objectlist of an Advanced Firewall/QoS Policy
6	400	1805	Multiple Rule objects in a single Source/Destination objectlist 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 objectlist is not applicable for Classic Firewall Policy
10	400	1809	Application objectlist is not applicable for Classic Firewall Policy
11	400	1810	Multiple Rule objects in a single Service objectlist 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 objectlist is not provided
15	400	1814	Service/Application objectlist is not provided
16	400	1815	Time objectlist is not provided
17	400	1816	Firewall Policy Name is required
18	400	1817	For Stateless Action, Application objectlist is not applicable
19	400	1818	Unsupported Firewall Policy Type

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
20	406	1819	Stateless Response with Any/TCP/IP Protocol no.6/Default services are not allowed
21	400	1820	Islogging should not enabled for Stateless Action
22	400	1821	Either Application or Service objectlist can be defined in a MemberRule for an Advanced Firewall Policy
23	400	1822	Composite Rule object(Multiple items in a RuleObject) is allowed for Advanced Firewall Policy only
24	400	1824	SourceUser objectlist is not applicable for Classic Firewall Policy
25	400	1825	SourceAddress objectlist is not applicable for Classic Firewall Policy
26	400	1826	DestinationAddress objectlist 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	SourceAddress and DestinationAddress objectlist 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 SourceUser objectlist 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	SourceUser objectlist is not provided
38	400	1838	Time objectlist can contain one Finite time period
39	400	1839	Stateless Response with Source User or Source User 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://<NSM\_IP>/sdkapi/firewallpolicy/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	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

Field Name	Description	Data Type
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
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" / "APPLICATION_ON_CUSTOM_PORT" / "SERVICE" / "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://<NSM\\_IP>/sdkapi/firewallpolicy/120](https://<NSM_IP>/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" : "applicaionOncustomPort",
    "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" : "recurringTimePeriod",
    "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://<NSM\\_IP>/sdkapi/domain/0/firewallpolicy](https://<NSM_IP>/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 Codes are returned by this URL:

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

# 15

## Scanning Exception Resource

### Contents

- ▶ *Create a new Scanning Exception at sensor*
- ▶ *Get Scanning Exception details on a sensor*
- ▶ *Delete Scanning Exception on a sensor*
- ▶ *Enable/Disable Scanning Exception on a sensor*
- ▶ *Get Scanning Exception status on a sensor*

### 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 portRange :

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://<NSM\\_IP>/sdkapi/sensor/<sensor\\_id>/scanningexception](https://<NSM_IP>/sdkapi/sensor/<sensor_id>/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
2	400	1502	Please provide port info object

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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
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://<NSM\\_IP>/sdkapi/sensor/<sensor\\_id>/scanningexception](https://<NSM_IP>/sdkapi/sensor/<sensor_id>/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](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](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](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



# 16 IPS Quarantine Resource

## Contents

- *Quarantine Host*
- *Update IPS Quarantine duration for a Host*
- *Release Quarantined Host*
- *Get Quarantined Hosts*
- *Get Quarantined Host Details*

## 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" / "TWELVE_HOURS" / "SIXTEEN_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": "SIXTEEN_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 "FIFTEEN_MINUTES" / "THIRTY_MINUTES" / "FORTYFIVE_MINUTES" / "SIXTY_MINUTES" / "FOUR_HOURS" / "EIGHT_HOURS" / "TWELVE_HOURS" / "SIXTEEN_HOURS" / "UNTIL_EXPLICITLY_RELEASED"	string	Yes



Field Name	Description	Data Type	Mandatory
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://<NSM\\_IP>/sdkapi/sensor/1001/action/quarantinehost](https://<NSM_IP>/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://<NSM\\_IP>/sensor/1001/action/quarantinehost/102.102.102.102](https://<NSM_IP>/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://<NSM\\_IP>/sdkapi/sensor/1001/action/quarantinehost](https://<NSM_IP>/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
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](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: Wvftftp 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

# 17

## Connection Limiting Policies Resource

### Contents

- *Add a new connection limiting policy*
- *Update a connection limiting policy*
- *Get a connection limiting policy*
- *Delete a connection limiting policy*
- *Get the list of available country*
- *Get Connection Limiting Policies in a domain*

---

### 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
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://<NSM\\_IP>/sdkapi/connectionlimitingpolicy](https://<NSM_IP>/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 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 from the list of country obtained using the URL: <a href="https://&lt;NSM_IP&gt;/sdkapi/connectionlimitingpolicy/countrylist">https://&lt;NSM_IP&gt;/sdkapi/connectionlimitingpolicy/countrylist</a>	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
status	Set to 1 if the operation was successful, -1 otherwise	number

## Example

### Request

PUT [https://<NSM\\_IP>/sdkapi/connectionlimitingpolicy/104](https://<NSM_IP>/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
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

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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

Field Name	Description	Data Type
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
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://<NSM\\_IP>/sdkapi/connectionlimitingpolicy/104](https://<NSM_IP>/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 Codes are 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://<NSM\\_IP>/sdkapi/connectionlimitingpolicy/104](https://<NSM_IP>/sdkapi/connectionlimitingpolicy/104)

#### 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	1901	Invalid Connection Limiting Policy Id/Connection Limiting Policy not visible in this domain

## Get the list of available country

This URL gets the list of available country

### 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://<NSM\\_IP>/sdkapi/connectionlimitingpolicy/countrylist](https://<NSM_IP>/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
visibleToChild	Policy visible to Child Domain	boolean
lastModTimestamp	Last Modified Timestamp of the policy	string

## Example

### Request

PUT [https://<NSM\\_IP>/sdkapi/sensor/1001/interface/105/connectionlimitingpolicy/101](https://<NSM_IP>/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 Codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404		Invalid Connection Limiting Policy Id

# 18

## Non Standard Ports Resource

### Contents

- *Add a Non Standard Port at Domain level*
- *Add a Non Standard Port at Sensor level*
- *Get Non Standard Ports at Domain level*
- *Get Non Standard Ports at Sensor level*
- *Delete a Non Standard Port at Domain level*
- *Delete a Non Standard Port at Sensor level*

---

### 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://<NSM\\_IP>/sdkapi/domain/0/nonstandardports](https://<NSM_IP>/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://<NSM\\_IP>/sdkapi/sensor/1002/nonstandardports](https://<NSM_IP>/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	domainId	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://<NSM\\_IP>/sdkapi/domain/0/nonstandardports](https://<NSM_IP>/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://<NSM\\_IP>/sdkapi/sensor/1002/nonstandardports](https://<NSM_IP>/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://<NSM\\_IP>/sdkapi/domain/101/nonstandardports?transport=TCP&nonStandardPortNumber=32](https://<NSM_IP>/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
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://<NSM\\_IP>/sdkapi/sensor/1002/nonstandardports?transport=UDP&nonStandardPortNumber=15](https://<NSM_IP>/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

# 19 SSL Key Resource

## Contents

- ▶ *Import SSL Key to the Manager*
- ▶ *Delete SSL Key*
- ▶ *Get SSL Keys*
- ▶ *Get the SSL configuration*
- ▶ *Update the SSL configuration*
- ▶ *Get the SSL configuration at the domain level*
- ▶ *Update the SSL configuration at the domain level*
- ▶ *Get the Resign Certificates on the Manager*
- ▶ *Regenerate the default re-sign certificate*
- ▶ *Export the public key of the active re-sign certificate*
- ▶ *Import a custom re-sign certificate*
- ▶ *Get all the trusted CA certificates on the Manager*
- ▶ *Get a single trusted CA certificate on the Manager*
- ▶ *Enable or Disable multiple trusted CA certificates*
- ▶ *Update the default trusted CA certificates*
- ▶ *Import a custom trusted CA certificate*
- ▶ *Delete multiple trusted CA certificates*
- ▶ *Get all the internal Web Server certificates*
- ▶ *Import custom internal Web Server certificate*
- ▶ *Delete multiple internal Web Server certificates*
- ▶ *Get all Inbound Proxy Rules*
- ▶ *Get Inbound Proxy Rule Details*
- ▶ *Add Inbound Proxy Rule*
- ▶ *Update Inbound Proxy Rule*
- ▶ *Delete multiple Inbound Proxy Rules*
- ▶ *Get the SSL configuration at the Sensor level*
- ▶ *Update the SSL configuration at the Sensor level*

---

## 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 BodyPart 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 UserCredential:

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 InputStream	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://<NSM\\_IP>/sdkapi/sensor/1001/action/sslkey](https://<NSM_IP>/sdkapi/sensor/1001/action/sslkey)

Payload:

```
PUT /sdkapi/sensor/1001/action/sslkey HTTP/1.1
NSM-SDK-API: OD1GRkEwQzEwMTE4QkFFRDc5MUUwMDk5OTg3OTI0NDk6MQ==
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
ÔrÝ?ü0¥ÿ<^}c, ¢eXœ^:4 Jhí2p♦rDYñÇÚd¶/Â¿i♦F~      ÆIc$4éá©ÿ_8Öø« C6Ô654iBq`J6?x ,*T2;qhã4îÂVµ-
Gfo9ŸCÖª,,i¹î      -Äë&1¹i,Ú<y i^i`Vö5U.kŸ$±Ñ g$zi0♦ wî [:...œ`Žiî' DÆ¾,xE7è♦L""t"á}ñÖùA+B6W!P!;Ð?
j*;G¾=X!Šls(♦i_œ8•-Ð"°fMiQ,"UEÔ `7»©2xN£o+¾$h;Öe ÆÄŸ0ÄÑÄ|ûNü,1"1Sö±œ'n`$èE`I#©ã¥?
$^hé_gÜî♦4L[gàî©:•œÖ òH%KÄiÄÖ"ÑÆ*¾²žØ|r-Ð,,“¶KŸ*¾♦k}ddZ;♦BÖ      ¥dK9ŸÐ¾ýîk""{Oj♦-¾
eýb3Öî&«PfTF      âê; ,4Ä{0ä!ÈŸ]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://<NSM\\_IP>/sdkapi/sensor/1001/action/sslkey/1002](https://<NSM_IP>/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 SSLDescriptor	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://<NSM\\_IP>/sdkapi/sensor/1001/action/sslkey](https://<NSM_IP>/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://<NSM\\_IP>/sdkapi/sensor/1002/sslconfiguration](https://<NSM_IP>/sdkapi/sensor/1002/sslconfiguration)

#### Response

```
{
  "enableSSL": true,
  "currentStatus": "Enabled[25000]",
```

```

    "enablePktLogging": false,
    "sslFlows": "25000",
    "sslCacheTimer": "5",
    "maxConcurrentTCPUDPFows": 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](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: <ul style="list-style-type: none"> <li>• DISABLED</li> <li>• INBOUND</li> <li>• OUTBOUND</li> <li>• PROXY_INBOUND (For Inbound Proxy)</li> <li>• PROXY_INBOUND_OUTBOUND (For Inbound and Outbound Proxy)</li> </ul>	string
anticipatedSSLTrafficUsage	Anticipated inbound SSL traffic usage. Values can be: <ul style="list-style-type: none"> <li>• VERY_LIGHT</li> <li>• LIGHT</li> <li>• MEDIUM</li> <li>• HEAVY</li> <li>• VERY_HEAVY</li> </ul>	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: <ul style="list-style-type: none"> <li>• Block Flow</li> <li>• Decrypt</li> </ul>	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

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: <ul style="list-style-type: none"> <li>DISABLED</li> <li>INBOUND</li> <li>OUTBOUND</li> <li>PROXY_INBOUND (For Inbound Proxy)</li> <li>PROXY_INBOUND_OUTBOUND (For Inbound and Outbound Proxy)</li> </ul>	string	Yes
anticipatedSSLTrafficUsage	Anticipated inbound SSL traffic usage. Values can be: <ul style="list-style-type: none"> <li>VERY_LIGHT</li> <li>LIGHT</li> <li>MEDIUM</li> <li>HEAVY</li> <li>VERY_HEAVY</li> </ul>	string	Yes
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: <ul style="list-style-type: none"><li>• Block Flow</li><li>• Decrypt</li></ul>	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](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

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	500	1001	Internal error

## Get the Resign Certificates on the Manager

This URL gets the resign 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	Resign 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
certType	Type of the certificate. It can be Default or Custom.	string

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/domain/sslconfiguration/resigncert](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": "Default"
    }
  ]
}
```

## Error Information

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](https://<NSM_IP>/sdkapi/domain/sslconfiguration/generateresigncert)

#### Response

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

### Error Information

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](https://<NSM_IP>/sdkapi/domain/sslconfiguration/exportresigncert)

### Response

<public key>

### Error Information

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 BodyPart objects	object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the ImportResignCert 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 InputStream	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](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

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	5301	Invalid FileType given for import : The file name does not have any extension
3	400	5301	Invalid FileType 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: <ul style="list-style-type: none"> <li>• VALID</li> <li>• EXPIRING</li> <li>• EXPIRED</li> </ul>	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](https://<NSM_IP>/sdkapi/domain/sslconfiguration/trustedcerts)

### Response

```
{
  "trustedCerts": [
    {
      "state": true,
      "alias": "IGC/A",
      "issuedBy": "IGC/A",
      "fileName": null,
      "certType": "Default",
      "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": "Default",
"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

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: <ul style="list-style-type: none"> <li>• VALID</li> <li>• EXPIRING</li> <li>• EXPIRED</li> </ul>	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](https://<NSM_IP>/sdkapi/domain/sslconfiguration/trustedcert?alias=EC-ACC)

#### Response

```
{
  "state": true,
  "alias": "EC-ACC",
  "issuedBy": "EC-ACC",
  "fileName": null,
  "certType": "Default",
  "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

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](https://<NSM_IP>/sdkapi/domain/sslconfiguration/updatetrustedcertstate)

#### Payload

```
{
  "alias": ["alias1", "alias2"],
  "state": true
}
```

#### Response

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

### Error Information

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](https://<NSM_IP>/sdkapi/domain/sslconfiguration/updatedefaulttrustedcerts)

### Response

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

## Error Information

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 BodyPart objects	object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the ImportResignCert 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 InputStream	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](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

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	5301	Invalid FileType given for import : The file name does not have any extension
3	400	5301	Invalid FileType 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](https://<NSM_IP>/sdkapi/domain/sslconfiguration/deletetrustedcerts)

#### Payload

```
{
  "alias": ["alias1", "alias2"]
}
```

#### Response

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

### Error Information

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	2203	Certs with following alias are not present : <alias_list>
3	400	2203	Following certs 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 internalWebServerCert	array

Details of objects in internalWebServerCerts:

Field Name	Description	Data Type
id	State of the cert file. If enabled or not.	boolean
alias	Alias for the SSL key	string
issuedBy	Name of the issuer	string
fileName	Cert file name	string
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: <ul style="list-style-type: none"><li>• VALID</li><li>• EXPIRING</li><li>• EXPIRED</li></ul>	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](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

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 BodyPart objects	object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the 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 IDs 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 InputStream	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
status	Status is the import was successful	boolean
comment	Comments regarding the import	string

## Example

### Request

PUT [https://<NSM\\_IP>/sdkapi/domain/sslconfiguration/importinternalwebservercerts](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

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	5301	Invalid FileType given for import : The file name does not have any extension
3	400	5301	Invalid FileType 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](https://<NSM_IP>/sdkapi/domain/sslconfiguration/deleteinternalwebservercerts)

#### Payload

```
{
  "alias": ["test.p12", "test1.p12"]
}
```

**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

---

## 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 SSLInboundProxyRule	array

Details of objects in sslInboundProxyRuleList:

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 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](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

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](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

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](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

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](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**

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](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: <ul style="list-style-type: none"> <li>• DISABLED</li> <li>• INBOUND</li> <li>• OTBOUND</li> </ul>	string
anticipatedSSLTrafficUsageAnticipated	Anticipated inbound SSL traffic usage. The values can be: <ul style="list-style-type: none"> <li>• VERY_LIGHT</li> <li>• LIGHT</li> <li>• MEDIUM</li> <li>• HEAVY</li> <li>• VERY_HEAVY</li> </ul>	string
maxFlow	Maximum flow allowed in the Sensor.	number
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: <ul style="list-style-type: none"> <li>• Block Flow</li> <li>• Decrypt</li> </ul>	number

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/sensor/1001/decryptionsettings](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

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: <ul style="list-style-type: none"> <li>DISABLED</li> <li>INBOUND</li> <li>OTBOUND</li> </ul>	string	Yes
anticipatedSSLTrafficUsage	Anticipated inbound SSL traffic usage. The values can be: <ul style="list-style-type: none"> <li>VERY_HIGH</li> <li>LIGHT</li> <li>MEDIUM</li> <li>HEAVY</li> <li>VERY_HEAVY</li> </ul>	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
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 <code>delete</code> 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: <ul style="list-style-type: none"> <li>Block Flow</li> <li>Decrypt</li> </ul>	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](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





# 20

## Rate Limiting Profiles Resource

### Contents

- [Add Rate Limiting Profile](#)
- [Update Rate Limiting Profile](#)
- [Delete Rate Limiting Profile](#)
- [Get Rate Limiting Profile](#)
- [Get Rate Limiting Profiles in a Domain](#)

### 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
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	RateLimiting 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

Field Name	Description	Data Type	Mandatory
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://<NSM\\_IP>/sdkapi/ratelimitingprofile/1003](https://<NSM_IP>/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	RateLimiting Profile Name is required
3	404	2403	Invalid Ratelimiting ProfileId / Profile not visible in this domain
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://<NSM\\_IP>/sdkapi/ratelimitingprofile/1001](https://<NSM_IP>/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
2	404	2403	Invalid Ratelimiting ProfileId / 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://<NSM\\_IP>/sdkapi/ratelimitingprofile/1003](https://<NSM_IP>/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 Ratelimiting ProfileId / 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://<NSM\\_IP>/sdkapi/domain/0/ratelimitingprofile](https://<NSM_IP>/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

# 21

## QoS Policy Resource

### Contents

- [Add QoS Policy](#)
- [Update QoS Policy](#)
- [Delete QoS Policy](#)
- [Get QoS Policy](#)
- [Get QoS Policies in a 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
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

Field Name	Description	Data Type	Mandatory
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://<NSM\\_IP>/sdkapi/qospolicy](https://<NSM_IP>/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

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
5	400	1804	Maximum of 10 Rule objects are allowed in each objectlist of an Advanced Firewall/QoS Policy
6	400	1813	Source/Destination objectlist is not provided
7	400	1814	Service/Application objectlist is not provided
8	400	1815	Time objectlist is not provided
9	400	1821	Either Application or Service objectlist can be defined in a MemberRule for an Advanced Firewall/QoS Policy
10	400	1832	SourceAddress and DestinationAddress objectlist 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	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 objectlist is not applicable for Classic QoS Policy
17	400	2711	Application objectlist is not applicable for Classic QoS Policy
18	400	2712	SourceAddress objectlist is not applicable for Classic QoS Policy
19	400	2713	SourceAddress objectlist is not applicable for Classic QoS Policy
20	400	2714	SourceUser objectlist 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 atleast one Service objectlist
25	400	2720	QoS Policy with the same name was defined
26	400	2721	QoS Policy provided is not upto date
27	400	2722	Policy Type cannot be modified
28	400	2723	Either Application or Service objectlist can be defined in a MemberRule 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	Lastest User that modified the policy	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
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://<NSM\\_IP>/sdkapi/qospolicy/183](https://<NSM_IP>/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 objectlist of an Advanced Firewall/QoS Policy
6	400	1813	Source/Destination objectlist is not provided
7	400	1814	Service/Application objectlist is not provided
8	400	1815	Time objectlist is not provided
9	400	1821	Either Application or Service objectlist can be defined in a MemberRule for an Advanced Firewall/QoS Policy
10	400	1832	SourceAddress and DestinationAddress objectlist 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 objectlist is not applicable for Classic QoS Policy
18	400	2711	Application objectlist is not applicable for Classic QoS Policy
19	400	2712	SourceAddress objectlist is not applicable for Classic QoS Policy
20	400	2713	SourceAddress objectlist is not applicable for Classic QoS Policy
21	400	2714	SourceUser objectlist is not applicable for Classic QoS Policy
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 atleast one Service objectlist

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
26	400	2720	QoS Policy with the same name was defined
27	400	2721	QoS Policy provided is not upto date
28	400	2722	Policy Type cannot be modified
29	400	2723	Either Application or Service objectlist can be defined in a MemberRule 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

DELETE https://<NSM\_IP>/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
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

Field Name	Description	Data Type
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://<NSM\\_IP>/sdkapi/qospolicy/183](https://<NSM_IP>/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
QoS PoliciesForDomainResponseList	List of QoS Policies defined in the domain	array

Details of object in QoS PoliciesForDomainResponseList:

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

Field Name	Description	Data Type
domainId	Domain ID	number
policyVersion	Policy version	number

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/domain/0/qospolicy](https://<NSM_IP>/sdkapi/domain/0/qospolicy)

#### Response

```
{
  "QoS Policies For Domain":
  [
    {
      "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

# 22

## Advanced Malware Policy Resource

### Contents

- ▶ *Add Advanced Malware Policy*
- ▶ *Update Malware Policy*
- ▶ *Delete Malware Policy*
- ▶ *Get Malware Policy*
- ▶ *Get Malware Policies in a Domain*
- ▶ *Get Default Protocol List*
- ▶ *Get Default Scanning Option Configuration List*
- ▶ *Get Blacklisted Hashes*
- ▶ *Get Whitelisted Hashes*
- ▶ *Action on Blacklisted Hash*
- ▶ *Action on Whitelisted Hash*
- ▶ *Action on Multiple Blacklisted Hashes*
- ▶ *Action on Multiple Whitelisted Hashes*
- ▶ *Remove All Blacklisted Hashes*
- ▶ *Remove All Whitelisted Hash*
- ▶ *Add FileHash to Blacklist or Whitelist*
- ▶ *Update Details of file hash*
- ▶ *Delete some file hashes from Blacklist or Whitelist*

---

## 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
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
addToBlackList	Add to blacklist 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://<NSM\\_IP>/sdkapi/malwarepolicy](https://<NSM_IP>/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": "Blacklist and Whitelist",
          "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",
        "addToBlackList": "DISABLED"
      }
    },
    {
      "fileType": "MS Office Files",
      "maximumFileSizeScannedInKB": 1024,
      "malwareEngines":
```

```
[
  {
    "name": "GTI File Reputation",
    "id": 1,
    "status": "DISABLED"
  },
  {
    "name": "Blacklist and Whitelist ",
    "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",
  "addToBlackList": "DISABLED"
}
},
{
  "fileType": "PDF Files",
  "maximumFileSizeScannedInKB": 1024,
  "malwareEngines":
  [
    {
      "name": "GTI File Reputation",
      "id": 1,
      "status": "UNCHECKED"
    },
    {
      "name": " Blacklist and Whitelist ",
      "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",
    "addToBlackList": "DISABLED"
  }
}
```



```
    },
    {
      "fileType": "Compressed Files",
      "maximumFileSizeScannedInKB": 5120,
      "malwareEngines":
      [
        {
          "name": "GTI File Reputation",
          "id": 1,
          "status": "DISABLED"
        },
        {
          "name": " Blacklist and Whitelist ",
          "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",
        "addToBlackList": "DISABLED"
      }
    },
    {
      "fileType": "Android Application Package",
      "maximumFileSizeScannedInKB": 2048,
      "malwareEngines":
      [
        {
          "name": "GTI File Reputation",
          "id": 1,
          "status": "CHECKED"
        },
        {
          "name": " Blacklist and Whitelist ",
          "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",
            "addToBlackList": "DISABLED"
        }
    },
    {
        "fileType": "Java Archive",
        "maximumFileSizeScannedInKB": 2048,
        "malwareEngines":
        [
            {
                "name": "GTI File Reputation",
                "id": 1,
                "status": "DISABLED"
            },
            {
                "name": " Blacklist and Whitelist ",
                "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",
            "addToBlackList": "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

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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
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
addToBlackList	Add to blacklist 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://<NSM\\_IP>/sdkapi/malwarepolicy/301](https://<NSM_IP>/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": " Blacklist and Whitelist",
        "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",
      "addToBlackList": "DISABLED"
    }
  },
  {
    "fileType": "MS Office Files",
    "maximumFileSizeScannedInKB": 1024,
    "malwareEngines":
    [
      {
        "name": "GTI File Reputation",
        "id": 1,
        "status": "DISABLED"
      },
      {
        "name": "Blacklist and Whitelist ",
        "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",
        "addToBlackList": "DISABLED"
    }
},
{
    "fileType": "PDF Files",
    "maximumFileSizeScannedInKB": 1024,
    "malwareEngines":
    [
        {
            "name": "GTI File Reputation",
            "id": 1,
            "status": "UNCHECKED"
        },
        {
            "name": " Blacklist and Whitelist ",
            "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",
        "addToBlackList": "DISABLED"
    }
},
{
    "fileType": "Compressed Files",
    "maximumFileSizeScannedInKB": 5120,
    "malwareEngines":
    [
        {
            "name": "GTI File Reputation",
            "id": 1,
            "status": "DISABLED"
        },
        {
            "name": " Blacklist and Whitelist ",
            "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",
    "addToBlackList": "DISABLED"
}
},
{
    "fileType": "Android Application Package",
    "maximumFileSizeScannedInKB": 2048,
    "malwareEngines":
    [
        {
            "name": "GTI File Reputation",
            "id": 1,
            "status": "CHECKED"
        },
        {
            "name": " Blacklist and Whitelist ",
            "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",
    "addToBlackList": "DISABLED"
}
},
{
    "fileType": "Java Archive",
    "maximumFileSizeScannedInKB": 2048,
    "malwareEngines":
    [
        {
            "name": "GTI File Reputation",
            "id": 1,
            "status": "DISABLED"
        },
        {
            "name": " Blacklist and Whitelist ",
            "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",
          "addToBlackList": "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 upto 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
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

DELETE [https://<NSM\\_IP>/sdkapi/malwarepolicy/301](https://<NSM_IP>/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	Lastest 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
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

Field Name	Description	Data Type
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

GET [https://<NSM\\_IP>/sdkapi/malwarepolicy/301](https://<NSM_IP>/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 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

## 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://<NSM\\_IP>/sdkapi/domain/0/malwarepolicy](https://<NSM_IP>/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 Codes are 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://<NSM\\_IP>/sdkapi/malwarepolicy/malwareprotocols](https://<NSM_IP>/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" / "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
addToBlackList	Add to blacklist can be "DISABLED" / "VERY_LOW" / "LOW" / "MEDIUM" / "HIGH" / "VERY_HIGH"	string

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/malwarepolicy/defaultscanningoptions](https://<NSM_IP>/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 Blacklisted Hashes

This URL gets the list of blacklisted hashes.

**Resource URL**

GET /advancedmalware/blacklistedhashes?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
blacklistedHashList	List of blacklisted hashes	array

Details of blacklistedHashList :

Field Name	Description	Data Type
filehash	File Hash	string
fileName	File Name	string
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://<NSM\\_IP>/sdkapi/advancedmalware/blacklistedhashes](https://<NSM_IP>/sdkapi/advancedmalware/blacklistedhashes)

### Response

```
{
  "blacklistedHashList": [
    {
      "fileHash": "1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa16", "fileName": "file1",
      "lastUpdated": "2018-01-17 20:30:34.0 (Administrator)"
      "comment": "Blacklisted based on user request "
    },
    {
      "fileHash": "1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa18", "fileName": "file2",
      "lastUpdated": "2018-01-17 20:35:36.0 (Administrator)"
      "comment": "Blacklisted 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 Whitelisted Hashes

This URL gets the list of whitelisted hashes.

### Resource URL

GET /advancedmalware/whitelistedhashes?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
whitelistedHashList	List of whitelisted hashes	array

Details of blacklistedHashList :

Field Name	Description	Data Type
filehash	File Hash	string
fileName	File Name	string
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://<NSM\_IP>/sdkapi/advancedmalware/whitelistedhashes

#### Response

```
{
  "whitelistedHashList": [{ {
    "fileHash": "1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa16", "fileName": "file1",
    "lastUpdated": "2018-01-17 20:30:34.0 (Administrator)"
    "comment": "Blacklisted 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 Blacklisted Hash

This URL moves the given hashes into whitelist.

### Resource URL

PUT /advancedmalware/blacklistedhashes/<hash>/takeaction/whitelist

### Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
hash	Hash	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	number

### Example

#### Request

PUT

[https://<NSM\\_IP>/sdkapi/advancedmalware/blacklistedhashes/1aaaaaaaaaaaaaaaaaaaaaaaaaaaa16/takeaction/whitelist](https://<NSM_IP>/sdkapi/advancedmalware/blacklistedhashes/1aaaaaaaaaaaaaaaaaaaaaaaaaaaa16/takeaction/whitelist)

#### 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 Whitelisted Hash

This URL moves the given hashes into blacklist.

### Resource URL

PUT /advancedmalware/whitelistedhashes/<hash>/takeaction/blacklist

### Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
hash	Hash	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	number

## Example

### Request

PUT [https://<NSM\\_IP>/sdkapi/advancedmalware/whitelistedhashes/1aaaaaaaaaaaaaaaaaaaaaaaaaaaa17/takeaction/blacklist](https://<NSM_IP>/sdkapi/advancedmalware/whitelistedhashes/1aaaaaaaaaaaaaaaaaaaaaaaaaaaa17/takeaction/blacklist)

### 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 Blacklisted Hashes

This URL moves the given hashes into blacklist.

## Resource URL

PUT /advancedmalware/blacklistedhashes/multipleHash/takeaction/whitelist

## 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/blacklistedhashes/multipleHash/takeaction/whitelist](https://<NSM_IP>/sdkapi/advancedmalware/blacklistedhashes/multipleHash/takeaction/whitelist)

### Payload

```
{
  "hashes": ["1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa16",
    "1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa17",
    "1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa18"]
}
```

### 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 Whitelisted Hashes

This URL moves the given hashes into blacklist.

### Resource URL

PUT </advancedmalware/whitelistedhashes/multipleHash/takeaction/blacklist>

### 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/whitelistedhashes/multipleHash/takeaction/blacklist](https://<NSM_IP>/sdkapi/advancedmalware/whitelistedhashes/multipleHash/takeaction/blacklist)

### Payload

```
{
  "hashes": [ "1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa16",
    "1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa17",
    "1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa18" ]
}
```

### 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

---

## Remove All Blacklisted Hashes

This URL to removes all the blacklisted hashes.

### Resource URL

PUT /advancedmalware/blacklistedhashes/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://<NSM\\_IP>/sdkapi/advancedmalware/blacklistedhashes/takeaction/removeall](https://<NSM_IP>/sdkapi/advancedmalware/blacklistedhashes/takeaction/removeall)

#### 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

---

## Remove All Whitelisted Hash

This URL removes all the whitelisted hashes.

### Resource URL

PUT /advancedmalware/whitelistedhashes/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://<NSM\\_IP>/sdkapi/advancedmalware/whitelistedhashes/takeaction/removeall](https://<NSM_IP>/sdkapi/advancedmalware/whitelistedhashes/takeaction/removeall)

#### 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

---

## Add FileHash to Blacklist or Whitelist

This URL adds the filehash to either the blacklist or whitelist.

### Resource URL

POST /advancedmalware?type=<hashtype>

## Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
type	Hashtype. Can be whitelist or blacklist.	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

## Response Parameters

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://<NSM\\_IP>/sdkapi/advancedmalware?type=blacklist](https://<NSM_IP>/sdkapi/advancedmalware?type=blacklist)

### Payload

```
{
  "fileHash": "1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa16",
  "fileName": "file1",
  "comment": "Blacklisted filehash "
}
```

### Response

```
{
  "createdResourceId": 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	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 whitelist/blacklist.
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 whitelisted or blacklisted filehash.

### Resource URL

PUT /advancedmalware?type=<hashtype>

### Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
type	Hashtype. Can be whitelist or blacklist.	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

### Response Parameters

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=blacklist](https://<NSM_IP>/sdkapi/advancedmalware?type=blacklist)

#### Payload

```
{
  "oldFileHash": "1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa16"
  "fileHash": "1aaaaaaaaaaaaaaaaaaaaaaaaaaaaa1116", "fileName": "file1",
  "comment": "updated Blacklisted filehash "
}
```

#### 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	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 whitelist/blacklist.
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 Blacklist or Whitelist

This URL deletes the Domain Name Exceptions specified in the stringList.

### Resource URL

DELETE /advancedmalware?type=blacklist

### Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
type	Hashtype. Can be whitelist or blacklist.	string	Yes

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. Set to 1 if the operation was successful.	number

### Example

#### Request

DELETE [https://<NSM\\_IP>/sdkapi/advancedmalware?type=blacklist](https://<NSM_IP>/sdkapi/advancedmalware?type=blacklist)

#### 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	500	1001	Internal Error Message: Internal Server Error



# 23

## File Reputation Resource

### Contents

- *Import GTI Configuration*
- *Import Whitelisted Fingerprints*
- *Delete Whitelisted Fingerprints*
- *Import Custom Fingerprints*
- *Delete Custom Fingerprints*
- *Manage Blacklist File Types*
- *Number of Fingerprints in use*
- *Get Blacklist File Types*
- *Get GTI File Types*
- *Get Severity for GTI*

---

## 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://<NSM\\_IP>/sdkapi/domain/0/filereputation/gti](https://<NSM_IP>/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 Whitelisted Fingerprints

This URL imports the list of Whitelisted Fingerprints to NSM

### Resource URL

PUT /domain/<domain\_id>/filereputation/whitelistedfingerprints

### 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 BodyParts Object	object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	It holds the .csv file as InputStream	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 update	number

## Example

### Request

PUT [https://<NSM\\_IP>/sdkapi/domain/0/filereputation/whitelistedfingerprints](https://<NSM_IP>/sdkapi/domain/0/filereputation/whitelistedfingerprints)

Payload:

```
NSM-SDK-API: RERFNUIyODFCQTdGRDM1MTRBQTA4QzAwQUUQ4MzAwQjE6MQ==
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/octet-stream
H;EÀ¶;Qoø*Ä"tTĐc[pbñšB=ã ¥Lh;bē²gà-*Æe#èÄñð-1€>!´Øùb&ck¾â•)9R-ë?0Ÿ;°]'3 9 ütþù9o\Đ...'ăž|}à!
ÿDŠ-Wâ+´ê-_"v`©BÈøe8ÄJ=L=ÖÝc¤¤Ä~^, tu$S?, Sámát6AÖôŽ¹%×L-•e«"Öô©Ä"âyò¤EI5)%5a7¥P¾E¤Öñú¤, xœÖEieÓ
°«Q{îB¤¤9-ëX+°%-îlÄ/9¤¤, ÑPð3; EZNq(é{h+ò7Y, á%«ÈvOâazîGöi"à`êÊâ*6ð)²BÈ,...KU[Šâ«FA^¤[gÝI"•F|ý
Qe¤'Y}, 6Ø³m
ÔQ£VÄ'°É«ûú >\'HĐ > ;¥žód», †, 3oÉæBðe, òöd[°Ýg-ðÈÝE
'0•+Ôµ(-Ú>îKSöð•¤eß>ß"Z612,"Äâ±ÄR+ |g_-¤P, ÝNÄú4jÆ;ÔO'îOi+^VaÄO±K8ØáTÜe¤ ^Y=êN¾?Eµİ-f
+Óo÷~uNvG=†•»ÈÈ.†EÓ->vðA?`°È-(Mc`U, ºtXÈ;+|) ¶úVE²"e¿Z-] `¤z-Jó\]Iðe¤Ô sµ `ÝT`°ý"...ÇiV^î^ÒÆü
¥}Tç÷îÖ,,>îcoM, 1>¾¤+ç]`£/ðÈ-}EÄ8NA¤j m...JÇÇc•î <¤eÚ+Ä¤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
3	500	1001	File hashes entries exceeded the maximum supported limit of 99,000

## Delete Whitelisted Fingerprints

This URL deletes the Whitelisted Fingerprints imported in NSM

### Resource URL

DELETE /domain/<domain\_id>/filereputation/whitelistedfingerprints

## Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	domainID	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://<NSM\\_IP>/sdkapi/domain/0/filereputation/whitelistedfingerprints](https://<NSM_IP>/sdkapi/domain/0/filereputation/whitelistedfingerprints)

### 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 Blacklisted Fingerprints to NSM

## 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 BodyParts Object	object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart [0]	It holds the .csv File as InputStream	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 from an update	number

## Example

### Request

PUT [https://<NSM\\_IP>/sdkapi/domain/0/filereputation/customfingerprints](https://<NSM_IP>/sdkapi/domain/0/filereputation/customfingerprints)

Payload:

```
NSM-SDK-API: OEZDNzAwNUQ3OTM2MjUzM0I3QTBREQ4MENFMzExMTM6MQ==
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/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
3	500	1001	File hashes entries exceeded the maximum supported limit of 99,000

## Delete Custom Fingerprints

This URL deletes the Custom Fingerprints imported in NSM

### Resource URL

DELETE /domain/<domain\_id>/filereputation/customfingerprints

### Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	DomainID	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://<NSM\\_IP>/sdkapi/domain/0/filereputation/customfingerprints](https://<NSM_IP>/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 Blacklist 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	DomainID	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

PUT [https://<NSM\\_IP>/sdkapi/domain/0/filereputation/filetypes](https://<NSM_IP>/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 Whitelisted Fingerprints in use

**Resource URL**

GET /domain/<domain\_id>/filereputation/fingerprintscount

**Request Parameters**

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain	domainID	number	Yes

## Response Parameters

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

Field Name	Description	Data Type
WhitelistedFingerprintsCount	Number of Whitelisted Fingerprints in use	number
CustomFingerprintsCount	Number of Custom Fingerprints in use	number

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/domain/0/filereputation/fingerprintscount](https://<NSM_IP>/sdkapi/domain/0/filereputation/fingerprintscount)

### Response

```
{
  "WhitelistedFingerprintsCount": 0,
  "CustomFingerprintsCount": 10
}
```

## 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

## Get Blacklist File Types

This URL provides the Blacklist File Types.

### Resource URL

GET [/domain/<domain\\_id>/filereputation/filetypes](#)

### Request Parameters:

URL parameters:

Field Name	Description	Data Type	Mandatory
domain_id	DomainID	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://<NSM\\_IP>/sdkapi/domain/0/filereputation/filetypes](https://<NSM_IP>/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	DomainID	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](https://<NSM_IP>/sdkapi/domain/0/filereputation/gti/filetypes)

#### Response

```
{  
  "fileFormat":  
    [  
      "apk",  
      "cpl",  
      "drv",  
      "exe",  
      "ocx",  
    ]  
}
```

```

    "pdf",
    "scr",
    "sys"
  ]
}
```

### 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

## 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	DomainID	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](https://<NSM_IP>/sdkapi/domain/0/filereputation/gti)

#### Response

```

{
  "inheritSettings": false,
  "Sensitivity": "VERY_LOW"
}
```

### 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

# 24 Alert Relevance Resource

## Contents

- [Update Alert Relevance](#)
- [Get Alert Relevance](#)

---

## Update Alert Relevance

This URL enables or disables Alert Relevance on NSM

### 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](https://<NSM_IP>/sdkapi/alertrelevance)

Payload:

```
{
  "isEnabled":true
}
```

#### Response

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

---

## Get Alert Relevance

This URL gets the current status of Alert Relevance on NSM

### 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://<NSM\\_IP>/sdkapi/alertrelevance](https://<NSM_IP>/sdkapi/alertrelevance)

#### Response

```
{
  "isEnabled":true
}
```

# 25

## Manage Import Resource

### Contents

- ▶ *Automatic Botnet File Download to Manager*
- ▶ *Manual Botnet File Import to Manager*
- ▶ *Manual Signature Set Import to Manager*
- ▶ *Manual Device Software Import to Manager*
- ▶ *Get the Device Softwares Available in the Server*
- ▶ *Manual Gateway Anti-Malware File Import to Manager*
- ▶ *Download the Device Software from the Server*
- ▶ *Get all the Device Software Available in the Server*

---

## Automatic Botnet File Download to Manager

This URL automatically downloads the latest Botnet file from Update Server to 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://<NSM\\_IP>/sdkapi/botnetdetectors/import/automatic](https://<NSM_IP>/sdkapi/botnetdetectors/import/automatic)

#### 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

## Manual Botnet File Import to Manager

This URL imports the Botnet file manually to Manager

### Resource URL

PUT /botnetdetectors/import/manual

### Request Parameters

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
MultiPart	Holds the BodyPart Objects	object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the FileFormat object	application/json object	Yes

Details of FileFormat:

Field Name	Description	Data Type	Mandatory
fileName	Name of the file	string	Yes
type	FileType should be "ZIP"	string	Yes

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
BodyPart[1]	Holds the File as InputStream	application/octet-stream	Yes

Details of .ZIP File:

Field Name	Description	Data Type	Mandatory
File	BotnetFile 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://<NSM\\_IP>/sdkapi/botnetdetectors/import/manual](https://<NSM_IP>/sdkapi/botnetdetectors/import/manual)

Payload:

```
NSM-SDK-API: QkI2Q0Y4Njg5NzUzNkY0Rtc5Qjc5NUJCRUFRCRUZEOM6MQ==
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": "d37a91be6f92f2620bf0bdf0bdba985a2eeced94", "file-length":
229869, "iv": "D+grgU2y12NHI/Oft8LaRVzP0an/1Fwin8TWhuGIS4aQYfjBhZEqLTzmUGxYjePyPC+v6fQoDfEp
\nT5qHAaZX4xn5blgdeR9iQgIx9mui2hkHed2zxaLwzzS/1mWOYbvoK04DPxYpT3UdDFxhe5nd8PPI
\nCGkDMExlmo2OwHjxiuUIwOOZfGEEA1SVHf8DiGKsmv25WVjF7LsTndRpeksyWyQX1/WESlnc+Vke
\nOaJK6l4DBCfzror7GuFADOKIPcGeZzgUCn/EMYfG/QhFw2vfu+OVub4f6qJZB6fDBn1li8KL+DQ5\niDCI/
Gq6zCIGksHPFJ9W+RN1RdlKVIkATdkkQQ==\n", "version": 31.0, "key":
"sFXb40h4vS6dWlaynBPdojhuXJDv9WoN1Jh0ts5+G9x9siDy/
tMwGo9U8pxoLveHJKu7mspI5nL5\nxFI8rR8EMzHjdeO9c9qMs/
x6djhKpDn8LQDQT03zdIW5QXwt5uA2tByLAOoKK5LKsveApJzqJMGw\nnu/
20sgvouKBLESGVE1WTZlrlRWC6JPPQ516ZzkW4kkjtcqGbgSnATipJmyKD2a5sAztXpp7vpNOrK
\nGUHH8jViWzgwzlgW/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 sigset file manually to Manager

### Resource URL

PUT /signatureset/import/manual

## Request Parameters

Payload Request Parameters:

Field Name	Description	Data Type	Mandatory
MultiPart	Holds the BodyPart Objects	object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the FileFormat object	application/json object	Yes

Details of FileFormat:

Field Name	Description	Data Type	Mandatory
fileName	Name of the file	string	Yes
type	FileType can be "JAR""IVU"	string	Yes

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
BodyPart1]	Holds the File as InputStream	application/octet-stream	Yes

Details of .JAR/.IVU File:

Field Name	Description	Data Type	Mandatory
File	Sigset 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://<NSM\\_IP>/sdkapi/signatureset/import/manual](https://<NSM_IP>/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?ú0¥ÿ<^>c, ¢eXœ^:4 Jhí2p♦rDYñÇÚd¶/Â¿i♦F~      ¤IcS%éá©ÿ_8Öø« C6Ô654iBg`J6?
x,*T2;qhã4iÁVµ~Gfo9ŸCÔª,i¹İ      -Äë&1¹i,Ú<yì^i`Vô5U.kŸ$±Ñ g$zi0♦wI [:...
œ`Žii' DEª, xE7è♦L"t"á)ñÖùA+B6W|P!;Ð?j*;G% =X|Šls (♦i_œ8•-Ð"°fMiQ,°UEÔ`7»©2xNŁo+¼$H;ÖeÆÄŸ0ÄÑÄ|ûNü,
```



```
1"1Sô±æ'n`$èÈ`I#@ã¥?.$^hé_gÛÎ4L[gâi@:•œÔ òH%KÃiÃÔ"ÑÆ*4²žØ|r-È,, "ŒKY*¥-k}ddZ;BÔ
¥dK9¥Ð¥ýîk`{Oj- ¥Eýb3Ôî&«PfTF âê; ,4Â{0ä!ÈÝ]ðä["ç1•!;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 format
3	400	3004	Specified Sigset version is not supported or EMS already has this update version
4	400	3005	Invalid Sigset 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 BodyPart Objects	object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the FileFormat object	application/json object	Yes

Details of FileFormat:

Field Name	Description	Data Type	Mandatory
fileName	Name of the file	string	Yes
type	FileType should be "JAR"	string	Yes

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
BodyPart1]	Holds the File as InputStream	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 update	number

### Example

#### Request

PUT [https://<NSM\\_IP>/sdkapi/devicesoftware/import/manual](https://<NSM_IP>/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
ÔrÝ?ü0¥ÿ<^}c, ¢eXœ^:4 JhÍ2µ♦rDYñÇÜd¶/Ã¿i♦F~      ÆIc$%éá©ÿ_8Öø« C6Ô654iBg`J6?
x,*T2;qhã4îÂVµ-Gfo9ŸCÒª,,i¹î      -Áë&1¹i,Ú<yî^î`Vö5U.kÝ$±Ñ g$Zi0♦wî [:...
œ`Žii'DE%,xœ7ë♦L``t"á)ñõùA+B6W|P!;Ð?j*;G%=X;Š1s(♦i_œ8-`Ð""fMîQ,"UEÔ`7»©2xN£ot%$h;öeÆÄŸ0ÄÑÄ;ûNü,
1"1Sö±œ'n`$èE`I#@ã¥?.$^hé_gÜî♦4L[gãî©:•œÔ òH%KÄiÄÖ"NÆ*¼?žØ|r-Ð,, "¶K¥*¼-♦k}ddZ;♦BÔ
¥dK9¥Ð%ýîk"{Oj♦- %œýb3Ôİs«PfTF      âê;,4Ä{0ä!ÈŸ]ðä["¿l•!;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 Softwares Available in the Server

This URL gets the Device softwares 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 softwares present in the Manager	Array
availableVersions	Device softwares available in the server for download	Array

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/devicesoftware/versions](https://<NSM_IP>/sdkapi/devicesoftware/versions)

### Response

```
{
  "downloadedVersions":
  [
    {
      "model": "IPS-VM600",
      "versions":
      [
        "8.2.7.11"
      ]
    },
    {
      "model": "M-2950",
      "versions":
      [
        "8.0.2.26"
      ]
    }
  ],
  "availableVersions":
  [
    {
      "model": "M-3030",
      "versions":
      [
        "8.2.3.12",
        "8.1.3.43",
        "8.1.3.5"
      ]
    },
    ...
  ]
}
```

## 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

## 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 BodyPart Objects	object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the FileFormat object	application/json object	Yes

Details of FileFormat:

Field Name	Description	Data Type	Mandatory
fileName	Name of the file	string	Yes
type	FileType should be "UPD"	string	Yes

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
BodyPart1]	Holds the File as InputStream	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](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	GAM 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](https://<NSM_IP>/sdkapi/devicesoftware/import/automatic)

### Request

Payload:

```
{
  'model' : 'M-3050',
  'version' : '8.2.3.12'
}
```

### 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

### Example

PUT [https://<NSM\\_IP>/sdkapi/devicesoftware/versions](https://<NSM_IP>/sdkapi/devicesoftware/versions)

### Response

```
{
  "downloadedVersions":
  [
    {
      "model": "IPS-VM600",
```

```
      "versions":
      [
        "8.2.7.11"
      ]
    },
    {
      "model": "M-2950",
      "versions":
      [
        "8.0.2.26"
      ]
    }
  ],
  "availableVersions":
  [
    {
      "model": "M-3030",
      "versions":
      [
        "8.2.3.12",
        "8.1.3.43",
        "8.1.3.5"
      ]
    }, ...
  ]
}
```

### 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





# 26

## IP Reputation Resource

### Contents

- [Update IP Reputation setting at Domain Level](#)
- [Get IP Reputation setting at Domain Level](#)

### Update IP Reputation setting at Domain Level

This URL updates IP Reputation setting at the domain level

#### Resource URL

PUT /domain/<domain\_id>/ipreputation

#### Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
domain_id	Domain Id	number	Yes

Payload Parameters:

Field Name	Description	Data Type	Mandatory
IPReputationElementForDomain	Object that contains the details of the field to be sent	object	Yes

Details of fields in IPReputationElementForDomain :

Field Name	Description	Data Type	Mandatory
augmentSmartBlocking	Use IP reputation to augment SmartBlocking decisions	boolean	Yes
whiteListAllInternalIPAddr	Exclude hosts from the lookup process (IP reputation will not be queried for whitelisted hosts)	boolean	Yes
inheritCIDRExclusionList	Inherit CIDR Exclusion list from GTI Participation Page	boolean	Yes
queriedProtocolsList	Supported protocol list	array	No
whitelistedProtocolsList	Whitelisted protocol list	array	No
whiteListedNetworkList	Exclude these networks from the lookup process (IP reputation will not be queried for whitelisted networks)	array	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 update	number

## Example

### Request

PUT [https://<NSM\\_IP>/sdkapi/domain/0/ipreputation](https://<NSM_IP>/sdkapi/domain/0/ipreputation)

### Payload

```
{
  "augmentSmartBlocking": true,
  "whiteListAllInternalIPAddr": false,
  "inheritCIDRExclusionList": false,
  "queriedProtocolsList":
  [
    "Point-to-Point Tunneling Protocol",
    "Ident Protocol ",
    "WINS",
    "Post Office Protocol",
    "Kerberos",
    "Real Time Streaming Protocol",
    "Remote EXEC",
    "CVS",
    "Remote Desktop Protocol",
    "RADIUS Accounting",
    "Telnet Protocol",
    "Socks Protocol",
    "Line Printer Daemon Protocol",
    "Session Initiation Protocol",
    "Universal Plug and Play",
    "L3 ACL for TCP",
    "Network File System",
    "Network News Transfer Protocol",
    "Finger Protocol",
    "Tabular DataStream Protocol",
    "Remote Shell",
    "Internet Control Message Protocol",
    "X Font Service Protocol",
    "MS SQL Server Resolution Service",
    "Simple Mail Transfer Protocol",
    "Secure Socket Layer",
    "L3 ACL for UDP",
    "Light-weight Directory Access Protocol",
    "Oracle TNS Protocol",
    "Instant Messenger And P2P Applications",
    "Secure Shell Protocol",
    "RTSP DATA",
    "HyperText Transfer Protocol",
    "FTP DATA",
    "SIP DATA",
    "H225",
    "Internet Security Association Key Management Protocol",
    "L3 ACL for ICMP",
    "Bootstrap Protocol and Dynamic Host Configuration Protocol",
    "Internet Relay Chat Protocol",
    "Internet Message ACCESS Protocol",
    "Network Time Protocol",
    "Known Multimedia and Encrypted Channels",
    "Remote Sync Protocol",
    "Remote Authentication Dial In User Service",
    "Windows Bind Shell",
    "Simple Network Management Protocol ",
    "Back Orifice",
    "File Transfer Protocol",
    "NETBIOS Name Service",
  ]
}
```

```
        "RPC Portmapper Protocol",
        "MMS",
        "Trivial File Transfer Protocol",
        "NETBIOS Session Service",
        "Internet Control Message Protocol Version 6",
        "Remote Procedure Call Protocol",
        "Remote Login"
    ],
    "whitelistedProtocolsList":
    [
        "CDE dtspcd Protocol",
        "MySQL",
        "DCE RPC Protocol"
    ],
    "whiteListedNetworkList":
    [
        "1.0.0.0/8",
        "2.0.0.0/8"
    ]
}
```

### 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	400	1701	Invalid CIDR notation

## Get IP Reputation setting at Domain Level

This URL provides IP Reputation setting at the domain level

### Resource URL

GET /domain/<domain\_id>/ipreputation

### 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
IPReputationElementForDomain	Object that contains the details of the fields to be sent	object

Details of fields in IPReputationElementForDomain :

Field Name	Description	Data Type
augmentSmartBlocking	use IP reputation to augment SmartBlocking decisions	boolean
whiteListAllInternalIPAddr	Exclude hosts from the lookup process (IP reputation will not be queried for whitelisted hosts)	boolean
inheritCIDRExclusionList	Inherit CIDR Exclusion list from GTI Participation Page	boolean
queriedProtocolsList	Supported protocol list	array
whitelistedProtocolsList	Whitelisted protocol list	array
whiteListedNetworkList	Exclude these networks from the lookup process (IP reputation will not be queried for whitelisted networks)	array

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/domain/0/ipreputation](https://<NSM_IP>/sdkapi/domain/0/ipreputation)

### Response

```
{
  "augmentSmartBlocking": true,
  "whiteListAllInternalIPAddr": false,
  "inheritCIDRExclusionList": false,
  "queriedProtocolsList":
  [
    "Point-to-Point Tunneling Protocol",
    "Ident Protocol ",
    "WINS",
    "Post Office Protocol",
    "Kerberos",
    "Real Time Streaming Protocol",
    "Remote EXEC",
    "CVS",
    "Remote Desktop Protocol",
    "RADIUS Accounting",
    "Telnet Protocol",
    "Socks Protocol",
    "Line Printer Daemon Protocol",
    "Session Initiation Protocol",
    "Universal Plug and Play",
    "L3 ACL for TCP",
    "Network File System",
    "Network News Transfer Protocol",
    "Finger Protocol",
    "Tabular DataStream Protocol",
    "Remote Shell",
    "Internet Control Message Protocol",
    "X Font Service Protocol",
    "MS SQL Server Resolution Service",
    "Simple Mail Transfer Protocol",
    "Secure Socket Layer",
    "L3 ACL for UDP",
    "Light-weight Directory Access Protocol",
    "Oracle TNS Protocol",
    "Instant Messenger And P2P Applications",
    "Secure Shell Protocol",
    "RTSP DATA",
    "HyperText Transfer Protocol",
    "FTP DATA",
    "SIP DATA",
    "H225",
    "Internet Security Association Key Management Protocol",
    "L3 ACL for ICMP",
    "Bootstrap Protocol and Dynamic Host Configuration Protocol",
    "Internet Relay Chat Protocol",
  ]
}
```

```
        "Internet Message ACCESS Protocol",
        "Network Time Protocol",
        "Known Multimedia and Encrypted Channels",
        "Remote Sync Protocol",
        "Remote Authentication Dial In User Service",
        "Windows Bind Shell",
        "Simple Network Management Protocol ",
        "Back Orifice",
        "File Transfer Protocol",
        "NETBIOS Name Service",
        "RPC Portmapper Protocol",
        "MMS",
        "Trivial File Transfer Protocol",
        "NETBIOS Session Service",
        "Internet Control Message Protocol Version 6",
        "Remote Procedure Call Protocol",
        "Remote Login"
    ],
    "whitelistedProtocolsList":
    [
        "CDE dtspcd Protocol",
        "MySQL",
        "DCE RPC Protocol"
    ],
    "whiteListedNetworkList":
    [
        "1.0.0.0/8",
        "2.0.0.0/8"
    ]
}
```

### 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



# 27

## Malware Archive Resource

### Contents

- ▶ [Whitelist Malware Archive File](#)
- ▶ [Download Malware File](#)
- ▶ [Get List of Archived Malware Files](#)
- ▶ [Delete Malware Archive File](#)

---

### Whitelist Malware Archive File

This URL adds the filehash to the White 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 "WHITELIST"	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://<NSM\\_IP>/sdkapi/malwarearchive/action](#)

Payload:

```
{
  "fileHash": " 0bea3f79a36b1f67b2ce0f595524c77c",
  "action": "WHITELIST"
}
```

**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 filehash 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://<NSM\\_IP>/sdkapi/malwarearchive/download/0bea3f79a36b1f67b2ce0f595524c77c](https://<NSM_IP>/sdkapi/malwarearchive/download/0bea3f79a36b1f67b2ce0f595524c77c)

**Response**

```
{
  "byteStream": "TVqOAEAAAAEAAAA//
8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyB
wcm9ncmFtIHJlcXVpcmVzIE1pY3Jvc29mdCBXaW5kb3dzLg0KJAAAAAAAAABORQU8JgEtAAAAAABgwMAABQAALiWAgAA
AAAAwADAE8AQABYAOWADQETAdMBAAHAAQAAAACCCQAdhYAAAOdJgBiYVAdYsnoDNTQUB3bUAlSKElxDShJBAAFGAQAA
AAAAJoWCAAwHGWAAAAAAKIWGg"
}
```



## 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 filehash 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 NSM	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://<NSM\\_IP>/sdkapi/malwarearchive/list](https://<NSM_IP>/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 Codes are 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



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://<NSM\\_IP>/sdkapi/malwarearchive?filehash=0bea3f79a36b1f67b2ce0f595524c77c](https://<NSM_IP>/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 filehash value
3	400	3402	No file to delete



# 28

## Passive Device Profiling

### Contents

- ▶ *Get Passive Device Profiling setting at the domain level*
- ▶ *Update Passive Device Profiling setting at domain level*
- ▶ *Get Passive Device Profiling setting at sensor level*
- ▶ *Update Passive Device Profiling setting at sensor level*

### 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
unit	Profile Expiration duration unit, can be "MINUTES" / "HOURS"	string

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/domain/0/passivedeviceprofiling](https://<NSM_IP>/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 Codes are 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
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://<NSM\\_IP>/sdkapi/domain/0/passivedeviceprofiling](https://<NSM_IP>/sdkapi/domain/0/passivedeviceprofiling)

Payload

```
{
  "inheritSettingsfromIPSSettingsNode": true,
  "passiveDeviceProfilingSetting": {
    "profilingTechniques": {
      "DHCPEnableStatus": true,
```

```

    "TCPEnableStatus": true,
    "HTTPEnableStatus": false
  },
  "profileExpiration":
  {
    "duration": 30,
    "unit": "MINUTES"
  },
  "hostInactivityTimerInHrs": 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	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
4	400	3303	Profile Expiration value cannot be greater than Host Inactivity Timer
5	400	3304	Please enable atleast 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



Field Name	Description	Data Type
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
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 subinterfaces 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://<NSM\\_IP>/sdkapi/sensor/1001/passivedeviceprofiling](https://<NSM_IP>/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 Codes are 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
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 subinterfaces 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://<NSM\\_IP>/sdkapi/sensor/1001/passivedeviceprofiling](https://<NSM_IP>/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 atleast one Profiling Technique
6	400	3305	InterConnecting 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

# 29

## Alert Exception

### Contents

- [Add Alert Exception](#)
- [Get Alert Exception](#)
- [Get All Alert Exception](#)
- [Delete Alert Exception](#)

## 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 AttackId	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://<NSM\\_IP>/sdkapi/alertexception](https://<NSM_IP>/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
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 AttackId	string
sourceIp	IPV4/IPV6 address/"ANY"	string
destinationIp	IPV4/IPV6 address/"ANY"	string



Field Name	Description	Data Type
expiration	Expiration of the Exception	string
lastModified	Last Modified Time of the Alert Exception	string

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/alertexception/106](https://<NSM_IP>/sdkapi/alertexception/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 NSM

### 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 AlertException in the NSM	array

Details of alertExceptionDescriptorList:

Field Name	Description	Data Type
alertId	Unique Alert Id	number
attackId	Unique Hexadecimal AttackId	string
sourceIp	IPV4/IPV6 address/"ANY"	string
destinationIp	IPV4/IPV6 address/"ANY"	string

Field Name	Description	Data Type
expiration	Expiration of the Exception	string
lastModified	Last Modified Time of the Alert Exception	string

**Example****Request**

GET [https://<NSM\\_IP>/sdkapi/alertexception/list](https://<NSM_IP>/sdkapi/alertexception/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://<NSM\\_IP>/sdkapi/alertexception/106](https://<NSM_IP>/sdkapi/alertexception/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



# 30

## Global Auto Acknowledgment

### Contents

- [Configure Global Auto Ack Setting](#)
- [Get Global Auto Ack Setting](#)
- [Get attacks for rules configuration](#)
- [Get Global Auto Ack Rules](#)
- [Get Global Auto Ack Rule](#)
- [Create Global Auto Ack Rules](#)
- [Update Global Auto Ack Rules](#)

### 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 Acknowledgement	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://<NSM\\_IP>/sdkapi/globalautoack](https://<NSM_IP>/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 retrieve 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 Acknowledgement	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://<NSM\\_IP>/sdkapi/globalautoack](https://<NSM_IP>/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](https://<NSM_IP>/sdkapi/globalautoack/attacks/malware)

## Response

```
{
  [
    "attackId": "0x23323223"
    "attackName": "malwareBlacklistd"
  ]
}
```

## 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](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](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 URL is 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](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/&lt;rule\_id&gt;

**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](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

# 31

## Name Resolution Resource

### Contents

- *Update Name Resolution settings at domain level*
- *Get Name Resolution Configuration at Domain level*
- *Update Name Resolution settings at sensor level*
- *Get Name Resolution Configuration at Sensor level*

### 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://<NSM\\_IP>/sdkapi/domain/0/nameresolution](https://<NSM_IP>/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
5	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://<NSM\\_IP>/sdkapi/domain/0/nameresolution](https://<NSM_IP>/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 Codes are 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://<NSM\_IP>/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
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

Field Name	Description	Data Type
secondaryDNSServer	Secondary DNS server IP	string
refreshIntervalInHours	Refresh interval in hours, applicable only for NTBA device	number

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/sensor/1001/nameresolution](https://<NSM_IP>/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 Codes are returned by this URL:

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

# 32

## Device Resource

### Contents

- [Add Device](#)
- [Get Device](#)
- [Update Device](#)
- [Delete Device](#)
- [Get All Device](#)

## 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://<NSM\\_IP>/sdkapi/domain/0/device](https://<NSM_IP>/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
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 upto 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](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 DeviceId / 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
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://<NSM\\_IP>/sdkapi/domain/0/device/1006](https://<NSM_IP>/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 DeviceId / 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
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 upto 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://<NSM\\_IP>/sdkapi/domain/0/device/120](https://<NSM_IP>/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 NSM

### 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 Devices 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

Field Name	Description	Data Type
contactInformation	Contact Information	string
location	Device Location	string

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/domain/0/device](https://<NSM_IP>/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 Codes are returned by this URL:

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

# 33

## NTBA Resource

### Contents

- ▶ *Get NTBA Monitors*
- ▶ *Get Hosts Threat Factor*
- ▶ *Get Top URLs*
- ▶ *Get Top Zone URLs*
- ▶ *Get Top Host URLs*
- ▶ *Get Top URLs by Reputations*
- ▶ *Get URL Activity*
- ▶ *Get URLs by Category*
- ▶ *Get URLs for Category*
- ▶ *Get Top files*
- ▶ *Get Top zone files*
- ▶ *Get Top Host files*
- ▶ *Get File Activity*
- ▶ *Get External Hosts by Reputation*
- ▶ *Get New Hosts*
- ▶ *Get Active Hosts*
- ▶ *Get Top Hosts Traffic*
- ▶ *Get Application Traffic*
- ▶ *Get Application Profile*
- ▶ *Get Throughput Traffic*
- ▶ *Get Bandwidth Utilization*
- ▶ *Get Zone Traffic*
- ▶ *Get Active Services*
- ▶ *Get Host Active Services*
- ▶ *Get New Services*
- ▶ *Get Active Applications*
- ▶ *Get New Applications*
- ▶ *Get Host Active Applications*
- ▶ *Get Host Ports*

---

## 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 ntbas	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://<NSM\\_IP>/sdkapi/ntbamonitors](https://<NSM_IP>/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/{ntbald}/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 <ul style="list-style-type: none"><li>• LAST_MINUTE</li><li>• LAST_10_MINUTES</li><li>• LAST_HOUR</li><li>• LAST_24_HOURS</li><li>• CUSTOM Custom incase start and end time is provided</li></ul>	string	No
startTime	Start time in the format: yyyy-MMM-dd HH:mm	string	No
endTime	End time in the format: yyyy-MMM-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://<NSM\\_IP>/sdkapi/ntbamonitors/1006/hostsThreatFactor?  
timePeriod=CUSTOM&startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11](https://<NSM_IP>/sdkapi/ntbamonitors/1006/hostsThreatFactor?timePeriod=CUSTOM&startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11)

### 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 /ntbamonitor/{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 <ul style="list-style-type: none"> <li>• LAST_MINUTE</li> <li>• LAST_10_MINUTES</li> <li>• LAST_HOUR</li> <li>• LAST_24_HOURS</li> <li>• CUSTOM</li> </ul> Custom incase start and end time is provided	string	No
startTime	Start time in the format: yyyy-MMM-dd HH:mm	string	No
endTime	End time in the format: yyyy-MMM-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://<NSM\\_IP>/sdkapi/ntbamonitors/1006/topurls?timePeriod=CUSTOM&startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11](https://<NSM_IP>/sdkapi/ntbamonitors/1006/topurls?timePeriod=CUSTOM&startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11)

### 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/{ntbald}/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://<NSM\\_IP>/sdkapi/ntbamonitors/1006/topzoneurls/9898](https://<NSM_IP>/sdkapi/ntbamonitors/1006/topzoneurls/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
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/{ntbald}/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

GET [https://<NSM\\_IP>/sdkapi/ntbamonitors/1006/tophosturls/9](https://<NSM_IP>/sdkapi/ntbamonitors/1006/tophosturls/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 /ntbamonitor/{ntbald}/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 <ul style="list-style-type: none"> <li>• LAST_MINUTE</li> <li>• LAST_10_MINUTES</li> <li>• LAST_HOUR</li> <li>• LAST_24_HOURS</li> <li>• CUSTOM</li> </ul> Custom incase start and end time is provided	string	No

Field Name	Description	Data Type	Mandatory
startTime	Start time in the format: yyyy-MMM-dd HH:mm	string	No
endTime	End time in the format: yyyy-MMM-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://<NSM\\_IP>/sdkapi/ntbamonitor/1006/topurlsbyreputation?timePeriod=CUSTOM&startTime=2012-APR-20](https://<NSM_IP>/sdkapi/ntbamonitor/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 urlId.

### Resource URL

GET /ntbamonitor/{ntbald}/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 <ul style="list-style-type: none"> <li>• LAST_MINUTE</li> <li>• LAST_10_MINUTES</li> <li>• LAST_HOUR</li> <li>• LAST_24_HOURS</li> <li>• CUSTOM</li> </ul> Custom incase start and end time is provided	string	No
startTime	Start time in the format: yyyy-MMM-dd HH:mm	string	No
endTime	End time in the format: yyyy-MMM-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://<NSM\_IP>/sdkapi/ntbamonitors/1006/showurlactivity /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/{ntbald}/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

Field Name	Description	Data Type	Mandatory
timePeriod	Duration : can be <ul style="list-style-type: none"> <li>• LAST_MINUTE</li> <li>• LAST_10_MINUTES</li> <li>• LAST_HOUR</li> <li>• LAST_24_HOURS</li> <li>• CUSTOM</li> </ul> Custom incase start and end time is provided	string	No
startTime	Start time in the format: yyyy-MMM-dd HH:mm	string	No
endTime	End time in the format: yyyy-MMM-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://<NSM\\_IP>/sdkapi/ntbamonitors/1006/topurlsbycategory?timePeriod=CUSTOM&startTime=2012-APR-20](https://<NSM_IP>/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



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 URLs for Category

This URL gets the list of urls for category.

### Resource URL

GET /ntbamonitor/{ntbald}/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 <ul style="list-style-type: none"><li>• LAST_MINUTE</li><li>• LAST_10_MINUTES</li><li>• LAST_HOUR</li><li>• LAST_24_HOURS</li><li>• CUSTOM</li></ul> Custom incase start and end time is provided	string	No
startTime	Start time in the format: yyyy-MMM-dd HH:mm	string	No
endTime	End time in the format: yyyy-MMM-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://<NSM\_IP>/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 topfiles.

### Resource URL

GET /ntbamonitors/{ntbald}/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

Field Name	Description	Data Type	Mandatory
timePeriod	Duration : can be <ul style="list-style-type: none"><li>• LAST_MINUTE</li><li>• LAST_10_MINUTES</li><li>• LAST_HOUR</li><li>• LAST_24_HOURS</li><li>• CUSTOM</li></ul> Custom incase start and end time is provided	string	No
startTime	Start time in the format: yyyy-MMM-dd HH:mm	string	No
endTime	End time in the format: yyyy-MMM-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://<NSM\\_IP>/sdkapi/ntbamonitors/1006/topfiles?timePeriod=CUSTOM&startTime=2012-APR-20](https://<NSM_IP>/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 topfiles.

### Resource URL

GET /ntbamonitors/{ntbald}/topzonefiles/<zone\_id

### Request Parameters

Field Name	Description	Data Type	Mandatory
ntbaId	NTBA monitor Id	number	Yes
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://<NSM\\_IP>/sdkapi/ntbamonitors/1006/topzonefiles/9](https://<NSM_IP>/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

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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 /ntbamonitor/{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 <ul style="list-style-type: none"><li>• LAST_MINUTE</li><li>• LAST_10_MINUTES</li><li>• LAST_HOUR</li><li>• LAST_24_HOURS</li><li>• CUSTOM</li></ul> Custom incase start and end time is provided	string	No
startTime	Start time in the format: yyyy-MMM-dd HH:mm	string	No
endTime	End time in the format: yyyy-MMM-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

Field Name	Description	Data Type
srcZone	Source Zone	string
destEndpoint	Dest Endpoint	string
destUser	Dest User	string
destZone	Dest Zone	string
action	Action	string
lastAccessed	Last Accessed	string

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/ntbamonitors/1006/fileactivity/8389181?timePeriod=CUSTOM&startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11](https://<NSM_IP>/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/{ntbald}/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 <ul style="list-style-type: none"><li>• LAST_MINUTE</li><li>• LAST_10_MINUTES</li><li>• LAST_HOUR</li><li>• LAST_24_HOURS</li><li>• CUSTOM</li></ul> Custom incase start and end time is provided	string	No
startTime	Start time in the format: yyyy-MMM-dd HH:mm	string	No
endTime	End time in the format: yyyy-MMM-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://<NSM\\_IP>/sdkapi/ntbamonitor/1006/topexthostsbyreputation?timePeriod=CUSTOM&startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11](https://<NSM_IP>/sdkapi/ntbamonitor/1006/topexthostsbyreputation?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
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 /ntbamonitor/{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://<NSM\\_IP>/sdkapi/ntbamonitor/1006/newhosts](https://<NSM_IP>/sdkapi/ntbamonitor/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
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 /ntbamonitor/{ntbald}/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 <ul style="list-style-type: none"><li>• LAST_MINUTE</li><li>• LAST_10_MINUTES</li><li>• LAST_HOUR</li><li>• LAST_24_HOURS</li><li>• CUSTOM</li></ul> Custom incase start and end time is provided	string	No
startTime	Start time in the format: yyyy-MMM-dd HH:mm	string	No
endTime	End time in the format: yyyy-MMM-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 activeHosts :

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://<NSM\\_IP>/sdkapi/ntbamonitor/1006/activehosts?timePeriod=CUSTOM&startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11](https://<NSM_IP>/sdkapi/ntbamonitor/1006/activehosts?timePeriod=CUSTOM&startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11)

#### 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 /ntbamonitor/{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
startTime	Start time in the format: yyyy-MMM-dd HH:mm	string	No

Field Name	Description	Data Type	Mandatory
endTime	End time in the format: yyyy-MMM-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 hostsTraffic:

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://<NSM\\_IP>/sdkapi/ntbamonitor/1006/tophoststraffic?startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11](https://<NSM_IP>/sdkapi/ntbamonitor/1006/tophoststraffic?startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11)

#### 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 /ntbamonitor/{ntbald}/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-MMM-dd HH:mm	string	No
endTime	End time in the format: yyyy-MMM-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://<NSM\_IP>/sdkapi/ntbamonitor/1006/applicationtraffic?startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11

## 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 /ntbamonitor/{ntbaId}/ applicationtraffic/profile/{appld}? 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-MMM-dd HH:mm	string	No
endTime	End time in the format: yyyy-MMM-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

Field Name	Description	Data Type
inboundTraffic	Inbound traffic	string
outboundTraffic	outbound traffic	string
totalTraffic	Total traffic	string
noOfConnections	Number of connection	number

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/ntbamonitor/1006/applicationprofile/profile/131231?startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11](https://<NSM_IP>/sdkapi/ntbamonitor/1006/applicationprofile/profile/131231?startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11)

#### 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/{ntbald}/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-MMM-dd HH:mm	string	No
endTime	End time in the format: yyyy-MMM-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://<NSM\_IP>/sdkapi/ntbamonitors/1006/throughputtraffic?startTime=2012-APR-20  
12:15&endTime=2012-APR-20 12:11

### 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
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 Bandwidth Utilization**

This URL gets the details of bandwidthutilization

**Resource URL**

GET /ntbamonitors/{ntbald}/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	InterfaceId	number
linkSpeed	Link Speed	string
inbound	Inbound traffic percentage	string
outbound	Outbound traffic percentage	string

**Example****Request**

GET [https://<NSM\\_IP>/sdkapi/ntbamonitors/1006/bandwidthutilization](https://<NSM_IP>/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 /ntbamonitor/{ntbald}/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://<NSM\\_IP>/sdkapi/ntbamonitors/1006/zonetraffic](https://<NSM_IP>/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/{ntbald}/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
timePeriod	Duration : can be <ul style="list-style-type: none"><li>• LAST_MINUTE</li><li>• LAST_10_MINUTES</li><li>• LAST_HOUR</li><li>• LAST_24_HOURS</li><li>• CUSTOM</li></ul> Custom incase start and end time is provided	string	No
startTime	Start time in the format: yyyy-MMM-dd HH:mm	string	No
endTime	End time in the format: yyyy-MMM-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	Lastseen	string

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/ntbamonitors/1006/activeservices?timePeriod=CUSTOM&startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11](https://<NSM_IP>/sdkapi/ntbamonitors/1006/activeservices?timePeriod=CUSTOM&startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11)

### 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

## Get Host Active Services

This URL gets the list of host active services.

### Resource URL

GET /ntbamonitor/{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 <ul style="list-style-type: none"> <li>• LAST_MINUTE</li> <li>• LAST_10_MINUTES</li> <li>• LAST_HOUR</li> <li>• LAST_24_HOURS</li> <li>• CUSTOM</li> </ul> Custom incase start and end time is provided	string	No
startTime	Start time in the format: yyyy-MMM-dd HH:mm	string	No
endTime	End time in the format: yyyy-MMM-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
protocol	Protocol	string
lastSeen	Lastseen	string

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/ntbamonitor/1006/tophostactiveservices/9?timePeriod=CUSTOM&startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11](https://<NSM_IP>/sdkapi/ntbamonitor/1006/tophostactiveservices/9?timePeriod=CUSTOM&startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11)

#### 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 /ntbamonitor/{ntbald}/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	Lastseen	string

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/ntbamonitors/1006/newservices](https://<NSM_IP>/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/{ntbald}/activeapplications? 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 <ul style="list-style-type: none"><li>• LAST_MINUTE</li><li>• LAST_10_MINUTES</li><li>• LAST_HOUR</li><li>• LAST_24_HOURS</li><li>• CUSTOM</li></ul> Custom incase start and end time is provided	string	No
startTime	Start time in the format: yyyy-MMM-dd HH:mm	string	No
endTime	End time in the format: yyyy-MMM-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	Lastseen	string

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/ntbamonitors/1006/activeapplications?  
timePeriod=CUSTOM&startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11](https://<NSM_IP>/sdkapi/ntbamonitors/1006/activeapplications?timePeriod=CUSTOM&startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11)

### 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

## Get New Applications

This URL gets the list of new applications.

### Resource URL

GET /ntbamonitors/{ntbald}/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	Lastseen	string

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/ntbamonitors/1006/newapplications](https://<NSM_IP>/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 /ntbamonitor/{ntbald}/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-MMM-dd HH:mm	string	No
endTime	End time in the format: yyyy-MMM-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	Lastseen	string

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/ntbamonitors/1006/tophostactiveapplications/9?timePeriod=CUSTOM&startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11](https://<NSM_IP>/sdkapi/ntbamonitors/1006/tophostactiveapplications/9?timePeriod=CUSTOM&startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11)

### 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/{ntbald}/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 <ul style="list-style-type: none"><li>• LAST_MINUTE</li><li>• LAST_10_MINUTES</li><li>• LAST_HOUR</li><li>• LAST_24_HOURS</li><li>• CUSTOM</li></ul> Custom incase start and end time is provided	string	No
startTime	Start time in the format: yyyy-MMM-dd HH:mm	string	No
endTime	End time in the format: yyyy-MMM-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	Lastseen	string

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/ntbamonitor/1006/tophostports/9?timePeriod=CUSTOM&startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11](https://<NSM_IP>/sdkapi/ntbamonitor/1006/tophostports/9?timePeriod=CUSTOM&startTime=2012-APR-20 12:15&endTime=2012-APR-20 12:11)

### 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

# 34 Endpoint Executables Resource

## Contents

- *Get Endpoint Intelligence*
- *Get Executable Information*
- *Get Endpoints*
- *Get Applications*
- *Get Events*
- *Action on Hash*

---

## 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 <ul style="list-style-type: none"><li>• any</li><li>• blacklisted</li><li>• whitelisted</li><li>• unclassified</li></ul> Default: any	string	No

Field Name	Description	Data Type	Mandatory
classificationtype	Classification Type <ul style="list-style-type: none"> <li>• high</li> <li>• any</li> </ul> Default: any	string	No
duration	Duration <ul style="list-style-type: none"> <li>• LAST_5_MINUTES</li> <li>• LAST_1_HOUR</li> <li>• LAST_6_HOURS</li> <li>• LAST-12_HOURS</li> <li>• LAST_24_HOURS</li> <li>• LAST_48_HOURS</li> <li>• LAST_7_DAYS</li> <li>• LAST_14_DAYS</li> </ul>	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
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://<NSM\\_IP>/sdkapi/1001/endpointintelligence/endpointintelligence?duration=LAST\\_14\\_DAYS&&confidencetype=any&&classificationtype=any](https://<NSM_IP>/sdkapi/1001/endpointintelligence/endpointintelligence?duration=LAST_14_DAYS&&confidencetype=any&&classificationtype=any)

#### Response

```
{
  "endpointExecutableList": [
    {
      "executableHash": "laaaaaaaaaaaaaaaaaaaaaaaaaa23",
      "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 <ul style="list-style-type: none"><li>• LAST_5_MINUTES</li><li>• LAST_1_HOUR</li><li>• LAST_6_HOURS</li><li>• LAST_12_HOURS</li><li>• LAST_24_HOURS</li><li>• LAST_48_HOURS</li><li>• LAST_7_DAYS</li><li>• LAST_14_DAYS</li></ul>	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
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

Field Name	Description	Data Type
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
filesize	Filesize	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://<NSM\_IP>/sdkapi/1001/endpointintelligence/aaaaaaa16/ executableinformation?  
duration=LAST\_14\_DAYS

### Response

```
{
  "properties":
  {
    "hash": "1aaaaaaaaaaaaaaaaaaaaaaaaa23",
    "binaryType": "Process",
    "binaryName": "abc.exe",
    "productName": "",
    "productVersion": "file_version",
    "overallMalwareConfidence": "Medium",
    "eiaAgentMalwareConfidence": "Medium",
    "classification": "unclassified",
    "classifier": "---", "filesize": 2566795},
    "heuristics": {},
    "suspiciousLibraries": [{
      "hash": "1aaaaaaaaaaaaaaaaaaaaaaaaa1",
      "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 <ul style="list-style-type: none"><li>• LAST_5_MINUTES</li><li>• LAST_1_HOUR</li><li>• LAST_6_HOURS</li><li>• LAST-12_HOURS</li><li>• LAST_24_HOURS</li><li>• LAST_48_HOURS</li><li>• LAST_7_DAYS</li><li>• LAST_14_DAYS</li></ul>	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 Endpoint	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://<NSM\\_IP>/sdkapi/1001/endpointintelligence/aaaaaaaa16/endpoints?duration=LAST\\_14\\_DAYS](https://<NSM_IP>/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 <ul style="list-style-type: none"><li>• LAST_5_MINUTES</li><li>• LAST_1_HOUR</li><li>• LAST_6_HOURS</li><li>• LAST_12_HOURS</li><li>• LAST_24_HOURS</li><li>• LAST_48_HOURS</li><li>• LAST_7_DAYS</li><li>• LAST_14_DAYS</li></ul>	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 Application	array

Details of ApplicationList:

Field Name	Description	Data Type
applicationName	Application Name	string
connectionsCount	Connections count	int
eventsCount	Events count	int

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/1001/endpointintelligence/aaaaaaaa16/applications?duration=LAST\\_14\\_DAYS](https://<NSM_IP>/sdkapi/1001/endpointintelligence/aaaaaaaa16/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 <ul style="list-style-type: none"> <li>• LAST_5_MINUTES</li> <li>• LAST_1_HOUR</li> <li>• LAST_6_HOURS</li> <li>• LAST-12_HOURS</li> <li>• LAST_24_HOURS</li> <li>• LAST_48_HOURS</li> <li>• LAST_7_DAYS</li> <li>• LAST_14_DAYS</li> </ul>	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://<NSM\\_IP>/sdkapi/1001/endpointintelligence/aaaaaaaa16/events?duration=LAST\\_14\\_DAYS](https://<NSM_IP>/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":"---","victimIpAddresses":"0.1.138.146","victimPort":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 whitelist/blacklist/classified

### Resource URL

PUT /<nbaId>/endpointintelligence/<hash>/takeaction/<action>

### Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
hash	Hash	string	Yes
Action	Action <ul style="list-style-type: none"><li>Whitelist</li><li>Blacklist</li><li>Unclassified</li></ul>	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
Status	Status	int

### Example

#### Request

PUT [https://<NSM\\_IP>/sdkapi/1001/endpointintelligence/aaaaaaaa16/takeaction/whitelist](https://<NSM_IP>/sdkapi/1001/endpointintelligence/aaaaaaaa16/takeaction/whitelist)

#### 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

**Contents**

- *Get NMS IPs at Domain*
- *Create NMS IP at Domain*
- *Delete the NMS IP at Domain*
- *Get NMS IPs at Sensor*
- *Get available NMS IPs at Sensor*
- *Create NMS IP at Sensor*
- *Allocate NMS IP to Sensor*
- *Delete the NMS IP at Sensor*

---

## Get NMS IPs at Domain

This URL gets the NMS IPs 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 IPs	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](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](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
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

### 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](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 IPs	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](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 IPs	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/available](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 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](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](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
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

#### 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](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



No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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



# 36

## NMS Users Resource

### Contents

- ▶ *Get NMS Users at Domain*
- ▶ *Create NMS User at Domain*
- ▶ *Update NMS User at Domain*
- ▶ *Get the NMS User Details at Domain*
- ▶ *Delete the NMS User at Domain*
- ▶ *Get NMS Users at Sensor*
- ▶ *Get available NMS Users at Sensor*
- ▶ *Create NMS User at Sensor*
- ▶ *Allocate NMS User to Sensor*
- ▶ *Update NMS User at Sensor*
- ▶ *Get the NMS User Details at Sensor*
- ▶ *Delete the NMS User at Sensor*

---

### 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](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 Codes are 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](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

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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
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](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
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](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](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
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](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](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](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
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](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/&lt;sensor\_id&gt;/nmsuser/&lt;nmsuser\_id&gt;

## Request Parameters

URL Parameters:

Field Name	Description	Data Type	Mandatory
sensorId	sensorId 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](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
3	400	5602	User name, private key and authorization key should be alphanumeric

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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](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

### 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](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

# 37

## Policy Export Import Resource

### Contents

- ▶ *Get the list of importable IPS and Reconnaissance policies*
- ▶ *Import the IPS and Reconnaissance policies*
- ▶ *Import the Malware policies*
- ▶ *Import the Firewall policies*
- ▶ *Import the Exceptions*
- ▶ *Gets the exportable IPS Reconnaissance policies from the Manager*
- ▶ *Export the IPS Reconnaissance policies*
- ▶ *Gets the exportable Malware policies from the Manager*
- ▶ *Export the Malware policies*
- ▶ *Gets the exportable Firewall policies from the Manager*
- ▶ *Export the Firewall policies*
- ▶ *Gets the exportable Exceptions from the Manager*
- ▶ *Export the Exceptions*

---

## 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 BodyPart Objects	object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the ImportFileElement object	application/json object	Yes

Details of ImportFileElement:

Field Name	Description	Data Type	Mandatory
fileName	Name of the file	string	Yes
fileType	FileType 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 InputStream	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 NSM	ObjectList

Details of fields in PolicyDiffElementList :

Field Name	Description	Data Type
PolicyDiffElement	Difference between the policy present on NSM 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 NSM)	string
policyName	Name of the policy	string
status	Status of the policy when the policy on XML and NSM are compared	string
outboundPolicyId	Outbound ID of the policy ( -1 if not present on the NSM)	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](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

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	5301	Invalid FileType 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

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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 BodyPart Objects	object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the ImportFileElement object	application/json object	Yes

Details of ImportFileElement:

Field Name	Description	Data Type	Mandatory
fileName	Name of the file	string	Yes
fileType	FileType 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 InputStream	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](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**

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	5301	Invalid FileType 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 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 BodyPart Objects	object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the ImportFileElement object	application/json object	Yes

Details of ImportFileElement:

Field Name	Description	Data Type	Mandatory
fileName	Name of the file	string	Yes
fileType	FileType 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 InputStream	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](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" quarantineConfidence="0" saveFileConfidence="1"
blacklistConfidence="0" fileSize="0"/>
      <MalwarePolicyFileActions groupId="2" engineStatus="18" alertingConfidence="5"
blockingConfidence="5" sendTcpConfidence="5" quarantineConfidence="0" saveFileConfidence="1"
blacklistConfidence="0" fileSize="0"/>
      <MalwarePolicyFileActions groupId="3" engineStatus="27" alertingConfidence="5"
blockingConfidence="5" sendTcpConfidence="5" quarantineConfidence="0" saveFileConfidence="1"
blacklistConfidence="0" fileSize="0"/>
      <MalwarePolicyFileActions groupId="4" engineStatus="18" alertingConfidence="5"
blockingConfidence="5" sendTcpConfidence="5" quarantineConfidence="0" saveFileConfidence="1"
blacklistConfidence="0" fileSize="0"/>
      <MalwarePolicyFileActions groupId="5" engineStatus="3" alertingConfidence="5"
blockingConfidence="5" sendTcpConfidence="5" quarantineConfidence="0" saveFileConfidence="1"
blacklistConfidence="0" fileSize="0"/>
    </MalwarePolicy>
  </MalwarePolicyExport>
</MalwarePolicyConfig>
```

```
<MalwarePolicyFileActions groupId="6" engineStatus="18" alertingConfidence="5"
blockingConfidence="5" sendTcpConfidence="5" quarantineConfidence="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**

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	5301	Invalid FileType 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 BodyPart Objects	object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the ImportFileElement object	application/json object	Yes

Details of ImportFileElement:

Field Name	Description	Data Type	Mandatory
fileName	Name of the file	string	Yes
fileType	FileType 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 InputStream	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](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>
      </FWPolicyRules>
    </FWPolicy>
  </FWPolicies>
</NetworkObjects>
</FWConfig>
```

```
//.....//
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

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	5301	Invalid FileType 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 BodyPart Objects	object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the ImportFileElement object	application/json object	Yes

Details of ImportFileElement:

Field Name	Description	Data Type	Mandatory
fileName	Name of the file	string	Yes
fileType	FileType 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 InputStream	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](https://<NSM_IP>/sdkapi/domain/0/exceptions/import)

Payload

```

----Boundary_1_12424925_1353496814940
Content-Type: application/json

{"fileType": "xml", "skipDuplicate": false, "fileName": "IDSAAlertFilter"}

----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>
  </AlertFilterExport>
</AFConfig>

```

```
<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

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	5301	Invalid FileType 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: <ul style="list-style-type: none"><li>• IPS_POLICY</li><li>• RECON_POLICY</li></ul>	string
policyId	ID of the policy	integer

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/domain/0/ipsreconpolicy/export](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

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](https://<NSM_IP>/sdkapi/domain/0/ipsreconpolicy/export)

### Payload

```
{
  "selectedPolicyNameList":["DefaultInlineIPS","NSAT 7.1 Reconnaissance Policy"]
}
```

### Response

```
{
  "byteStream": "<?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

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: <ul style="list-style-type: none"><li>MALWARE_POLICY</li></ul>	string
policyId	ID of the policy	integer

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/domain/0/malwarepolicy/export](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**

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](https://<NSM_IP>/sdkapi/domain/0/malwarepolicy/export)

### Payload

```
{
  "selectedPolicyNameList":[" TestMalwarePolicy_1"," TestMalwarePolicy_2" ,"malware
archive"]
}
```

### Response

```
{
  "byteStream": " <?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" quarantineConfidence="0" saveFileConfidence="1" blacklistConfidence="0" fileSize="0"/>
<MalwarePolicyFileActions groupId="2" engineStatus="18" alertingConfidence="5" blockingConfidence="5"
sendTcpConfidence="5" quarantineConfidence="0" saveFileConfidence="1" blacklistConfidence="0" fileSize="0"/>
<MalwarePolicyFileActions groupId="3" engineStatus="27" alertingConfidence="5" blockingConfidence="5"
sendTcpConfidence="5" quarantineConfidence="0" saveFileConfidence="1" blacklistConfidence="0" fileSize="0"/>
<MalwarePolicyFileActions groupId="4" engineStatus="18" alertingConfidence="5" blockingConfidence="5"
sendTcpConfidence="5" quarantineConfidence="0" saveFileConfidence="1" blacklistConfidence="0" fileSize="0"/>
```

```

<MalwarePolicyFileActions groupId="5" engineStatus="3" alertingConfidence="5" blockingConfidence="5"
sendTcpConfidence="5" quarantineConfidence="0" saveFileConfidence="1" blacklistConfidence="0" fileSize="0"/>

<MalwarePolicyFileActions groupId="6" engineStatus="18" alertingConfidence="5" blockingConfidence="5"
sendTcpConfidence="5" quarantineConfidence="0" saveFileConfidence="1" blacklistConfidence="0" fileSize="0"/>

</MalwarePolicy>

</MalwarePolicyExport>

</MalwarePolicyConfig> "
}

```

### Error Information

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: <ul style="list-style-type: none"><li>• FIREWALL_POLICY</li></ul>	string
policyId	ID of the policy	integer

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/domain/0/firewallpolicy/export](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

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](https://<NSM_IP>/sdkapi/domain/0/firewallpolicy/export)

### Payload

```
{
  "selectedPolicyNameList":["FirewallPolicy4","FirewallPolicy3"]
}
```

### Response

```
{
  "byteStream": "<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>
    </FWPolicyRules>
  </FWPolicy>
  //.....//
  <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

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
policyType	Type of the policy: <ul style="list-style-type: none"><li>EXCEPTIONS</li></ul>	string
policyId	ID of the policy	integer

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/domain/0/exceptions/export](https://<NSM_IP>/sdkapi/domain/0/exceptions/export)

### Response

```
{
  'exportablePolicyDetail': [{
    'policyName': 'test1',
    'policyType': 'EXCEPTIONS',
    'policyId': 301
  },
  {
    'policyName': 'test2',
    'policyType': 'EXCEPTIONS',
    'policyId': 302
  }
  ]
}
```

### Error Information

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](https://<NSM_IP>/sdkapi/domain/0/exceptions/export)

### Payload

```
{
  "selectedPolicyNameList":["test1","test2", "test3"]
}
```

### Response

```
{
  "byteStream": "<?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

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>



# 38

## TCP Settings

### Contents

- [Get TCP Settings Configuration at Sensor level](#)
- [Update the TCP Settings on Sensor](#)

## 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

Field Name	Description	Data Type
coldStartAckScanAlertDiscardIntervalInMinutes	The Cold start Ack Scan Alert Discard Interval(minutes)	number
coldStartDropAction	The Cold Start Drop Action. The value can be: <ul style="list-style-type: none"> <li>• DROP_FLOWS</li> <li>• FORWARD_FLOWS</li> </ul>	string
tcpFlowViolation	The TCP Flow Violation. The value can be: <ul style="list-style-type: none"> <li>• PERMIT</li> <li>• DENY</li> <li>• PERMIT_OUT_OF_ORDER</li> <li>• DENY_NO_TC B</li> <li>• STATELESS_I NSPECTION</li> </ul>	string
unsolicitedUDPPacketTimeOutInSeconds	The Unsolicited UDP Packets Timeout(seconds)	number
Normalization	The Normalization. The value can be: <ul style="list-style-type: none"> <li>• ON</li> <li>• OFF</li> </ul>	string
tcpOverlapOption	The TCP Overlap Option. The value can be: <ul style="list-style-type: none"> <li>• OLD_DATA</li> <li>• NEW_DATA</li> </ul>	string
synCookie	The SYN Cookie Data	object
resetUnfinished3WayHandshakeConnection	The Reset Unfinished 3 way handshake connection. The value can be: <ul style="list-style-type: none"> <li>• DISABLED</li> <li>• SET_FOR_ALL_TRAFFIC</li> <li>• SET_FOR_DOS_ATTACK_TRAFFIC_ONLY</li> </ul>	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: <ul style="list-style-type: none"> <li>• DISABLED</li> <li>• INBOUND_ONLY</li> <li>• OUTBOUND_ONLY</li> <li>• BOTH_INBOUND_AND_OUTBOUND</li> </ul>	string
inboundThresholdValue	The inbound threshold value	number
outboundThresholdValue	The outbound threshold value	number

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/sensor/1002/tcpsettings](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

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: <ul style="list-style-type: none"> <li>• DROP_FLOWS</li> <li>• FORWARD_FLOWS</li> </ul>	string	No
tcpFlowViolation	The TCP Flow Violation. The value can be: <ul style="list-style-type: none"> <li>• PERMIT</li> <li>• DENY</li> <li>• PERMIT_OUT_OF_ORDER</li> <li>• DENY_NO_TC CB</li> <li>• STATELESS_INSPECTION</li> </ul>	string	No
unsolicitedUDPPacketTimeOutInSeconds	The Unsolicited UDP Packets Timeout(seconds)	number	No
Normalization	The Normalization. The value can be: <ul style="list-style-type: none"> <li>• ON</li> <li>• OFF</li> </ul>	string	No
tcpOverlapOption	The TCP Overlap Option. The value can be: <ul style="list-style-type: none"> <li>• OLD_DATA</li> <li>• NEW_DATA</li> </ul>	string	No
synCookie	The SYN Cookie Data	object	No
resetUnfinished3WayHandshakeConnection	The Reset Unfinished 3 way handshake connection. The value can be: <ul style="list-style-type: none"> <li>• DISABLED</li> <li>• SET_FOR_ALL_TRAFFIC</li> <li>• SET_FOR_DOS_ATTACK_TRAFFIC_ONLY</li> </ul>	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: <ul style="list-style-type: none"><li>• DISABLED</li><li>• INBOUND_ONLY</li><li>• OUTBOUND_ONLY</li><li>• BOTH_INBOUND_AND_OUTBOUND</li></ul>	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](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

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
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



# 39

## IP Settings

### Contents

- [Update IP Settings Configuration at Sensor level](#)
- [Get IP Settings Configuration at Sensor level](#)

## 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: <ul style="list-style-type: none"><li>• ENABLED</li><li>• DISABLED</li></ul>	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: <ul style="list-style-type: none"> <li>• OLD_DATA</li> <li>• NEW_DATA</li> </ul>	string	no
smallestFragmentSize	The Smallest Fragment Size	number	no
smallFragmentThreshold	The Small Fragment Threshold	number	no
fragmentReassembly	The Fragment Reassembly. The value can be: <ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>	string	no

Details of fields in ipv6Parameter :

Field Name	Description	Data Type	Mandatory
ipv6Scanning	The IPv6 Scanning data. The value can be: <ul style="list-style-type: none"> <li>• SCAN_IPV_6_TRAFFIC_FOR_ATTACKS</li> <li>• DROP_ALL_IPV_6_TARFFIC_INLINE_ONLY</li> <li>• PASS_IPV_6_TRAFFIC_WITHOUT_SCANNING</li> </ul>	string	no
overlapOption	The Overlap Option. The value can be: <ul style="list-style-type: none"> <li>• OLD_DATA</li> <li>• NEW_DATA</li> <li>• DROP</li> </ul>	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](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

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
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: <ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>	string

Details of fields in ipv4Parameter :

Field Name	Description	Data Type
fragmentTimer	The Fragment timer(seconds)	number
overlapOption	The Overlap Option. The value can be: <ul style="list-style-type: none"> <li>• OLD_DATA</li> <li>• NEW_DATA</li> </ul>	string
smallestFragmentSize	The Smallest Fragment Size	number
smallFragmentThreshold	The Small Fragment Threshold	number
fragmentReassembly	The Fragment Reassembly. The value can be: <ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>	string

Details of fields in ipv6Parameter :

Field Name	Description	Data Type
ipv6Scanning	The IPv6 Scanning data. The value can be: <ul style="list-style-type: none"> <li>• SCAN_IPV_6_TRAFFIC_FOR_ATTACKS</li> <li>• DROP_ALL_IPV_6_TARFFIC_INLINE_ONLY</li> <li>• PASS_IPV_6_TRAFFIC_WITHOUT_SCANNING</li> </ul>	string
overlapOption	The Overlap Option. The value can be: <ul style="list-style-type: none"> <li>• OLD_DATA</li> <li>• NEW_DATA</li> <li>• DROP</li> </ul>	string
smallestFragmentSize	The Smallest Fragment Size	number
smallFragmentThreshold	The Small Fragment Threshold	number

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/sensor/1002/ipsettings](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

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



## Firewall Logging Resource

### Contents

- [Update the Firewall Logging](#)
- [Get the Firewall Logging](#)

---

## 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
isSuppressionEnabled	To enable the Suppression
individualMessage	Individual Message
suppressionInterval	Suppression Interval
uniqueSourceDestinationIPpairs	Unique Source Destination IP pairs
loggingType	Logging Type can be "DISABLE_DEVICE", "LOG_ALL_MATCHED_TRAFFIC", "LOG_ALL_DROPPED_DENIED"
deliveryType	Delivery Type can be "MESSAGES_TO_TARGET_SYSLOGSERVER_VIA_MANAGER", "

### 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](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

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 l 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
isSuppressionEnabled	To enable the Suppression
individualMessage	Individual Message



Field Name	Description
suppressionInterval	Suppression Interval
uniqueSourceDestinationIPpairs	Unique Source Destination IP pairs
loggingType	Logging Type can be "DISABLE_DEVICE","LOG_ALL_MATCHED_TRAFFIC","LOG_ALL_DROPPED_DENIED"
deliveryType	Delivery Type can be "MESSAGES_TO_TARGET_SYSLOGSERVER_VIA_MANAGER",""

**Example**

**Request**

GET [https://<NSM\\_IP>/sdkapi/sensor/1001/firewalllogging](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**

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



# 41

## IPS Alerting Resource

### Contents

- [Get the Alert Suppression](#)
- [Update the Alert Suppression](#)

### 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

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
enablePacketLogChannelEncryptio	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](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

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid sensor
2	500	1124	The Sensor is Inactive
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



# 42

## Failover Resource

### Contents

- [Add Failover](#)
- [Get the Failover Pair](#)
- [Get the Failover Pair list](#)

## 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](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**

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
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

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](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

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



# 43

## Syslog Firewall Notification Resource

### Contents

- [Get Syslog Configuration](#)
- [Create/Update Syslog Configuration](#)

### 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": "192.168.1.1",  
      "serverPort": 514,  
      "facilities": "all",  
      "severity": "info",  
      "Message": "Syslog notification enabled for firewall notification"    }  
  ]  
}
```

```

    "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

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](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

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





# 44

## Syslog Faults Notification Resource

### Contents

- [Get Syslog Configuration](#)
- [Create/Update Syslog Configuration](#)

### 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 severityMapping:

Field Name	Description	Data Type	Mandatory
inforamtionTo	Information mapping	string	No
warningTo	Warning Mapping	string	No

Field Name	Description	Data Type	Mandatory
errorTo	Error Mapping	string	No
criticalTo	Critical Mapping	string	No

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/domain/0/notification/faults/syslog](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

GET /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 severityMapping:

Field Name	Description	Data Type
inforamtionTo	Information mapping	string
warningTo	Warning Mapping	string
errorTo	Error Mapping	string
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](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**

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

# 45

## Tacacs Resource

### Contents

- [Get Tacacs on Domain](#)
- [Update Tacacs on Domain](#)
- [Get Tacacs on Sensor](#)
- [Update Tacacs on Sensor](#)

---

### 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](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 Codes are 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](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

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 Tacacsconfiguration.

### 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

Field Name	Description	Data Type
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](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



Field Name	Description	Data Type	Mandatory
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](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
4	400	4713	Invalid IP address



# 46

## Active Botnets Resource

### Contents

- [Get the list of active botnets](#)
- [Get the List of zombies for an active botnet](#)

### 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: <ul style="list-style-type: none"> <li>• LAST_5_MINUTES</li> <li>• LAST_1_HOUR</li> <li>• LAST_6_HOUR</li> <li>• LAST_12_HOUR</li> <li>• LAST_24_HOUR</li> <li>• LAST_48_HOUR</li> <li>• LAST_7_DAYS</li> <li>• LAST_14_DAYS</li> </ul>	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	Id of the active botnet	number
ccCommunication	C&C Communication	string

Field Name	Description	Data Type
events	Number of events	number
lastEvent	Last event time	string

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/domain/0/activebotnets](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: <ul style="list-style-type: none"><li>• LAST_5_MINUTES</li><li>• LAST_1_HOUR</li><li>• LAST_6_HOUR</li><li>• LAST_12_HOUR</li><li>• LAST_24_HOUR</li><li>• LAST_48_HOUR</li><li>• LAST_7_DAYS</li><li>• LAST_14_DAYS</li></ul>	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
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](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**

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

## Automatic Update Configuration Resource

### Contents

- [Get the Signature Set Automatic Update Configuration](#)
- [Get the Botnet Automatic Update Configuration](#)
- [Update the Signature Set Automatic Download Configuration](#)
- [Update the Botnet Automatic Download Configuration](#)
- [Update the Signature Set Automatic Deployment Configuration](#)
- [Update the Botnet Automatic Deployment Configuration](#)

---

### 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: <ul style="list-style-type: none"><li>• FREQUENTLY</li><li>• DAILY</li><li>• WEEKLY</li></ul>	string
startTime	Time when the update should start. Should be in hh:mm format.	string

Field Name	Description	Data Type
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: <ul style="list-style-type: none"> <li>• FREQUENTLY</li> <li>• DAILY</li> <li>• WEEKLY</li> </ul>	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](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 NSM 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: <ul style="list-style-type: none"><li>• FREQUENTLY</li><li>• DAILY</li><li>• WEEKLY</li></ul>	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: <ul style="list-style-type: none"><li>• FREQUENTLY</li><li>• DAILY</li><li>• WEEKLY</li></ul>	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](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: <ul style="list-style-type: none"><li>• FREQUENTLY</li><li>• DAILY</li><li>• WEEKLY</li></ul>	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](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
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: <ul style="list-style-type: none"> <li>• FREQUENTLY</li> <li>• DAILY</li> <li>• WEEKLY</li> </ul>	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/botnetdownloadconfig](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.

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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: <ul style="list-style-type: none"><li>• FREQUENTLY</li><li>• DAILY</li><li>• WEEKLY</li></ul>	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](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
schedule	Schedule for the update. Values can be following: <ul style="list-style-type: none"><li>• FREQUENTLY</li><li>• DAILY</li><li>• WEEKLY</li></ul>	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](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

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



# 48

## Malware Downloads Resource

### Contents

- [Get Malware Downloads](#)
- [Get Malware Alerts](#)

---

### 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 <ul style="list-style-type: none"><li>• LAST_5_MINUTES</li><li>• LAST_1_HOUR</li><li>• LAST_6_HOURS</li><li>• LAST_12_HOURS</li><li>• LAST_24_HOURS</li><li>• LAST_48_HOURS</li><li>• LAST_7_DAYS</li><li>• LAST_14_DAYS</li></ul>	string	No

Field Name	Description	Data Type	Mandatory
resultType	Result Type can be <ul style="list-style-type: none"> <li>• ANY_RESULT</li> <li>• BLOCKED</li> <li>• UNBLOCKED</li> </ul>	string	No
confidenceType	Confidence Type : can be <ul style="list-style-type: none"> <li>• ANY_MALWARE_CONFIDENCE</li> <li>• VERY_HIGH_MALWARE_CONFIDENCE</li> <li>• HIGH_MALWARE_CONFIDENCE</li> <li>• LOW_MALWARE_CONFIDENCE</li> <li>• MEDIUM_MALWARE_CONFIDENCE</li> <li>• VERY_LOW_MALWARE_CONFIDENCE</li> </ul>	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 MalwareSummaryDetail defined in the domain	array

Details of object in MalwareSummaryDetailList:

Field Name	Description	Data Type
filehash	File Hash	string
overAllConfidence	OverAllConfidence can be: "VERY_LOW"/"LOW"/"MEDIUM"/"HIGH"/"VERY_HIGH"/"UNKNOWN"	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	CustomFingerPrints can be: "VERY_LOW"/"LOW"/"MEDIUM"/"HIGH"/"VERY_HIGH"/"UNKNOWN"	string
GTIFileReputation	GTIFileReputation can be: "VERY_LOW"/"LOW"/"MEDIUM"/"HIGH"/"VERY_HIGH"/"UNKNOWN"	string
PDFEmulation	PDFEmulation can be: "VERY_LOW"/"LOW"/"MEDIUM"/"HIGH"/"VERY_HIGH"/"UNKNOWN"	string
GatewayAntiMalware	GatewayAntiMalware can be: "VERY_LOW"/"LOW"/"MEDIUM"/"HIGH"/"VERY_HIGH"/"UNKNOWN"	string

### Example

#### Request

GET [https://<NSM\\_IP>/domain/0/malwaredownloads](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 <ul style="list-style-type: none"><li>• LAST_5_MINUTES</li><li>• LAST_1_HOUR</li><li>• LAST_6_HOURS</li><li>• LAST_12_HOURS</li><li>• LAST_24_HOURS</li><li>• LAST_48_HOURS</li><li>• LAST_7_DAYS</li><li>• LAST_14_DAYS</li></ul>	string	No

Field Name	Description	Data Type	Mandatory
resultType	Result Type can be <ul style="list-style-type: none"> <li>• ANY_RESULT</li> <li>• BLOCKED</li> <li>• UNBLOCKED</li> </ul>	string	No
confidenceType	Confidence Type : can be <ul style="list-style-type: none"> <li>• ANY_MALWARE_CONFIDENCE</li> <li>• VERY_HIGH_MALWARE_CONFIDENCE</li> <li>• HIGH_MALWARE_CONFIDENCE</li> <li>• LOW_MALWARE_CONFIDENCE</li> <li>• MEDIUM_MALWARE_CONFIDENCE</li> <li>• VERY_LOW_MALWARE_CONFIDENCE</li> </ul>	string	No

### 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 MalwareAlertDetail 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"/"UNKNOWN"	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"/"BLOCKING_SIMULATED_INCONCLUSIVE"/"BLOCKING_SIMULATED_ATTACK_FAILED"/"BLOCKING_SIMULATED_NOT_APPLICABLE"	string
direction	Direction can be: "INBOUND"/" OUTBOUND"/" UNKNOWN"/" BOTH"	

### Example

#### Request

GET [https://<NSM\\_IP>/domain/0/malwaredownloads/filehash/493d146a59a155ed2eb890f5fd3bb182](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 filehash value
4	400	3801	Invalid result filter value
5	400	3802	Invalid duration filter value

# 49

## Nessus Scan Report Resource

### 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 BodyPart 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 InputStream	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](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
ÔrÝ?ü0Ýÿ<^}c,¢eXæ^:4 Jhí2p♦rDYñÇÚd¶/Â¿i♦F~      ÆIcS4éá©ÿ_8Öø« C6Ô654iPg`J6?x ,*T2;qhã4îÂVu-
Gfo9ŸCÖª„i¹İ      -Äë&1¹i,Ú<y i^i`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



# 50

## ATD Configuration Resource

### Contents

- [Get ATD Integration in Domain](#)
- [Update ATD Integration Configuration in Domain](#)
- [Get ATD Integration in sensor](#)
- [Update ATD Integration Configuration in Sensor](#)

---

### 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	enableCommunication	boolean
atdUsername	atdUsername	string
atdPassword	atdPassword	string
sensorToATDCommunicationPort	sensorToATDCommunicationPort	number
managerToATDCommunicationPort	managerToATDCommunicationPort	number
atdApplianceIPAddr	atdApplianceIPAddr	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

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	enableCommunication	boolean
atdUsername	atdUsername	string
atdPassword	atdPassword	string
sensorToATDCommunicationPort	sensorToATDCommunicationPort	number
managerToATDCommunicationPort	managerToATDCommunicationPort	number
atdApplianceIPAddr	atdApplianceIPAddr	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](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	enableCommunication	boolean
inheritSettings	Inherit settings	string
atdUsername	atdUsername	string
atdPassword	atdPassword	string
sensorToATDCommunicationPort	sensorToATDCommunicationPort	number
managerToATDCommunicationPort	managerToATDCommunicationPort	number
atdApplianceIPAddr	atdApplianceIPAddr	string

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/sensor/0/atdintegration](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

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	enableCommunication	boolean
inheritSettings	Inherit settings	string
atdUsername	atdUsername	string
atdPassword	atdPassword	string
sensorToATDCommunicationPort	sensorToATDCommunicationPort	number
managerToATDCommunicationPort	managerToATDCommunicationPort	number
atdApplianceIPAddr	atdApplianceIPAddr	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](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 Codes are returned by this URL:

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



# 51

## Sensor Configuration Export Import Resource

### Contents

- [Export the Sensor Configuration](#)
- [Import the Sensor Configuration](#)

### 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 Fail over 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](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

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 BodyPart Objects	object	Yes



Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the ImportFileElement object	application/json object	Yes

Details of ImportFileElement:

Field Name	Description	Data Type	Mandatory
fileName	Name of the file	string	Yes
fileType	FileType should be "XML"	string	Yes

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
BodyPart[1]	Holds the File as InputStream	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](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

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid sensor
2	400	5301	Invalid FileType given for import
3	400	1124	The sensor is inactive
4	500	2202	Input Stream read error
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 NSM

# 52

## Denial Of Service Resource

### Contents

- ▶ *Get the DoS profiles on the manager for Sensors*
- ▶ *Update the DoS learning mode on the Sensor*
- ▶ *Get the DoS packet forwarding*
- ▶ *Upload the DoS Profile from the Sensor*
- ▶ *Restore the DoS Profile to the Sensor*
- ▶ *Delete the DoS Profile*
- ▶ *Export the DoS Profile to the Manager client*

---

### 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>/dosprofilesmanager

#### 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/dosprofilesmanager

## 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

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: <ul style="list-style-type: none"> <li>• LEARNING_MODE</li> <li>• DETECTION_MODE</li> </ul>	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](https://<NSM_IP>/sdkapi/sensor/1002/dosprofilelearningmode)

### Payload

```
{
  "dosProfileLearning" : "LEARNING_MODE"
}
```

### Response

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

### Error Information

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](https://<NSM_IP>/sdkapi/sensor/1002/dospacketforwarding)

#### Response

```
{
  "dosPacketForwarding": "Do Not Copy DoS Packets (Dos Packet Logging is disabled)"
}
```

**Error Information**

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](https://<NSM_IP>/sdkapi/sensor/1002/uploaddosprofile)

**Response**

```
{
  "status": 1,
  "message": "Upload Complete for Dos (from sensor to manager)"
}
```

**Error Information**

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](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

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](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

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](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**

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1124	The Sensor is inactive

# 53

## Domain Name Exceptions Resource

### Contents

- ▶ *Get the Domain Name Exceptions from the Manager*
- ▶ *Import the Domain Name Exceptions to the Manager*
- ▶ *Export the Domain Name Exceptions from the Manager*
- ▶ *Update a Domain Name exception's comment*
- ▶ *Delete some Domain Name Exceptions*
- ▶ *Delete all Domain Name Exceptions*
- ▶ *Add domain name to callback detector whitelist*
- ▶ *Update the details of Domain Name Exception*

---

## 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](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 BodyPart Objects	object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the DNEFileElement object	application/json object	Yes

Details of DNEFileElement:

Field Name	Description	Data Type	Mandatory
fileName	Name of the file	string	Yes
fileType	FileType should be .csv	string	No

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
BodyPart[1]	Holds the file as InputStream	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](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

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 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

---

## 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](https://<NSM_IP>/sdkapi/domainnameexceptions)

### Payload

```
{
  "domainName": "www.google.com",
  "comment": "Google"
}
```

### Response

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

## Error Information

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 stringList.

### 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](https://<NSM_IP>/sdkapi/domainnameexceptions)**Payload**

```
{
  "domainName": ["www.google.com",
    "abc",
    "test"]
}
```

**Response**

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

**Error Information**

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](https://<NSM_IP>/sdkapi/domainnameexceptions/all)**Payload**



None

### Response

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

### Error Information

None

---

## Add domain name to callback detector whitelist

This URL adds domain name to callback detection whitelist.

### 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](https://<NSM_IP>/sdkapi/domainnameexceptions)

#### Payload

```
{
  "domainName": "www.google1.com",
  "comment": "updated domain"
}
```

#### Response

```
{
  "createdResourceId": 1
}
```

### Error Information

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
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 whitelist.

### 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](https://<NSM_IP>/sdkapi/domainnameexceptions/updatedetail)

#### Payload

```
{
  "oldDomainName": "www.google.com",
  "domainName": "www.google1.com",
  "comment": "updated domain"
}
```

#### Response

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

### Error Information

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 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



# 54

## Direct Syslog Resource

### Contents

- *Get the Direct Syslog Configuration for the domain*
- *Update the Direct Syslog Configuration for the domain*
- *Get the Direct Syslog Configuration for the Sensor*
- *Update the Direct Syslog Configuration for the Sensor*
- *Test the Direct Syslog Configuration for domain*
- *Test the Direct Syslog Configuration for the Sensor*

---

### Get the Direct Syslog Configuration for the domain

This URL retrieves the DXL Integration 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
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](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=$IV_ATTACK_TIME$Quarantine_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

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	6001	Direct Syslog 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

Field Name	Description	Data Type	Mandatory
syslogFacility	Syslog Facility. Allowed values are: <ul style="list-style-type: none"> <li>SECURITY_AUTHORIZATION_CODE_10</li> <li>SECURITY_AUTHORIZATION_CODE_4</li> <li>LOG_AUDIT_NOTE_1</li> <li>LOG_ALERT_NOTE_1</li> <li>CLOCK_DAEMON_NOTE_2</li> <li>LOCAL_USER_0</li> <li>LOCAL_USER_1</li> <li>LOCAL_USER_2</li> <li>LOCAL_USER_3</li> <li>LOCAL_USER_4</li> <li>LOCAL_USER_5</li> <li>LOCAL_USER_6</li> <li>LOCAL_USER_7</li> </ul>	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: <ul style="list-style-type: none"> <li>EMERGENCY_SYSTEM_UNUSABLE</li> <li>ALERT_ACTION_IMMEDIATELY</li> <li>CRITICAL_CONDITIONS</li> <li>ERROR</li> <li>WARNING_CONDITIONS</li> <li>NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>INFORMATIONAL_MESSAGES</li> <li>DEBUG_MESSAGES</li> </ul>	string	Yes
lowTo	Low severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>EMERGENCY_SYSTEM_UNUSABLE</li> <li>ALERT_ACTION_IMMEDIATELY</li> <li>CRITICAL_CONDITIONS</li> <li>ERROR</li> <li>WARNING_CONDITIONS</li> <li>NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>INFORMATIONAL_MESSAGES</li> <li>DEBUG_MESSAGES</li> </ul>	string	Yes



Field Name	Description	Data Type	Mandatory
mediumTO	Medium severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>EMERGENCY_SYSTEM_UNUSABLE</li> <li>ALERT_ACTION_IMMEDIATELY</li> <li>CRITICAL_CONDITIONS</li> <li>ERROR</li> <li>WARNING_CONDITIONS</li> <li>NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>INFORMATIONAL_MESSAGES</li> <li>DEBUG_MESSAGES</li> </ul>	string	yes
highTo	High severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>EMERGENCY_SYSTEM_UNUSABLE</li> <li>ALERT_ACTION_IMMEDIATELY</li> <li>CRITICAL_CONDITIONS</li> <li>ERROR</li> <li>WARNING_CONDITIONS</li> <li>NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>INFORMATIONAL_MESSAGES</li> <li>DEBUG_MESSAGES</li> </ul>	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: <ul style="list-style-type: none"> <li>INFORMATIONAL</li> <li>LOW</li> <li>MEDIUM</li> <li>HIGH</li> </ul>	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](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=$IV_ATTACK_TIME$Quarantine_Time=$IV_QUARANTINE_END_TIME$Result_Status=$IV_RESULT_STATUS$Alert_UUID=$IV_SENSOR_ALERT_UUID$PeerName=$IV_SENSOR_CLUSTER$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
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](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=$IV_ATTACK_TIME$Quarantine_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

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: <ul style="list-style-type: none"> <li>SECURITY_AUTHORIZATION_CODE_10</li> <li>SECURITY_AUTHORIZATION_CODE_4</li> <li>LOG_AUDIT_NOTE_1</li> <li>LOG_ALERT_NOTE_1</li> <li>CLOCK_DAEMON_NOTE_2</li> <li>LOCAL_USER_0</li> <li>LOCAL_USER_1</li> <li>LOCAL_USER_2</li> <li>LOCAL_USER_3</li> <li>LOCAL_USER_4</li> <li>LOCAL_USER_5</li> <li>LOCAL_USER_6</li> <li>LOCAL_USER_7</li> </ul>	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: <ul style="list-style-type: none"> <li>• EMERGENCY_SYSTEM_UNUSABLE</li> <li>• ALERT_ACTION_IMMEDIATELY</li> <li>• CRITICAL_CONDITIONS</li> <li>• ERROR</li> <li>• WARNING_CONDITIONS</li> <li>• NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>• INFORMATIONAL_MESSAGES</li> <li>• DEBUG_MESSAGES</li> </ul>	string	Yes
lowTo	Low severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>• EMERGENCY_SYSTEM_UNUSABLE</li> <li>• ALERT_ACTION_IMMEDIATELY</li> <li>• CRITICAL_CONDITIONS</li> <li>• ERROR</li> <li>• WARNING_CONDITIONS</li> <li>• NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>• INFORMATIONAL_MESSAGES</li> <li>• DEBUG_MESSAGES</li> </ul>	string	Yes
mediumTo	Medium severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>• EMERGENCY_SYSTEM_UNUSABLE</li> <li>• ALERT_ACTION_IMMEDIATELY</li> <li>• CRITICAL_CONDITIONS</li> <li>• ERROR</li> <li>• WARNING_CONDITIONS</li> <li>• NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>• INFORMATIONAL_MESSAGES</li> <li>• DEBUG_MESSAGES</li> </ul>	string	yes
highTo	High severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>• EMERGENCY_SYSTEM_UNUSABLE</li> <li>• ALERT_ACTION_IMMEDIATELY</li> <li>• CRITICAL_CONDITIONS</li> <li>• ERROR</li> <li>• WARNING_CONDITIONS</li> <li>• NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>• INFORMATIONAL_MESSAGES</li> <li>• DEBUG_MESSAGES</li> </ul>	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: <ul style="list-style-type: none"><li>• INFORMATIONAL</li><li>• LOW</li><li>• MEDIUM</li><li>• HIGH</li></ul>	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](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=$IV_ATTACK_TIME$Quarantine_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
serverIp	Syslog server IP	string	Yes
serverPort	Syslog server port (UDP)	number	Yes



Field Name	Description	Data Type	Mandatory
syslogFacility	Syslog Facility. Allowed values are: <ul style="list-style-type: none"> <li>SECURITY_AUTHORIZATION_CODE_10</li> <li>SECURITY_AUTHORIZATION_CODE_4</li> <li>LOG_AUDIT_NOTE_1</li> <li>LOG_ALERT_NOTE_1</li> <li>CLOCK_DAEMON_NOTE_2</li> <li>LOCAL_USER_0</li> <li>LOCAL_USER_1</li> <li>LOCAL_USER_2</li> <li>LOCAL_USER_3</li> <li>LOCAL_USER_4</li> <li>LOCAL_USER_5</li> <li>LOCAL_USER_6</li> <li>LOCAL_USER_7</li> </ul>	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: <ul style="list-style-type: none"> <li>EMERGENCY_SYSTEM_UNUSABLE</li> <li>ALERT_ACTION_IMMEDIATELY</li> <li>CRITICAL_CONDITIONS</li> <li>ERROR</li> <li>WARNING_CONDITIONS</li> <li>NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>INFORMATIONAL_MESSAGES</li> <li>DEBUG_MESSAGES</li> </ul>	string	Yes
lowTo	Low severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>EMERGENCY_SYSTEM_UNUSABLE</li> <li>ALERT_ACTION_IMMEDIATELY</li> <li>CRITICAL_CONDITIONS</li> <li>ERROR</li> <li>WARNING_CONDITIONS</li> <li>NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>INFORMATIONAL_MESSAGES</li> <li>DEBUG_MESSAGES</li> </ul>	string	Yes

Field Name	Description	Data Type	Mandatory
mediumTo	Medium severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>• EMERGENCY_SYSTEM_UNUSABLE</li> <li>• ALERT_ACTION_IMMEDIATELY</li> <li>• CRITICAL_CONDITIONS</li> <li>• ERROR</li> <li>• WARNING_CONDITIONS</li> <li>• NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>• INFORMATIONAL_MESSAGES</li> <li>• DEBUG_MESSAGES</li> </ul>	string	yes
highTo	High severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>• EMERGENCY_SYSTEM_UNUSABLE</li> <li>• ALERT_ACTION_IMMEDIATELY</li> <li>• CRITICAL_CONDITIONS</li> <li>• ERROR</li> <li>• WARNING_CONDITIONS</li> <li>• NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>• INFORMATIONAL_MESSAGES</li> <li>• DEBUG_MESSAGES</li> </ul>	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: <ul style="list-style-type: none"> <li>• INFORMATIONAL</li> <li>• LOW</li> <li>• MEDIUM</li> <li>• HIGH</li> </ul>	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](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=$IV_ATTACK_TIME$Quarantine_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: <ul style="list-style-type: none"> <li>SECURITY_AUTHORIZATION_CODE_10 • LOCAL_USER_2</li> <li>SECURITY_AUTHORIZATION_CODE_4 • LOCAL_USER_3</li> <li>LOG_AUDIT_NOTE_1 • LOCAL_USER_4</li> <li>LOG_ALERT_NOTE_1 • LOCAL_USER_5</li> <li>CLOCK_DAEMON_NOTE_2 • LOCAL_USER_6</li> <li>LOCAL_USER_0 • LOCAL_USER_7</li> <li>LOCAL_USER_1</li> </ul>	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: <ul style="list-style-type: none"> <li>EMERGENCY_SYSTEM_UNUSABLE</li> <li>ALERT_ACTION_IMMEDIATELY</li> <li>CRITICAL_CONDITIONS</li> <li>ERROR</li> <li>WARNING_CONDITIONS</li> <li>NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>INFORMATIONAL_MESSAGES</li> <li>DEBUG_MESSAGES</li> </ul>	string	Yes
lowTo	Low severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>EMERGENCY_SYSTEM_UNUSABLE</li> <li>ALERT_ACTION_IMMEDIATELY</li> <li>CRITICAL_CONDITIONS</li> <li>ERROR</li> <li>WARNING_CONDITIONS</li> <li>NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>INFORMATIONAL_MESSAGES</li> <li>DEBUG_MESSAGES</li> </ul>	string	Yes
mediumTo	Medium severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>EMERGENCY_SYSTEM_UNUSABLE</li> <li>ALERT_ACTION_IMMEDIATELY</li> <li>CRITICAL_CONDITIONS</li> <li>ERROR</li> <li>WARNING_CONDITIONS</li> <li>NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>INFORMATIONAL_MESSAGES</li> <li>DEBUG_MESSAGES</li> </ul>	string	yes
highTo	High severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>EMERGENCY_SYSTEM_UNUSABLE</li> <li>ALERT_ACTION_IMMEDIATELY</li> <li>CRITICAL_CONDITIONS</li> <li>ERROR</li> <li>WARNING_CONDITIONS</li> <li>NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>INFORMATIONAL_MESSAGES</li> <li>DEBUG_MESSAGES</li> </ul>	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: <ul style="list-style-type: none"> <li>• INFORMATIONAL</li> <li>• LOW</li> <li>• MEDIUM</li> <li>• HIGH</li> </ul>	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](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=$IV_ATTACK_TIME$Quarantine_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





# 55

## Packet Capture Resource

### Contents

- ▶ *Get the packet capture settings*
- ▶ *Update the packet capture settings*
- ▶ *Update the packet capturing status*
- ▶ *Get the list/a particular rule template*
- ▶ *Add a packet capture rule template*
- ▶ *Get the list of PCAP files captured*
- ▶ *Export the PCAP file captured*
- ▶ *Delete the PCAP file captured*
- ▶ *Get the list/a particular rule template*
- ▶ *Add a packet capture rule template*
- ▶ *Update a packet capture rule template*
- ▶ *Delete a packet capture rule template*

---

## 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

Field Name	Description	Data Type
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](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

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: monitoringSPANPort/manager/scpServer	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
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 scpServer:

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
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](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
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: <ul style="list-style-type: none"> <li>START</li> <li>STOP</li> <li>CANCEL</li> </ul>	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

PUT [https://<NSM\\_IP>/sensor/1001/packetcapturestate](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
templete	List of rule templates	array

Details of object in templete:

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/sensor/1001/packetcaptureruletemplate?name=test](https://<NSM_IP>/sdkapi/sensor/1001/packetcaptureruletemplate?name=test)

### Response

```
{
  "templete": [{
    "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

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
visibleToChild	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

Field Name	Description	Data Type	Mandatory
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/packetcapturetemplate](https://<NSM_IP>/sdkapi/sensor/1001/packetcapturetemplate)

### 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
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

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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](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

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](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
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
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
visibleToChild	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/domain/101/packetcaptureruletemplate?name=test](https://<NSM_IP>/sdkapi/domain/101/packetcaptureruletemplate?name=test)

#### Response

```
{
  "templete": [{
    "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

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](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
visibleToChild	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

Field Name	Description	Data Type	Mandatory
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/packetcapturetemplate/test](https://<NSM_IP>/sdkapi/domain/101/packetcapturetemplate/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
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](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



# 56

## Policy Group Resource

### Contents

- [Get All Policy Group](#)
- [Create Policy Group](#)
- [Get Policy Group](#)
- [Update Policy Group](#)
- [Delete Policy Group](#)

### 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

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



Field Name	Description	Data Type
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](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
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](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

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
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://<NSM\\_IP>/sdkapi/domain/0/policygroup/1](https://<NSM_IP>/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
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](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



# 57

## Policy Assignments Resource

### Contents

- [Get All Policy Assignments Interface](#)
- [Get Policy Assignments Interface](#)
- [Get All Policy Assignments Device](#)
- [Get Policy Assignments Device](#)
- [Update Policy Assignments Interface](#)
- [Update Policy Assignments Device](#)

---

### 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

Field Name	Description	Data Type
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/policyassignments/interface](https://<NSM_IP>/sdkapi/domain/0/policyassignments/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**

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
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/policyassignments/interface/137](https://<NSM_IP>/sdkapi/domain/0/policyassignments/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

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
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](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

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](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**

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
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](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](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

## 58

## Ignore Rules/NTBA Ignore Rules

### Contents

- ▶ [Get the Ignore Rules](#)
- ▶ [Create an Ignore Rule](#)
- ▶ [Update an Ignore Rule](#)
- ▶ [Delete an Ignore Rule](#)

### 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: <ul style="list-style-type: none"><li>• NTBA</li><li>• SENSOR</li></ul>	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 Rules 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: <ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>	string
name	Ignore Rule name	string
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: <ul style="list-style-type: none"> <li>• INBOUND</li> <li>• OUTBOUND</li> <li>• ANY</li> </ul>	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: <ul style="list-style-type: none"> <li>• 0: Resource Type is domain (for domain level rules)</li> <li>• 1: Resource Type is Sensor (for sensor level rules)</li> <li>• 2: Resource Type is Vids (for interface and sub-interface level rules)</li> <li>• 3: Resource Type is NTBA_ZONE (for rules defined for NTBA inside and outside zones)</li> <li>• 4: Resource Type is NTBA_SENSOR (for rules at NTBA level)</li> <li>• 5: Resource Type is NTBA_DOMAIN</li> </ul>	number
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: <ul style="list-style-type: none"><li>• TCP</li><li>• UDP</li><li>• TCP_UDP</li><li>• ANY</li></ul>	string
AttackerPortNumber	<ul style="list-style-type: none"><li>• Port Numbers</li></ul>	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: <ul style="list-style-type: none"><li>• TCP</li><li>• UDP</li><li>• TCP_UDP</li><li>• ANY</li></ul>	string
TargetPortNumber	<ul style="list-style-type: none"><li>• Port Numbers</li></ul>	string

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/domain/0/attackfilter82?context=SENSOR](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](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

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 is active or inactive. The values can be: <ul style="list-style-type: none"><li>• ENABLED</li><li>• DISABLED</li></ul>	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
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: <ul style="list-style-type: none"> <li>• INBOUND</li> <li>• OUTBOUND</li> <li>• ANY</li> </ul>	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: <ul style="list-style-type: none"> <li>• 0: Resource Type is domain (for domain level rules)</li> <li>• 1: Resource Type is Sensor (for sensor level rules)</li> <li>• 2: Resource Type is Vids (for interface and sub-interface level rules)</li> <li>• 3: Resource Type is NTBA_ZONE (for rules defined for NTBA inside and outside zones)</li> <li>• 4: Resource Type is NTBA_SENSOR (for rules at NTBA level)</li> <li>• 5: Resource Type is NTBA_DOMAIN</li> </ul>	number	No
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: <ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• TCP_UDP</li> <li>• ANY</li> </ul>	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: <ul style="list-style-type: none"><li>• TCP</li><li>• UDP</li><li>• TCP_UDP</li><li>• ANY</li></ul>	string	Yes (If not specified default is ANY)
TargetPortNumber	<ul style="list-style-type: none"><li>• Port numbers</li></ul>	string	Yes (not applicable for ANY port type)



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: <ul style="list-style-type: none"><li>• NTBA</li><li>• SENSOR</li></ul>	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](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](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
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: <ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>	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 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: <ul style="list-style-type: none"> <li>• INBOUND</li> <li>• OUTBOUND</li> <li>• ANY</li> </ul>	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)



Field Name	Description	Data Type	Mandatory
resourceType	Indicated the type of interface on which Ignore Rule is created. Its values can be: <ul style="list-style-type: none"> <li>• 0: Resource Type is domain (for domain level rules)</li> <li>• 1: Resource Type is Sensor (for sensor level rules)</li> <li>• 2: Resource Type is Vids (for interface and sub-interface level rules)</li> <li>• 3: Resource Type is NTBA_ZONE (for rules defined for NTBA inside and outside zones)</li> <li>• 4: Resource Type is NTBA_SENSOR (for rules at NTBA level)</li> <li>• 5: Resource Type is NTBA_DOMAIN</li> </ul>	number	NO
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: <ul style="list-style-type: none"> <li>• IPv4 Address Range</li> <li>• IPv4 Endpoint</li> <li>• IPv4 Network</li> <li>• IPv6 Address Range</li> <li>• IPv6 Endpoint</li> <li>• IPv6 Network</li> <li>• Network Group for Exception Object</li> </ul>	string	YES (Default is Match ANY)
AttackerPort	Port type. Its value can be: <ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• TCP_UDP</li> <li>• ANY</li> </ul>	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: <ul style="list-style-type: none"> <li>IPv4 Address Range</li> <li>IPv4 Endpoint</li> <li>IPv4 Network</li> <li>IPv6 Address Range</li> <li>IPv6 Endpoint</li> <li>IPv6 Network</li> <li>Network Group for Exception Object</li> </ul>	string	YES(If not specified, default is MATCH ANY)
TargetPort	Port Type. Its value can be: <ul style="list-style-type: none"> <li>TCP</li> <li>UDP</li> <li>TCP_UDP</li> <li>ANY</li> </ul>	string	YES(If not specified, default is ANY port type)
TargetPortNumber	<ul style="list-style-type: none"> <li>Port Numbers</li> </ul>	string	YES (not applicable for ANY port type)



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: <ul style="list-style-type: none"> <li>NTBA</li> <li>SENSOR</li> </ul>	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](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: <ul style="list-style-type: none"><li>• NTBA</li><li>• SENSOR</li></ul>	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](https://<NSM_IP>/sdkapi/domain/0/attackfilter82/143?context=SENSOR)

#### 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	1408	Invalid Rule id/provided Rule ID is not visible to this domain



## 59

## Inspection Options policy resource

### Contents

- *Get all Inspection Options policy*
- *Get Inspection Options policy*
- *Create Inspection Options policy*
- *Update Inspection Options policy*
- *Delete Inspection Options policy*

---

### 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

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



Field Name	Description	Data Type
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
webserverHuristicAnalysysOptions	Webserver heuristic analysis options	object
webserverDOSOptions	Webserver 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
domainNameWhitelistProcessing	Domain name whitelist processing	string

Field Name	Description	Data Type
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 <ul style="list-style-type: none"> <li>• INBOUND_ONLY</li> <li>• OUTBOUND_ONLY</li> <li>• DISABLED</li> <li>• INBOUND_AND_OUTBOUND</li> </ul>	string
useToInfluenceSmartBlocking	Use to influence SmartBlocking	boolean
excludeInternalEndpoint	Exclude internal endpoint	boolean
cidrsExcluded	CIDRs excluded	stringlist
protocolsExcluded	Protocols excluded	stringlist
urlReputationAnalysis	URL Reputation Analysis	string
urlReputationMinimumRisk	URL Reputation Min Risk	string

Details of webserverHuresticAnalysysOptions:

Field Name	Description	Data Type
huresticAnalysys	Hurestic analysis. Direction value as specified above	string
websitePathToProtect	Options : ALL or SPECIFIC	string
blackListedTextList	Black listed TextList	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

Field Name	Description	Data Type
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,
          "domainNameWhitelistProcessing": true,
          "cidrsExcluded": [],
        },
      },
      "gtiEndpointReputationAnalysysOptions": {
        {
          "gtiEndpointReputationAnalysys": "DISABLED",
          "useToInfluenceSmartBlocking": false,
          "excludeInternalEndpoint": false,
          "cidrsExcluded": [],
          "protocolsExcluded": [],
          "urlReputationAnalysis": null,
          "urlReputationMinimumRisk": null
        },
      },
      "webserverHuresticAnalysysOptions": {
        {
          "huresticAnalysys": "INBOUND_ONLY",
          "websitePathToProtect": "ALL",
          "blackListedTextList": [],
          "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

Field Name	Description	Data Type
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
domainNameWhitelistProcessing	Domain name whitelist 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 <ul style="list-style-type: none"> <li>• INBOUND_ONLY</li> <li>• OUTBOUND_ONLY</li> <li>• DISABLED</li> <li>• INBOUND_AND_OUTBOUND</li> </ul>	string
useToInfluenceSmartBlocking	Use to influence SmartBlocking	boolean
excludeInternalEndpoint	Exclude internal endpoint	boolean
cidrsExcluded	CIDRs excluded	stringlist
protocolsExcluded	Protocols excluded	stringlist
urlReputationAnalysis	URL Reputation Analysis <b>Valid Values:</b> <ul style="list-style-type: none"> <li>• INBOUND_ONLY</li> <li>• OUTBOUND_ONLY</li> <li>• DISABLED</li> <li>• INBOUND_AND_OUTBOUND</li> </ul>	string
urlReputationMinimumRisk	URL Reputation minium risk: <b>Valid Values:</b> <ol style="list-style-type: none"> <li>1 HIGH</li> <li>2 MEDIUM</li> </ol>	string

Details of webserverHuresticAnalysysOptions:

Field Name	Description	Data Type
huresticAnalysys	Hurestic analysis. Direction value as specified above	string
websitePathToProtect	Options : ALL or SPECIFIC	string
blackListedTextList	Black listed TextList	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/](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 codes are 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	Webserver 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
domainNameWhitelistProcessing	Domain name whitelist 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 <ul style="list-style-type: none"> <li>• INBOUND_ONLY</li> <li>• OUTBOUND_ONLY</li> <li>• DISABLED</li> <li>• INBOUND_AND_OUTBOUND</li> </ul>	string
useToInfluenceSmartBlocking	Use to influence SmartBlocking	boolean
excludeInternalEndpoint	Exclude internal endpoint	boolean
cidrsExcluded	CIDRs excluded	stringlist
protocolsExcluded	Protocols excluded	stringlist
urlReputationAnalysis	URL Reputation Analysis	string
urlReputationMinimumRisk	URL Reputation minium risk: <b>Valid Values:</b> 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
blackListedTextList	Black listed TextList	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](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",
      "blackListedTextList": [],
      "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 codes are 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](https://<NSM_IP>/sdkapi/protectionoptionspolicy/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

## Contents

- *Get the DXL Integration Configuration for domain*
- *Update the DXL Integration Configuration for domain*
- *Get the DXL Integration Configuration for Sensor*
- *Update the DXL Integration Configuration for Sensor*

---

## 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](https://<NSM_IP>/sdkapi/domain/0/dxlintegration)

#### Response

```
{
  "inheritSettings": true,
  "enableDXL": true
}
```

### Error Information

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](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](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**

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 8.3

**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 8.3
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



# 61

## Threat Explorer Resource

### Contents

- ▶ *Get the Threat explorer data*
- ▶ *Get the List of top attackers*
- ▶ *Get the List of top attacks*
- ▶ *Get the List of top targets*
- ▶ *Get the List of top attack applications*
- ▶ *Get the List of top malwares*
- ▶ *Get the list of top executables*

### 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: <ul style="list-style-type: none"> <li>• LAST_5_MINUTES</li> <li>• LAST_1_HOUR</li> <li>• LAST_6_HOURS</li> <li>• LAST_12_HOURS</li> <li>• LAST_24_HOURS</li> <li>• LAST_48_HOURS</li> <li>• LAST_7_DAYS</li> <li>• LAST_14_DAYS</li> </ul>	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: <ul style="list-style-type: none"> <li>• group(default)</li> <li>• filter</li> </ul>	string	No
value	<p>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 "::::".</p> <p>The format of value will be &lt;filter_name1&gt;=&lt;filter_value&gt;:::&lt;filter_name2&gt;=&lt;filter_value&gt; .</p> <p>The filter_name's and filter_values allowed are:</p> <ul style="list-style-type: none"> <li>• attack -&gt; value should be a valid attack name.</li> <li>• severity -&gt; value can be High, Low, Medium &amp; Informational (all are case sensitive).</li> <li>• category -&gt; value should be a valid category.</li> <li>• subCategory -&gt; value should be a valid sub category.</li> <li>• attackerIp -&gt; value should be a valid IP.</li> <li>• dnsName -&gt; value should be a string.</li> <li>• country -&gt; value should be a valid country name.</li> <li>• user -&gt; value should be a valid user name/unknown.</li> <li>• victimIp -&gt; value should be a valid IP.</li> <li>• victimDnsName -&gt; value should be a string.</li> <li>• victimCountry -&gt; value should be a valid country name.</li> <li>• victimUser -&gt; value should be a valid user name/unknown.</li> <li>• applicationName -&gt; value should be a valid application name.</li> <li>• applicationRisk -&gt; value can be high, low &amp; medium.</li> <li>• applicationCategory -&gt; value should be a valid application category.</li> <li>• fileHash -&gt; value should be a string.</li> <li>• executableHash -&gt; value should be a string.</li> <li>• malwareConfidence -&gt; value should be a valid malware confidence.</li> <li>• fileSize -&gt; value should be a number.</li> <li>• executableConfidence -&gt; value can be clean, high, low, medium, unknown,</li> </ul>	string	No

Field Name	Description	Data Type	Mandatory
	veryhigh & verylow. <ul style="list-style-type: none"><li>executableClassification -&gt; value can be blacklisted, none, unclassified &amp; whitelisted.</li><li>executableName</li></ul>		

## 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 TETopAttacks explained in 1.2.3	object
topAttackers	List of all the top attackers. The data is same as TETopAttackers explained in 1.3.3	object
topTargets	List of all the top targets. The data is same as TETopTargets explained in 1.4.3	object
topAttackApplications	List of all the top attack applications. The data is same as TETopAttackApplications explained in 1.5.3	object
topAttackExecutables	List of all the top executables. The data is same as TETopExecutables explained in 1.7.3	object
topMalware	List of all the top malwares. The data is same as TETopMalwareDownloads 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 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: <ul style="list-style-type: none"><li>• LAST_5_MINUTES</li><li>• LAST_1_HOUR</li><li>• LAST_6_HOURS</li><li>• LAST_12_HOURS</li><li>• LAST_24_HOURS</li><li>• LAST_48_HOURS</li><li>• LAST_7_DAYS</li><li>• LAST_14_DAYS</li></ul>	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 : <ul style="list-style-type: none"> <li>• group(default)</li> <li>• filter</li> </ul>	string	No
value	<p>If action is group, the values allowed are:</p> <ul style="list-style-type: none"> <li>• attackerIp (default)</li> <li>• dnsName</li> <li>• country</li> <li>• user</li> </ul> <p>If the action is filter.</p> <p>We can give multiple filters separated by "::::".</p> <p>The format of value will be &lt;filter_name1&gt;=&lt;filter_value&gt;::: &lt;filter_name2&gt;=&lt;filter_value&gt; .</p> <p>The filter_name's and filter_values allowed are:</p> <ul style="list-style-type: none"> <li>• attack -&gt; value should be a valid attack name.</li> <li>• severity -&gt; value can be High, Low, Medium &amp; Informational (all are case sensitive).</li> <li>• category -&gt; value should be a valid category.</li> <li>• subCategory -&gt; value should be a valid sub category.</li> <li>• attackerIp -&gt; value should be a valid IP.</li> <li>• dnsName -&gt; value should be a string.</li> <li>• country -&gt; value should be a valid country name.</li> <li>• user -&gt; value should be a valid user name/unknown.</li> <li>• victimIp -&gt; value should be a valid IP.</li> <li>• victimDnsName -&gt; value should be a string.</li> <li>• victimCountry -&gt; value should be a valid country name.</li> <li>• victimUser -&gt; value should be a valid user name/unknown.</li> <li>• applicationName -&gt; value should be a valid application name.</li> <li>• applicationRisk -&gt; value can be high, low &amp; medium.</li> <li>• applicationCategory -&gt; value should be a valid application category.</li> <li>• fileHash -&gt; value should be a string.</li> <li>• executableHash -&gt; value should be a string.</li> <li>• malwareConfidence -&gt; value should be a</li> </ul>	string	No



Field Name	Description	Data Type	Mandatory
	valid malware confidence. <ul style="list-style-type: none"><li>• fileSize -&gt; value should be a number.</li><li>• executableConfidence -&gt; value can be clean, high, low, medium, unknown, veryhigh &amp; verylow.</li><li>• executableClassification -&gt; value can be blacklisted, none, unclassified &amp; whitelisted.</li><li>• executableName</li></ul>		

### Response Parameters

Following fields are returned.

Field Name	Description	Data Type
TETopAttackers	List of top attackers. Contains TETopAttackersList	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](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
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 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: <ul style="list-style-type: none"> <li>• LAST_5_MINUTES</li> <li>• LAST_1_HOUR</li> <li>• LAST_6_HOURS</li> <li>• LAST_12_HOURS</li> <li>• LAST_24_HOURS</li> <li>• LAST_48_HOURS</li> <li>• LAST_7_DAYS</li> <li>• LAST_14_DAYS</li> </ul>	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: <ul style="list-style-type: none"><li>• group(default)</li><li>• filter</li></ul>	string	No
value	<p>If action is group, the values allowed are:</p> <ul style="list-style-type: none"><li>• attack (default)</li><li>• severity</li><li>• category</li><li>• subCategory</li></ul> <p>If the action is filter.</p> <p>We can give multiple filters separated by "::::".</p> <p>The format of value will be &lt;filter_name1&gt;=&lt;filter_value&gt;::: &lt;filter_name2&gt;=&lt;filter_value&gt; .</p> <p>The filter_name's and filter_values allowed are:</p> <ul style="list-style-type: none"><li>• attack -&gt; value should be a valid attack name.</li><li>• severity -&gt; value can be High, Low, Medium &amp; Informational (all are case sensitive).</li><li>• category -&gt; value should be a valid category.</li><li>• subCategory -&gt; value should be a valid sub category.</li><li>• attackerIp -&gt; value should be a valid IP.</li><li>• dnsName -&gt; value should be a string.</li><li>• country -&gt; value should be a valid country name.</li><li>• user -&gt; value should be a valid user name/unknown.</li><li>• victimIp -&gt; value should be a valid IP.</li><li>• victimDnsName -&gt; value should be a string.</li><li>• victimCountry -&gt; value should be a valid country name.</li><li>• victimUser -&gt; value should be a valid user name/unknown.</li><li>• applicationName -&gt; value should be a valid application name.</li><li>• applicationRisk -&gt; value can be high, low &amp; medium.</li><li>• applicationCategory -&gt; value should be a valid application category.</li><li>• fileHash -&gt; value should be a string.</li><li>• executableHash -&gt; value should be a string.</li><li>• malwareConfidence -&gt; value should be a</li></ul>	string	No

Field Name	Description	Data Type	Mandatory
	valid malware confidence. <ul style="list-style-type: none"> <li>• fileSize -&gt; value should be a number.</li> <li>• executableConfidence -&gt; value can be clean, high, low, medium, unknown, veryhigh &amp; verylow.</li> <li>• executableClassification -&gt; value can be blacklisted, none, unclassified &amp; whitelisted.</li> <li>• executableName</li> </ul>		

## Response Parameters

Following fields are returned.

Field Name	Description	Data Type
TETopAttacks	List of top attacks. Contains TETopAttacksList	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](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
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: <ul style="list-style-type: none"><li>• LAST_5_MINUTES</li><li>• LAST_1_HOUR</li><li>• LAST_6_HOURS</li><li>• LAST_12_HOURS</li><li>• LAST_24_HOURS</li><li>• LAST_48_HOURS</li><li>• LAST_7_DAYS</li><li>• LAST_14_DAYS</li></ul>	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 : <ul style="list-style-type: none"> <li>• group(default)</li> <li>• filter</li> </ul>	string	No
value	<p>If action is group, the values allowed are:</p> <ul style="list-style-type: none"> <li>• victimIp(default)</li> <li>• victimDnsName</li> <li>• victimCountry</li> <li>• victimUser</li> </ul> <p>If the action is filter.</p> <p>We can give multiple filters separated by "::::".</p> <p>The format of value will be &lt;filter_name1&gt;=&lt;filter_value&gt;::: &lt;filter_name2&gt;=&lt;filter_value&gt; .</p> <p>The filter_name's and filter_values allowed are:</p> <ul style="list-style-type: none"> <li>• attack -&gt; value should be a valid attack name.</li> <li>• severity -&gt; value can be High, Low, Medium &amp; Informational (all are case sensitive).</li> <li>• category -&gt; value should be a valid category.</li> <li>• subCategory -&gt; value should be a valid sub category.</li> <li>• attackerIp -&gt; value should be a valid IP.</li> <li>• dnsName -&gt; value should be a string.</li> <li>• country -&gt; value should be a valid country name.</li> <li>• user -&gt; value should be a valid user name/unknown.</li> <li>• victimIp -&gt; value should be a valid IP.</li> <li>• victimDnsName -&gt; value should be a string.</li> <li>• victimCountry -&gt; value should be a valid country name.</li> <li>• victimUser -&gt; value should be a valid user name/unknown.</li> <li>• applicationName -&gt; value should be a valid application name.</li> <li>• applicationRisk -&gt; value can be high, low &amp; medium.</li> <li>• applicationCategory -&gt; value should be a valid application category.</li> <li>• fileHash -&gt; value should be a string.</li> <li>• executableHash -&gt; value should be a string.</li> <li>• malwareConfidence -&gt; value should be a</li> </ul>	string	No

Field Name	Description	Data Type	Mandatory
	valid malware confidence. <ul style="list-style-type: none"><li>• fileSize -&gt; value should be a number.</li><li>• executableConfidence -&gt; value can be clean, high, low, medium, unknown, veryhigh &amp; verylow.</li><li>• executableClassification -&gt; value can be blacklisted, none, unclassified &amp; whitelisted.</li><li>• executableName</li></ul>		

### Response Parameters

Following fields are returned.

Field Name	Description	Data Type
TETopTargets	List of top targets. Contains TETopTargetsList	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](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: <ul style="list-style-type: none"> <li>• LAST_5_MINUTES</li> <li>• LAST_1_HOUR</li> <li>• LAST_6_HOURS</li> <li>• LAST_12_HOURS</li> <li>• LAST_24_HOURS</li> <li>• LAST_48_HOURS</li> <li>• LAST_7_DAYS</li> <li>• LAST_14_DAYS</li> </ul>	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 : <ul style="list-style-type: none"><li>• group(default)</li><li>• filter</li></ul>	string	No
value	If action is group, the values allowed are: <ul style="list-style-type: none"><li>• applicationName(default)</li><li>• applicationRisk</li><li>• applicationCategory</li></ul> 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: <ul style="list-style-type: none"><li>• attack -&gt; value should be a valid attack name.</li><li>• severity -&gt; value can be High, Low, Medium &amp; Informational (all are case sensitive).</li><li>• category -&gt; value should be a valid category.</li><li>• subCategory -&gt; value should be a valid sub category.</li><li>• attackerIp -&gt; value should be a valid IP.</li><li>• dnsName -&gt; value should be a string.</li><li>• country -&gt; value should be a valid country name.</li><li>• user -&gt; value should be a valid user name/unknown.</li><li>• victimIp -&gt; value should be a valid IP.</li><li>• victimDnsName -&gt; value should be a string.</li><li>• victimCountry -&gt; value should be a valid country name.</li><li>• victimUser -&gt; value should be a valid user name/unknown.</li><li>• applicationName -&gt; value should be a valid application name.</li><li>• applicationRisk -&gt; value can be high, low &amp; medium.</li><li>• applicationCategory -&gt; value should be a valid application category.</li><li>• fileHash -&gt; value should be a string.</li><li>• executableHash -&gt; value should be a string.</li><li>• malwareConfidence -&gt; value should be a</li></ul>	string	No

Field Name	Description	Data Type	Mandatory
	valid malware confidence. <ul style="list-style-type: none"> <li>• fileSize -&gt; value should be a number.</li> <li>• executableConfidence -&gt; value can be clean, high, low, medium, unknown, veryhigh &amp; verylow.</li> <li>• executableClassification -&gt; value can be blacklisted, none, unclassified &amp; whitelisted.</li> <li>• executableName</li> </ul>		

### Response Parameters

Following fields are returned.

Field Name	Description	Data Type
TETopAttackApplications	List of top attack applications. Contains TETopAttackApplicationsList	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](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: <ul style="list-style-type: none"><li>• LAST_5_MINUTES</li><li>• LAST_1_HOUR</li><li>• LAST_6_HOURS</li><li>• LAST_12_HOURS</li><li>• LAST_24_HOURS</li><li>• LAST_48_HOURS</li><li>• LAST_7_DAYS</li><li>• LAST_14_DAYS</li></ul>	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 : <ul style="list-style-type: none"> <li>• group(default)</li> <li>• filter</li> </ul>	string	No
value	<p>If action is group, the values allowed are:</p> <ul style="list-style-type: none"> <li>• fileHash (default)</li> <li>• malwareConfidence</li> <li>• fileSize</li> </ul> <p>If the action is filter.</p> <p>We can give multiple filters separated by "::::".</p> <p>The format of value will be &lt;filter_name1&gt;=&lt;filter_value&gt;::::&lt;filter_name2&gt;=&lt;filter_value&gt; .</p> <p>The filter_name's and filter_values allowed are:</p> <ul style="list-style-type: none"> <li>• attack -&gt; value should be a valid attack name.</li> <li>• severity -&gt; value can be High, Low, Medium &amp; Informational (all are case sensitive).</li> <li>• category -&gt; value should be a valid category.</li> <li>• subCategory -&gt; value should be a valid sub category.</li> <li>• attackerIp -&gt; value should be a valid IP.</li> <li>• dnsName -&gt; value should be a string.</li> <li>• country -&gt; value should be a valid country name.</li> <li>• user -&gt; value should be a valid user name/unknown.</li> <li>• victimIp -&gt; value should be a valid IP.</li> <li>• victimDnsName -&gt; value should be a string.</li> <li>• victimCountry -&gt; value should be a valid country name.</li> <li>• victimUser -&gt; value should be a valid user name/unknown.</li> <li>• applicationName -&gt; value should be a valid application name.</li> <li>• applicationRisk -&gt; value can be high, low &amp; medium.</li> <li>• applicationCategory -&gt; value should be a valid application category.</li> <li>• fileHash -&gt; value should be a string.</li> <li>• executableHash -&gt; value should be a string.</li> <li>• malwareConfidence -&gt; value should be a</li> </ul>	string	No

Field Name	Description	Data Type	Mandatory
	<p>valid malware confidence.</p> <ul style="list-style-type: none"><li>• fileSize -&gt; value should be a number.</li><li>• executableConfidence -&gt; value can be clean, high, low, medium, unknown, veryhigh &amp; verylow.</li><li>• executableClassification -&gt; value can be blacklisted, none, unclassified &amp; whitelisted.</li><li>• executableName</li></ul>		

### Response Parameters

Following fields are returned.

Field Name	Description	Data Type
TETopMalware	List of top malwares. Contains TETopMalwareDownloadsList	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](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: <ul style="list-style-type: none"> <li>• LAST_5_MINUTES</li> <li>• LAST_1_HOUR</li> <li>• LAST_6_HOURS</li> <li>• LAST_12_HOURS</li> <li>• LAST_24_HOURS</li> <li>• LAST_48_HOURS</li> <li>• LAST_7_DAYS</li> <li>• LAST_14_DAYS</li> </ul>	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 : <ul style="list-style-type: none"> <li>• group(default)</li> <li>• filter</li> </ul>	string	No
value	<p>If action is group, the values allowed are:</p> <ul style="list-style-type: none"> <li>• executableHash(default)</li> <li>• executableConfidence</li> <li>• executableClassification</li> <li>• executableName</li> </ul> <p>If the action is filter.</p> <p>We can give multiple filters separated by "::::".</p> <p>The format of value will be &lt;filter_name1&gt;=&lt;filter_value&gt;::: &lt;filter_name2&gt;=&lt;filter_value&gt; .</p> <p>The filter_name's and filter_values allowed are:</p> <ul style="list-style-type: none"> <li>• attack -&gt; value should be a valid attack name.</li> <li>• severity -&gt; value can be High, Low, Medium &amp; Informational (all are case sensitive).</li> <li>• category -&gt; value should be a valid category.</li> <li>• subCategory -&gt; value should be a valid sub category.</li> <li>• attackerIp -&gt; value should be a valid IP.</li> <li>• dnsName -&gt; value should be a string.</li> <li>• country -&gt; value should be a valid country name.</li> <li>• user -&gt; value should be a valid user name/unknown.</li> <li>• victimIp -&gt; value should be a valid IP.</li> <li>• victimDnsName -&gt; value should be a string.</li> <li>• victimCountry -&gt; value should be a valid country name.</li> <li>• victimUser -&gt; value should be a valid user name/unknown.</li> <li>• applicationName -&gt; value should be a valid application name.</li> <li>• applicationRisk -&gt; value can be high, low &amp; medium.</li> <li>• applicationCategory -&gt; value should be a valid application category.</li> <li>• fileHash -&gt; value should be a string.</li> <li>• executableHash -&gt; value should be a string.</li> <li>• malwareConfidence -&gt; value should be a</li> </ul>	string	No

Field Name	Description	Data Type	Mandatory
	valid malware confidence. <ul style="list-style-type: none"> <li>• fileSize -&gt; value should be a number.</li> <li>• executableConfidence -&gt; value can be clean, high, low, medium, unknown, veryhigh &amp; verylow.</li> <li>• executableClassification -&gt; value can be blacklisted, none, unclassified &amp; whitelisted.</li> <li>• executableName</li> </ul>		

## Response Parameters

Following fields are returned.

Field Name	Description	Data Type
TETopExecutables	List of top executables. Contains TETopExecutablesList	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](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": "Whitelisted",
      "attackCount": 327
    },
    {
      "executableHash": "fb104d17018b4ca9f0c1a9bed02d15fc",
      "executableConfidence": "veryLow",
      "executableName": "firefox.exe",
      "executableClassification": "Whitelisted",
      "attackCount": 13
    },
    {
      "executableHash": "f71d97b6b631d565af7c6e0bdf9d49f4",
```



```
        "executableConfidence": "veryLow",
        "executableName": "IEXPLORE.EXE.MUI",
        "executableClassification": "Whitelisted",
        "attackCount": 6
    },
    {
        "executableHash": "bcd9cbf0621f9a6767276a2e0bf1dd15",
        "executableConfidence": "veryLow",
        "executableName": "googletalk.exe",
        "executableClassification": "Whitelisted",
        "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



**Contents**

- *Get Host Summary*
- *Get Top Suspicious Flows*

---

**Get Host Summary**

This URL retrieves the host analysis summary for given IP Address for the time frame.

**Resource URL**

GET /networkforensics/<ipaddress>?starttime=<start\_time>&&duration=<duration>&&ntba=<ntba\_id>

URL Parameters: **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**

**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
zone	Zone	string
country	Country	string
etf	Etf	string
dataSource	Data dource	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](https://<NSM_IP>/sdkapi/networkforensics/1.1.1.1/?duration=NEXT_30_MINUTES&&starttime=2012-APR-20%2012:15&ntba=1001)

## Response

```
{
  " endpointSummary ":
    {
      " analysisWindow ": "",
      " zone ": "South",
      " country ": "India",
      " dataSource ": "Whitelisted",
      " 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 ?  
starttime=<start\_time>&&duration=<duration>&&ntba=<ntba\_id>

URL Parameters: **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**

## 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	Suspcious activity	string
sourceEndpoint	Source host	string
sourcePort	Source port	number
sourceEcecutable	Source executable name	string
destinationEndpoint	Destination Endpoint	string
destinationPort	Destination port	number
applications	Application names	string
attackName	Attacck 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](https://<NSM_IP>/sdkapi/networkforensics/1.1.1.1/suspiciousflows?duration=NEXT_30_MINUTES&&starttime=2012-APR-20%2012:15&ntba=1001)

### Response

```
{
  "suspiciousFlows":
  [
    {
      " time ": "10-Aug-2014 12:00",
      " suspciousActivity ": "",
      " sourceEcecutable ": "BitTorrent.exe",
      "executableClassification": "Whitelisted",
      "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





## Gateway Anti-Malware Update Resource

### Contents

- *Get the Gateway Anti-Malware Updating Configuration for domain*
- *Update the Gateway Anti-Malware Updating Configuration for domain*
- *Get the Gateway Anti-Malware Updating Configuration for sensor*
- *Update the Gateway Anti-Malwares Updating Configuration for sensor*

---

### 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](https://<NSM_IP>/sdkapi/domain/0/gamupdatesettings)

##### Response

```
{
  "inheritSettings": false,
  "enableAutoUpdate": false,
  "updateInterval": "6 hrs"
}
```

### Error Information

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](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	GAM 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](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

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	GAM 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](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"]



# 64 User Resource

## Contents

- *Get the User Details*
- *Create a user*
- *Update a User*
- *Delete a User*

## 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
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	<p>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.</p> <ul style="list-style-type: none"> <li>• ePO Dashboard Data Retriever</li> <li>• NOC Operator</li> <li>• Report Generator</li> <li>• Security Expert</li> <li>• Super User</li> <li>• System Administrator</li> <li>• No Role</li> </ul> <p> In addition to the above mentioned roles, the user can also be assigned a custom created role.</p>	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](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

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

Field Name	Description	Data Type	Mandatory
phone	Contact number of the user	string	No
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	<p>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.</p> <ul style="list-style-type: none"> <li>• ePO Dashboard Data Retriever</li> <li>• NOC Operator</li> <li>• Report Generator</li> <li>• Security Expert</li> <li>• Super User</li> <li>• System Administrator</li> <li>• No Role</li> </ul> <p>In addition to the above mentioned roles, the user can also be assigned a custom created role.</p>	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](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	<p>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.</p> <ul style="list-style-type: none"> <li>• ePO Dashboard Data Retriever</li> <li>• NOC Operator</li> <li>• Report Generator</li> <li>• Security Expert</li> <li>• Super User</li> <li>• System Administrator</li> <li>• No Role</li> </ul> <p>In addition to the above mentioned roles, the user can also be assigned a Custom created role.</p>	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](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](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 userId





## 65

## Alert Pruning Resource

### 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](https://<NSM_IP>/sdkapi/Maintenance/prunealerts)

Payload

```
{
  "enableAlertPruning": "true",
  "pruningStartTime": "12:40",
  "maxAlertsToStoreForDashboard": "10000",
  "maxAlertsToStoreForReport": "10000",
  "maxAlertAgeForReport": "20"
}
```

Response

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

Error Information

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

# 66

## Custom Role Resource

### Contents

- [Get the Details of Custom roles](#)
- [Create a Role](#)
- [Delete a Role](#)

---

### 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: <ul style="list-style-type: none"><li>• Manage Manager - View Only</li><li>• NTBA Policy - Edit</li><li>• Deploy Changes - IPS etc.</li></ul> 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](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: <ul style="list-style-type: none"> <li>• Manage Manager - View Only</li> <li>• NTBA Policy - Edit</li> <li>• Deploy Changes - IPS etc.</li> </ul> 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](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
2	400	9505	At least one role privilege is required

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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

# 67

## Direct Syslog Resource

### Contents

- *Get the Direct Syslog Configuration for the domain*
- *Update the Direct Syslog Configuration for the domain*
- *Get the Direct Syslog Configuration for the Sensor*
- *Update the Direct Syslog Configuration for the Sensor*
- *Test the Direct Syslog Configuration for domain*
- *Test the Direct Syslog Configuration for the Sensor*

---

### Get the Direct Syslog Configuration for the domain

This URL retrieves the DXL Integration 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
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](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=$IV_ATTACK_TIME$Quarantine_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

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	400	6001	Direct Syslog 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

Field Name	Description	Data Type	Mandatory
syslogFacility	Syslog Facility. Allowed values are: <ul style="list-style-type: none"> <li>SECURITY_AUTHORIZATION_CODE_10</li> <li>SECURITY_AUTHORIZATION_CODE_4</li> <li>LOG_AUDIT_NOTE_1</li> <li>LOG_ALERT_NOTE_1</li> <li>CLOCK_DAEMON_NOTE_2</li> <li>LOCAL_USER_0</li> <li>LOCAL_USER_1</li> <li>LOCAL_USER_2</li> <li>LOCAL_USER_3</li> <li>LOCAL_USER_4</li> <li>LOCAL_USER_5</li> <li>LOCAL_USER_6</li> <li>LOCAL_USER_7</li> </ul>	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: <ul style="list-style-type: none"> <li>EMERGENCY_SYSTEM_UNUSABLE</li> <li>ALERT_ACTION_IMMEDIATELY</li> <li>CRITICAL_CONDITIONS</li> <li>ERROR</li> <li>WARNING_CONDITIONS</li> <li>NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>INFORMATIONAL_MESSAGES</li> <li>DEBUG_MESSAGES</li> </ul>	string	Yes
lowTo	Low severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>EMERGENCY_SYSTEM_UNUSABLE</li> <li>ALERT_ACTION_IMMEDIATELY</li> <li>CRITICAL_CONDITIONS</li> <li>ERROR</li> <li>WARNING_CONDITIONS</li> <li>NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>INFORMATIONAL_MESSAGES</li> <li>DEBUG_MESSAGES</li> </ul>	string	Yes

Field Name	Description	Data Type	Mandatory
mediumTO	Medium severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>EMERGENCY_SYSTEM_UNUSABLE</li> <li>ALERT_ACTION_IMMEDIATELY</li> <li>CRITICAL_CONDITIONS</li> <li>ERROR</li> <li>WARNING_CONDITIONS</li> <li>NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>INFORMATIONAL_MESSAGES</li> <li>DEBUG_MESSAGES</li> </ul>	string	yes
highTo	High severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>EMERGENCY_SYSTEM_UNUSABLE</li> <li>ALERT_ACTION_IMMEDIATELY</li> <li>CRITICAL_CONDITIONS</li> <li>ERROR</li> <li>WARNING_CONDITIONS</li> <li>NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>INFORMATIONAL_MESSAGES</li> <li>DEBUG_MESSAGES</li> </ul>	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: <ul style="list-style-type: none"> <li>INFORMATIONAL</li> <li>LOW</li> <li>MEDIUM</li> <li>HIGH</li> </ul>	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](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=$IV_ATTACK_TIME$Quarantine_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
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](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=$IV_ATTACK_TIME$Quarantine_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

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: <ul style="list-style-type: none"> <li>SECURITY_AUTHORIZATION_CODE_10</li> <li>SECURITY_AUTHORIZATION_CODE_4</li> <li>LOG_AUDIT_NOTE_1</li> <li>LOG_ALERT_NOTE_1</li> <li>CLOCK_DAEMON_NOTE_2</li> <li>LOCAL_USER_0</li> <li>LOCAL_USER_1</li> <li>LOCAL_USER_2</li> <li>LOCAL_USER_3</li> <li>LOCAL_USER_4</li> <li>LOCAL_USER_5</li> <li>LOCAL_USER_6</li> <li>LOCAL_USER_7</li> </ul>	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: <ul style="list-style-type: none"> <li>• EMERGENCY_SYSTEM_UNUSABLE</li> <li>• ALERT_ACTION_IMMEDIATELY</li> <li>• CRITICAL_CONDITIONS</li> <li>• ERROR</li> <li>• WARNING_CONDITIONS</li> <li>• NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>• INFORMATIONAL_MESSAGES</li> <li>• DEBUG_MESSAGES</li> </ul>	string	Yes
lowTo	Low severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>• EMERGENCY_SYSTEM_UNUSABLE</li> <li>• ALERT_ACTION_IMMEDIATELY</li> <li>• CRITICAL_CONDITIONS</li> <li>• ERROR</li> <li>• WARNING_CONDITIONS</li> <li>• NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>• INFORMATIONAL_MESSAGES</li> <li>• DEBUG_MESSAGES</li> </ul>	string	Yes
mediumTo	Medium severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>• EMERGENCY_SYSTEM_UNUSABLE</li> <li>• ALERT_ACTION_IMMEDIATELY</li> <li>• CRITICAL_CONDITIONS</li> <li>• ERROR</li> <li>• WARNING_CONDITIONS</li> <li>• NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>• INFORMATIONAL_MESSAGES</li> <li>• DEBUG_MESSAGES</li> </ul>	string	yes
highTo	High severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>• EMERGENCY_SYSTEM_UNUSABLE</li> <li>• ALERT_ACTION_IMMEDIATELY</li> <li>• CRITICAL_CONDITIONS</li> <li>• ERROR</li> <li>• WARNING_CONDITIONS</li> <li>• NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>• INFORMATIONAL_MESSAGES</li> <li>• DEBUG_MESSAGES</li> </ul>	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: <ul style="list-style-type: none"><li>• INFORMATIONAL</li><li>• LOW</li><li>• MEDIUM</li><li>• HIGH</li></ul>	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](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=$IV_ATTACK_TIME$Quarantine_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
serverIp	Syslog server IP	string	Yes
serverPort	Syslog server port (UDP)	number	Yes

Field Name	Description	Data Type	Mandatory
syslogFacility	<p>Syslog Facility. Allowed values are:</p> <ul style="list-style-type: none"> <li>• SECURITY_AUTHORIZATION_CODE_10</li> <li>• SECURITY_AUTHORIZATION_CODE_4</li> <li>• LOG_AUDIT_NOTE_1</li> <li>• LOG_ALERT_NOTE_1</li> <li>• CLOCK_DAEMON_NOTE_2</li> <li>• LOCAL_USER_0</li> <li>• LOCAL_USER_1</li> <li>• LOCAL_USER_2</li> <li>• LOCAL_USER_3</li> <li>• LOCAL_USER_4</li> <li>• LOCAL_USER_5</li> <li>• LOCAL_USER_6</li> <li>• LOCAL_USER_7</li> </ul>	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	<p>Informational severity attack mapping. Values allowed are:</p> <ul style="list-style-type: none"> <li>• EMERGENCY_SYSTEM_UNUSABLE</li> <li>• ALERT_ACTION_IMMEDIATELY</li> <li>• CRITICAL_CONDITIONS</li> <li>• ERROR</li> <li>• WARNING_CONDITIONS</li> <li>• NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>• INFORMATIONAL_MESSAGES</li> <li>• DEBUG_MESSAGES</li> </ul>	string	Yes
lowTo	<p>Low severity attack mapping. Values allowed are:</p> <ul style="list-style-type: none"> <li>• EMERGENCY_SYSTEM_UNUSABLE</li> <li>• ALERT_ACTION_IMMEDIATELY</li> <li>• CRITICAL_CONDITIONS</li> <li>• ERROR</li> <li>• WARNING_CONDITIONS</li> <li>• NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>• INFORMATIONAL_MESSAGES</li> <li>• DEBUG_MESSAGES</li> </ul>	string	Yes

Field Name	Description	Data Type	Mandatory
mediumTO	Medium severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>• EMERGENCY_SYSTEM_UNUSABLE</li> <li>• ALERT_ACTION_IMMEDIATELY</li> <li>• CRITICAL_CONDITIONS</li> <li>• ERROR</li> <li>• WARNING_CONDITIONS</li> <li>• NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>• INFORMATIONAL_MESSAGES</li> <li>• DEBUG_MESSAGES</li> </ul>	string	yes
highTo	High severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>• EMERGENCY_SYSTEM_UNUSABLE</li> <li>• ALERT_ACTION_IMMEDIATELY</li> <li>• CRITICAL_CONDITIONS</li> <li>• ERROR</li> <li>• WARNING_CONDITIONS</li> <li>• NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>• INFORMATIONAL_MESSAGES</li> <li>• DEBUG_MESSAGES</li> </ul>	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: <ul style="list-style-type: none"> <li>• INFORMATIONAL</li> <li>• LOW</li> <li>• MEDIUM</li> <li>• HIGH</li> </ul>	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](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=$IV_ATTACK_TIME$Quarantine_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: <ul style="list-style-type: none"> <li>SECURITY_AUTHORIZATION_CODE_10 • LOCAL_USER_2</li> <li>SECURITY_AUTHORIZATION_CODE_4 • LOCAL_USER_3</li> <li>LOG_AUDIT_NOTE_1 • LOCAL_USER_4</li> <li>LOG_ALERT_NOTE_1 • LOCAL_USER_5</li> <li>CLOCK_DAEMON_NOTE_2 • LOCAL_USER_6</li> <li>LOCAL_USER_0 • LOCAL_USER_7</li> <li>LOCAL_USER_1</li> </ul>	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: <ul style="list-style-type: none"> <li>• EMERGENCY_SYSTEM_UNUSABLE</li> <li>• ALERT_ACTION_IMMEDIATELY</li> <li>• CRITICAL_CONDITIONS</li> <li>• ERROR</li> <li>• WARNING_CONDITIONS</li> <li>• NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>• INFORMATIONAL_MESSAGES</li> <li>• DEBUG_MESSAGES</li> </ul>	string	Yes
lowTo	Low severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>• EMERGENCY_SYSTEM_UNUSABLE</li> <li>• ALERT_ACTION_IMMEDIATELY</li> <li>• CRITICAL_CONDITIONS</li> <li>• ERROR</li> <li>• WARNING_CONDITIONS</li> <li>• NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>• INFORMATIONAL_MESSAGES</li> <li>• DEBUG_MESSAGES</li> </ul>	string	Yes
mediumTo	Medium severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>• EMERGENCY_SYSTEM_UNUSABLE</li> <li>• ALERT_ACTION_IMMEDIATELY</li> <li>• CRITICAL_CONDITIONS</li> <li>• ERROR</li> <li>• WARNING_CONDITIONS</li> <li>• NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>• INFORMATIONAL_MESSAGES</li> <li>• DEBUG_MESSAGES</li> </ul>	string	yes
highTo	High severity attack mapping. Values allowed are: <ul style="list-style-type: none"> <li>• EMERGENCY_SYSTEM_UNUSABLE</li> <li>• ALERT_ACTION_IMMEDIATELY</li> <li>• CRITICAL_CONDITIONS</li> <li>• ERROR</li> <li>• WARNING_CONDITIONS</li> <li>• NOTICE_NORAML_BUT_SIGNIFICANT_CONDITION</li> <li>• INFORMATIONAL_MESSAGES</li> <li>• DEBUG_MESSAGES</li> </ul>	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: <ul style="list-style-type: none"> <li>• INFORMATIONAL</li> <li>• LOW</li> <li>• MEDIUM</li> <li>• HIGH</li> </ul>	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](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=$IV_ATTACK_TIME$Quarantine_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



## Contents

- *Get the Radius Configuration for domain*
- *Update the Radius Configuration for the domain*

## 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
secondaryRadiusServer	Secondary 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 secondaryRadiusServer:

Field Name	Description	Data Type
serverIpAddr	IP address	string
sharedSecret	Shared secret key	string

Field Name	Description	Data Type
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](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
    },
  "seconddayRadiusServer":
    {
      "serverIpAddr": "1.1.1.5",
      "sharedSecret": "dssdfksdnfsdf",
      "authenticationPort": 1812,
      "connectionTimeoutInSeconds": 6,
      "enableAccounting": false,
      "accountingPort": 1813
    }
}
```

### Error Information

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 th 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
secondaryRadiusServer	Secondary 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 secondaryRadiusServer:

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

### 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/radius](https://<NSM_IP>/sdkapi/domain/0/remoteaccess/radius)

#### Payload

```
{
  "inheritSettings": false,
  "enableRadiusCLIAuthentication": true,
  "primaryRadiusServer": {
    "serverIpAddr": "1.1.1.3",
    "sharedSecret": "adsadas13232",
    "authenticationPort": 1812,
    "connectionTimeoutInSeconds": 6,
    "enableAccounting": false,
    "accountingPort": 1813
  },
  "secondaryRadiusServer": {
    "serverIpAddr": "1.1.1.5",
    "sharedSecret": "dssdfksdnfsdf",
    "authenticationPort": 1812,
    "connectionTimeoutInSeconds": 6,
    "enableAccounting": false,
    "accountingPort": 1813
  }
}
```

```
}  
}
```

**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

# 69

## Advanced Device Configuration Resource

### Contents

- [Get the Advanced Device Configuration at domain level](#)
- [Update the Advanced Device Configuration at domain level](#)
- [Get the Advanced Device Configuration at Sensor level](#)
- [Update the Advanced Device Configuration at Sensor level](#)

### 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: <ul style="list-style-type: none"> <li>• DISABLED</li> <li>• DEVICE_ONLY</li> <li>• MANAGER_ONLY</li> <li>• DEVICE_AND_MANAGER</li> </ul>	string
showCPUUsageinCLI	Show CPU usage in CLI	boolean
restrictSSHAccessstoCLI	Restrict CLI access using SSH	boolean
enableSSHLogging	Enable SSH logging	boolean

Field Name	Description	Data Type
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
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](https://<NSM_IP>/sdkapi/domain/0/advanceddeviceconfiguration)

### Response

```
{
  "inheritSettings": false,
  "preAttackBytestoCapture": 128,
  "inspectTunneledTraffic": false,
  "cliActivityLogging": "DISABLED",
  "showCPUUsageinCLI": false,
  "restrictSSHAccessstoCLI": true,
  "enableSSHLogging": false,
  "permittedIPv4CIDRBlocks":
  [
    {
      "id": 1,
      "cidr": "1.1.1.1/32",
      "action": null
    }
  ],
  "permittedIPv6CIDRBlocks":
  [
    {
      "id": 2,
      "cidr": "2001:0DB9:0000:0000:0000:0000:0001/128",
      "action": null
    }
  ],
  "useTraditionalSnort": true
}
```



## Error Information

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
preAttackBytestoCapture	Attack bytes to capture. Can be 128, 256	int	Yes
inspectTunneledTraffic	Inspect tunneled traffic	boolean	Yes
cliActivityLogging	Log CLI activity. Values allowed are: <ul style="list-style-type: none"><li>• DISABLED</li><li>• DEVICE_ONLY</li><li>• MANAGER_ONLY</li><li>• DEVICE_AND_MANAGER</li></ul>	string	Yes
showCPUUsageinCLI	Show CPU usage in CLI	boolean	Yes
restrictSSHAccessstoCLI	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](https://<NSM_IP>/sdkapi/domain/0/advanceddeviceconfiguration)

### Payload

```
{
  "inheritSettings": false,
  "preAttackBytestoCapture": 128,
  "inspectTunneledTraffic": false,
  "cliActivityLogging": "DISABLED",
  "showCPUUsageinCLI": false,
  "restrictSSHAccessstoCLI": 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: <ul style="list-style-type: none"><li>• DISABLED</li><li>• DEVICE_ONLY</li><li>• MANAGER_ONLY</li><li>• DEVICE_AND_MANAGER</li></ul>	string
showCPUUsageinCLI	Show CPU usage in CLI	boolean
restrictSSHAccessstoCLI	Restrict CLI access using SSH	boolean
enableSSHLogging	Enable SSH logging	boolean

Field Name	Description	Data Type
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
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](https://<NSM_IP>/sdkapi/sensor/1001/advanceddeviceconfiguration)

### Response

```
{
  "inheritSettings": false,
  "preAttackBytestoCapture": 128,
  "inspectTunneledTraffic": false,
  "cliActivityLogging": "DISABLED",
  "showCPUUsageinCLI": false,
  "restrictSSHAccessstoCLI": true,
  "enableSSHLogging": false,
  "permittedIPv4CIDRBlocks":
  [
    {
      "id": 1,
      "cidr": "1.1.1.1/32",
      "action": null
    }
  ],
  "permittedIPv6CIDRBlocks":
  [
    {
      "id": 2,
      "cidr": "2001:0DB9:0000:0000:0000:0000:0001/128",
      "action": null
    }
  ],
  "useTraditionalSnort": true
}
```

## Error Information

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1106	Invalid Sensor
2	400	1001	Advanced Device Configuration is not supported on Sensor softwares prior to 8.3
3	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: <ul style="list-style-type: none"><li>• DISABLED</li><li>• DEVICE_ONLY</li><li>• MANAGER_ONLY</li><li>• DEVICE_AND_MANAGER</li></ul>	string	Yes
showCPUUsageinCLI	Show CPU usage in CLI	boolean	Yes
restrictSSHAccessstoCLI	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](https://<NSM_IP>/sdkapi/sensor/1001/advanceddeviceconfiguration)

### Payload

```
{
  "inheritSettings": false,
  "preAttackBytestoCapture": 128,
  "inspectTunneledTraffic": false,
  "cliActivityLogging": "DISABLED",
  "showCPUUsageinCLI": false,
  "restrictSSHAccessstoCLI": true,
  "enableSSHLogging": false,
  "permittedIPv4CIDRBlocks":
  [
    {
      "id": 1,
      "cidr": "1.1.1.1/32",
      "action": null
    }
  ],
  "permittedIPv6CIDRBlocks":
  [
    {
      "id": 2,
      "cidr": "2001:0DB9:0000:0000:0000:0000:0001/128",
      "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	1001	Advanced Device Configuration is not supported on sensor softwares prior to 8.3
3	400	1124	The Sensor is inactive
4	400	1001	Pre Attack Packet Capture Bytes if provided, can only be 128 and 256
5	400	1701	The cidrs provided are not present in the resource :: <list>
6	400	1701	The cidrs provided for addition are already present in the resource :: <list>
7	400	1701	Invalid CIDR notation : <list>
8	400	1701	Duplicate CIDR entry : <list>
9	400	1001	IP list is required
10	500	1001	Internal server errors





# 70 Attack Log Resource

## Contents

- [Get All Alerts](#)
- [Delete All Alerts](#)
- [Update All Alerts](#)
- [Get Alert Details](#)
- [Update Alert Details](#)
- [Delete Alert](#)
- [Get Component Alert Packet Log](#)
- [Get Packet Capture of an Alert](#)

## 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 <ul style="list-style-type: none"><li>• LAST_5_MINUTES</li><li>• LAST_1_HOUR</li><li>• LAST_6_HOURS</li><li>• LAST_12_HOURS</li><li>• LAST_24_HOURS</li><li>• LAST_7_DAYS</li><li>• LAST_14_DAYS</li><li>• CUSTOM</li></ul>	string	No
starttime	Start time	string	No
endtime	End time		No
Page	Next/Previous	string	No

Field Name	Description	Data Type	Mandatory
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, nspld, 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.

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
endpointExecutable	Endpoint Executable	object
detection	Detection	object
application	Application string	string
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
ipAddr	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
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?](https://<NSM_IP>/sdkapi/alerts?fromalert=1334242&page=next&timeperiod=custom&starttime=10/10/2015%2012:00&endtime=01/12/2015%2012:00)

[fromalert=1334242&page=next&timeperiod=custom&starttime=10/10/2015 12:00&endtime=01/12/2015 12:00](https://<NSM_IP>/sdkapi/alerts?fromalert=1334242&page=next&timeperiod=custom&starttime=10/10/2015%2012:00&endtime=01/12/2015%2012:00)

## 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":
      {
        "ipAddr": "1.1.1.10",
        "port": 58719,
        "hostName": "",
        "country": null,
        "os": null,
        "vmName": null,
        "proxyIP": "",
        "user": null,
        "risk": "Minimal Risk",
        "networkObject": null
      },
      "target":
      {
        "ipAddr": "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
      },
      "endpointExecutable":
      {
        "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": {
    "ipAddr": "1.1.1.10",
    "port": 58719,
    "hostName": "",
    "country": null,
    "os": null,
    "vmName": null,
    "proxyIP": "",
    "user": null,
    "risk": "Minimal Risk",
    "networkObject": null
  },
  "target": {
    "ipAddr": "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
  },
  "endpointExecutable": {
    "name": "",
    "hash": "",
    "malwareConfidence": ""
  },
  "detection": {
    "domain": "/My Company",
    "device": "prabu-6050",
```

```

        "interface": "5A-5B"
      },
      "application": "DNS",
      "layer7Data": ""
    }
  ]
}

```

### Error Information

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 <ul style="list-style-type: none"> <li>LAST_5_MINUTES</li> <li>Last_1_HOUR</li> <li>LAST_6_HOURS</li> <li>LAST_12_HOURS</li> <li>LAST_24_HOURS</li> <li>LAST_7_DAYS</li> <li>LAST_14_DAYS</li> <li>CUSTOM</li> </ul>	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, nspld, bmp, 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](https://<NSM_IP>/sdkapi/alerts?fromalert=1334242&page=next&timeperiod=custom&starttime=10/10/2015%2012:00&endtime=01/12/2015%2012:00)

### Response

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

## Error Information

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> &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 <ul style="list-style-type: none"><li>• LAST_5_MINUTES</li><li>• Last_1_HOUR</li><li>• LAST_6_HOURS</li><li>• LAST_12_HOURS</li><li>• LAST_24_HOURS</li><li>• LAST_7_DAYS</li><li>• LAST_14_DAYS</li><li>• CUSTOM</li></ul>	string	No
starttime	Start time	string	No
endtime	End time		No

Field Name	Description	Data Type	Mandatory
search	Search	string	No
Filter	Filter on following column is allowed name, assignTo, application, layer7Data, result, attackCount, relevance, alertId, direction, device, domain, interface, attackSeverity, nspld, 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](https://<NSM_IP>/sdkapi/alerts?fromalert=1334242&page=next&timeperiod=custom&starttime=10/10/2015%2012:00&endtime=01/12/2015%2012:00)

```
{
  "alertState": "Acknowledged",
  "assignTo": "admin"
}
```

#### Response

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

### Error Information

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	uniqueAlertId	string
alertState	alertState	string
summary	summary	object
details	details	object
description	description	object

## Example

### Request

GET https://<NSM\_IP>/sdkapi/alerts/6245941293374080682

### Response

```
{
  "name": "MALWARE: Blacklisted File Detected",
  "uniqueAlertId": "6245941293374080682",
  "alertState": "UnAcknowledged",
  "assignTo": "---",
  "summary":
  {
    "event":
    {
      "application": "HTTP",
      "protocol": "http",
      "domain": "My Company",
      "device": "NS9100-50",
      "interface": "G3/1-G3/2",
      "matchedPolicy": "CustomFP_Engine_With_AlertOnly",
      "zone": null,
      "vlan": "-11",
      "detection": "Signature",
      "time": "Jan 04, 2016 09:50:39",
      "direction": "Inbound",
      "result": "Inconclusive",
      "attackCount": 1,
      "relevance": "Unknown",
      "alertId": "2246015847757997493"
    },
    "attacker":
    {
      "ipAddr": "61.1.1.200",
```

```

        "port": 80,
        "hostName": null,
        "country": "India",
        "os": "---",
        "vmName": null,
        "proxyIP": "0.0.0.0",
        "user": "Unknown",
        "risk": "N/A",
        "networkObject": "---"
    },
    "target":
    {
        "ipAddr": "61.1.1.200",
        "port": 41128,
        "hostName": null,
        "country": "India",
        "os": "---",
        "vmName": null,
        "proxyIP": "0.0.0.0",
        "user": "Unknown",
        "risk": "N/A",
        "networkObject": "---"
    },
    "source": null,
    "destination": null,
    "zombie": null,
    "cAndcServer": null,
    "fastFluxAgent": null,
    "attackedHIPPEndpoint":
    {
        "ipAddr": "61.1.1.200",
        "port": 41128,
        "hostName": null,
        "country": "India",
        "os": "---",
        "vmName": null,
        "proxyIP": "0.0.0.0",
        "user": "Unknown",
        "risk": "N/A",
        "networkObject": "---"
    },
    "compromisedEndpoint": null
},
"details":
{
    "matchedSignature": null,
    "layer7":
    {
        "httpServerType": "Apache/2.2.13 (Fedora)
Last-Modified: Wed, 10 Oct 2012 05:19:15 GMT",
        "httpReturnCode": 200,
        "httpURI": "/Firewall.cpl",
        "httpUserAgent": "Wget/1.11.4 (Red Hat modified)",
        "httpRequestMethod": "GET",
        "httpHostHeader": null
    },
    "malwareFile":
    {
        "fileName": "/Firewall.cpl",
        "fileHash": "3f3f7c3b9722912ddeddf006cff9d9d0",
        "malwareName": null,
        "malwareConfidence": "Very High",
        "engine": "Manager Blacklist",
        "size": "6144 bytes"
    },
    "hostSweep": null,
    "portScan": null,
    "fastFlux": null,
    "triggeredComponentAttacks": null,
    "sqlInjection": null,
    "callbackDetectors": null,
    "exceededThreshold": null,
    "communicationRuleMatch": null
},

```

```
"description":
{
  "definition": "This alert indicates that a file with a blacklisted hash has been
detected. There are two file hash blacklists available:
  Manager Blacklist. A global (root admin domain) blacklist that is managed by users.
  McAfee Blacklist: A McAfee-maintained blacklist that is dynamically updated with
Callback Detectors updates.",
  "btf": "Medium",
  "rfSB": "No",
  "protectionCategory": "[Malware/Bot]",
  "target": "ServerOrClient",
  "httpResponseAttack": "No",
  "protocols": "[smtp, ftp, http]",
  "attackCategory": "Malware",
  "attackSubCategory": "---",
  "reference":
  {
    "nspId": "0x4840c300",
    "cveId": "[]",
    "microsoftId": "[]",
    "bugtraqId": "[]",
    "certId": null,
    "arachNidsId": "[]",
    "additionInfo": null
  },
  "signatures":
  [
    {
      "conditions": null
    }
  ],
  "componentAttacks": null,
  "comments":
  {
    "comments": "",
    "availableToChildDomains": true,
    "parentDomainComments": null
  }
}
```

### Error Information

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](https://<NSM_IP>/sdkapi/alerts/66692334234234)

```
{
  "alertState": "Acknowledged",
  "assignTo": "admin"
}
```

### Response

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

## Error Information

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](https://<NSM_IP>/sdkapi/alerts/66692334234234)

### Response

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

## Error Information

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

PUT [https://<NSM\\_IP>/sdkapi/alerts/12345678/triggeredpkt?sensorId=1001](https://<NSM_IP>/sdkapi/alerts/12345678/triggeredpkt?sensorId=1001)

#### Payload

NA

#### Response

<packet logs data in ZIP file>

### Error Information

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](https://<NSM_IP>/sdkapi/domain/0/threatanalysis/packetlog?alertId=103&device=NS-9200)

### Payload

NA

### Response

<packet capture file data>

## Error Information

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





# 71

## Traffic Statistics

### Contents

- *Get the Traffic Send/Received statistics*
- *Get the Flows statistics*
- *Get dropped packets statistics*
- *Get Malware stats grouped by engine*
- *Get Malware stats grouped by file type*
- *Get traffic statistics for Advance callback detection*
- *Get the traffic statistics for the SSL*
- *Get the traffic statistics for internal web certificate matches*
- *Reset SSL counters*

---

### 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

Field Name	Description	Data Type
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
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](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

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: <ul style="list-style-type: none"><li>• Inactive</li><li>• Active</li></ul>	string
outboundSynCookieProtection	Shows whether Outbound SYN cookie protection is active or inactive. Can have two values: <ul style="list-style-type: none"><li>• Inactive</li><li>• Active</li></ul>	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](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 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 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
fragmentReAssemblyTimeoutIPv4	IPv4 packets dropped due to fragment reassembly timeout	string
fragmentReAssemblyTimeoutIPv6	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

Field Name	Description	Data Type
policyResponseActionsFirewall	Packets dropped due to firewall policy response action	string
policyResponseActionsIPS	Packets dropped due to IPS policy response action	string
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](https://<NSM_IP>/sdkapi/sensor/1009/port/124/trafficstats/droppedpackets)

#### Response

```
{
  "crcFailures": 0,
  "devicePowerUp": 0,
  "deviceResourceExhaustion": 0,
  "fragmentReAssemblyTimeoutIPv4": 0,
  "fragmentReAssemblyTimeoutIPv6": 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
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
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](https://<NSM_IP>/sdkapi/sensor/1009/trafficstats/malwarestatsgroupbyengine)

#### Response

```
{
  "mlawareEngineTrafficStats": [
    {
      "engine": "Blacklist",
      "values": {
```

```

        "filesSubmitted":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,
            "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,
            "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,
            "cleanFiles":0,
            "veryHighMalwareConfidenceMatches":0,
            "highMalwareConfidenceMatches":0,
            "mediumMalwareConfidenceMatches":0,
            "lowMalwareConfidenceMatches":0,
            "veryLowMalwareConfidenceMatches":0,
            "unknownMalwareConfidenceMatches":0,
            "alertsGenerated":0,
            "filesBlocked":0,
            "connectionsReset":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 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](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
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](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 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 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
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](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 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 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 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

## 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](https://<NSM_IP>/sdkapi/sensor/1009/trafficstats/resetsslcounters)

#### 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		Invalid Sensor: When the device ID given is not valid

## Contents

- ▶ *Get the CLI Auditing Configuration at the domain level*
- ▶ *Update the CLI Auditing Configuration at domain level*
- ▶ *Get the CLI Auditing Configuration at Sensor level*
- ▶ *Update the CLI Auditing Configuration at the Sensor level*

---

## 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](https://<NSM_IP>/sdkapi/domain/0/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	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](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](https://<NSM_IP>/sdkapi/sensor/1001/cliauditing)

#### Response

```
{
  "inheritSettings": false,
  "enable": true
}
```

### Error Information

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>/cadsintegration

### 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/cli auditing](https://<NSM_IP>/sdkapi/sensor/1001/cli auditing)

#### 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



# 73

## Diagnostics Trace Resource

### Contents

- *Get the diagnostic trace files*
- *Upload the diagnostic trace file*
- *Get the upload status*
- *Export the Diagnostic Trace file captured*
- *Delete the Diagnostic Trace file captured*

### Get the diagnostic trace files

This URL Gets the diagnostics trace files.

#### Resource URL

GET /sensor/<sensor\_id>/diagnostictrace

#### 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/diagnostictrace](https://<NSM_IP>/sdkapi/sensor/1001/diagnostictrace)

##### 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>/diagnostictrace/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/diagnostictrace/upload](https://<NSM_IP>/sdkapi/sensor/1001/diagnostictrace/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 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>/diagnostictrace/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/diagnostictrace/upload](https://<NSM_IP>/sensor/1001/diagnostictrace/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>/diagnostictrace/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/diagnostictrace/export](https://<NSM_IP>/sdkapi/sensor/1001/diagnostictrace/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>/diagnostictrace

### 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/diagnostictrace

### 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

# 74 Health Check Resource

## Contents

- *Get the Health Check*
- *Run the Health Check*

---

## 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](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 codes are 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: <ul style="list-style-type: none"><li>• Single value "default". Which will run health check only for the features which are selected by default</li><li>• Single value "all". Which will run health check for all the features</li><li>• Single value "summary". Which will run health check for summary features</li><li>• Single value "databasechecks". Which will run health check for database check features</li><li>• Single value "connectivitychecks". Which will run health check for connectivity check features</li><li>• List of the feature id for which the health check should run</li></ul>	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
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	Health check notes	string
lastRun	Health check last run time	string
run	If the feature check happened	boolean

### Example

#### Request

PUT [https://<NSM\\_IP>/healthcheck](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 codes are returned by this URL:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	400	3702	Invalid Id Provided : <list of invalid ids>

## Contents

- ▶ [Get the McAfee Cloud integration settings](#)
- ▶ [Update the McAfee Cloud Integration Settings](#)
- ▶ [Test the connection for McAfee Cloud integration settings](#)
- ▶ [Get the McAfee Cloud Statistics](#)
- ▶ [Reset McAfee cloud statistics](#)

---

## 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

Field Name	Description	Data Type
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>/sdkapi/mcafeecloudintegration](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': 'M46MS8MX1e/AVyAbtyqbxBdPwMPtXZTX1Fj2RibW0Ch68tpnCimU3V2u1KB4nnNO',
  'provisioningKey': 'Ya+WyijMltOTWuLpzRHSbvK7bLeSewQIzxmx6LzQca0='
}
```

### Error Information

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](https://<NSM_IP>/mcafeecloudintegration)

### Payload

```
{
  "enable": true,
  "tenantId": "5JT9TV3F7k9taFget0p37O5shpe0j+1FX8+ggrTZQ1/u99z8vkXzFTjRSkBD4BZu"
}
```

### 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 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>/mcafeeccloudintegrator/testconnection](https://<NSM_IP>/mcafeeccloudintegrator/testconnection)

### 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

---

## Get the McAfee Cloud Statistics

This URL gets the McAfee cloud statistics.

### Resource URL

GET /mcafeeccloudinteration/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

Field Name	Description	Data Type
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](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 codes are 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

PUT [https://<NSM\\_IP>/mcafeecloudintegraton/resetstatistics](https://<NSM_IP>/mcafeecloudintegraton/resetstatistics)

#### 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



# 76

## Performance Monitoring Resource

### Contents

- *Get the Performance Monitoring settings at the domain level*
- *Update the performance monitoring settings at the domain level*
- *Get the Performance monitoring settings at the Sensor level*
- *Update the Performance monitoring settings at the Sensor level*

---

### 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](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

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

Field Name	Description	Data Type	Mandatory
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

PUT [https://<NSM\\_IP>/sdkapi/domain/0/performancemonitoring](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 than high usage parameter

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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
11	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

Field Name	Description	Data Type
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](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": 51,
    "resetThresholdValue": 31,
    "enableAlarm": true
  }
]
}
```



```

        "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

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

PUT [https://<NSM\\_IP>/sdkapi/sensor/1001/performancemonitoring](https://<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
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



# Attack Set Profile

## Contents

- *Get attack set profile configuration details at domain level*
- *Get attack set profile configuration details using Policy ID at domain level*
- *Create new attack set profile at domain level*
- *Update attack set profile configuration detail*
- *Delete attack set profile*

## 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
enableRfSBExploit	RfSB exploit configuration	boolean

Field Name	Description	Data Type
enableRfSBMalware	RfSB malware configuration	boolean
enableRfSBRecon	RfSB Recon configuration	boolean
enableRfSBPolicy	RfSB Policy configuration	boolean
isEditable	AttackSet editable configuration	boolean

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/domain/0/attacksetprofile/getallrules](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",
      "enableRfSBExploit": 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",
      "enableRfSBExploit": 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",
      "enableRfSBExploit": false,
      "enableRfSBMalware": false,
      "enableRfSBRecon": false,
      "enableRfSBPolicy": false,
      "isEditable": false,
      "rules": [],
    },
  ],
}
```

### Error Information

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
enableRfSBExploit	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
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

Field Name	Description	Data Type
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>](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",
  "enableRfSBExploit": 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

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
enableRfSBExploit	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: <ul style="list-style-type: none"> <li>• INCLUDE</li> <li>• EXCLUDE</li> </ul>	string	No
comment	Comments	string	No
isSpecificAttack	Specific Attack name	boolean	No
AttackList	List of attacks	string	No

Field Name	Description	Data Type	Mandatory
minSeverity	Severity level values can be: <ul style="list-style-type: none"> <li>NONE</li> <li>HIGH_1</li> <li>HIGH_8</li> <li>HIGH_7</li> <li>MEDIUM_6</li> <li>MEDIUM_5</li> <li>MEDIUM_4</li> <li>LOW_3</li> <li>LOW_2</li> <li>LOW_1</li> <li>INFORMATIONAL_0</li> </ul>	string	No
maxBTP	BTP Level values can be: <ul style="list-style-type: none"> <li>NONE_0</li> <li>HIGH_7</li> <li>HIGH_6</li> <li>MEDIUM_5</li> <li>MEDIUM_4</li> <li>MEDIUM_3</li> <li>LOW_2</li> <li>LOW_1</li> </ul>	string	No
attackType	Type of attack values can be: <ul style="list-style-type: none"> <li>ANY</li> <li>RF_SB_ONLY</li> </ul>	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](https://<NSM_IP>/sdkapi/domain/<domainId>/attacksetprofile/createruleset)

```
{
  "policyName": "New Attackset API",
  "description": "Test creation ",
  "enableRfSBExploit": 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

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
5	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
enableRfSBExploit	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 • HIGH_9 • HIGH_8 • HIGH_7 • MEDIUM_6 • MEDIUM_5 • MEDIUM_4 • LOW_3 • LOW_2 • LOW_1 • INFORMATIONAL_0	string	No
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

Field Name	Description	Data Type	Mandatory
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>](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.",
  "enableRfSBExploit": 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

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
5	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>](https://<NSM_IP>/sdkapi/domain/<domainId>/attacksetprofile/deletruleset/<policyId>)

### Payload

None

### Response

```
{
  status:1
}
```

## Error Information

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

# 78

## Proxy Server

### Contents

- *Get the proxy server configuration at domain level*
- *Update Proxy Server configuration*
- *Get the proxy server configuration at device level*
- *Update the proxy server configuration at device level*
- *Get the proxy server configuration at the Manager level*
- *Update the proxy server configuration at the Manager level*

---

## 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	User name	string
password	Password	string

### Example

#### Request

GET [https://<NSM\\_IP>/sdkapi/domain/0/proxyserver](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**

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	User name	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](https://<NSM_IP>/sdkapi/domain/<domainId>/proxyserver)



## Payload

```
----Boundary_1_12424925_1353496814940
Content-Type: application/json

{"useDeviceListSettings":false,"useProxyserver":true,"proxyServerNameOrIPAddr":"1.1.1.1","proxyPort":8443,"userName":"admin","password":"admin123"}

----Boundary_1_12424925_1353496814940
Content-Type: application/octet-stream

<file_data>

----Boundary_1_12424925_1353496814940--
```

## Response

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

## Error Information

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	User name	string
password	Password	string

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/device/1001/proxyserver](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

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	User name	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](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 codes are 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	User name	string
password	Password	string

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/domain/proxyserver](https://<NSM_IP>/sdkapi/domain/proxyserver)

### Response

```
{
  "useProxyserver": false,
  "proxyServerNameOrIPAddr": 1.1.1.1,
  "proxyPort": 8443,
  "userName": null,
  "password": null
}
```

### Error Information

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
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](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 codes are returned by the URL:

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



**Contents**

- ▶ *Get the Cluster ID based on name*
- ▶ *Get the Controller ID based on name*
- ▶ *Get the Virtual Probe status*
- ▶ *Get the vNSP Controllers present in the domain*
- ▶ *Create the vNSP Controller*
- ▶ *Get the vNSP Controller details*
- ▶ *Test Manager-Controller connection*
- ▶ *Test Manager-Controller Cloud connection*
- ▶ *Update the vNSP Controller*
- ▶ *Delete the vNSP Controller*
- ▶ *Upgrade the vNSP Controller software*
- ▶ *Get the vNSP Clusters present in the domain*
- ▶ *Create the vNSP Cluster*
- ▶ *Get the vNSP Cluster details*
- ▶ *Update the vNSP Cluster*
- ▶ *Delete the vNSP Cluster*
- ▶ *Get the Protected VM Groups present in the vNSP Cluster*
- ▶ *Create the Protected VM Group under vNSP Cluster*
- ▶ *Get the Protected VM Group details*
- ▶ *Update the Protected VM Group*
- ▶ *Delete the Protected VM Group*
- ▶ *Download the Cluster Virtual Probe agent*
- ▶ *Download the Cluster probe agent without login*
- ▶ *Update the vNSP Cluster agent*
- ▶ *Get the list of Protected VM Hosts*

---

**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](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](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

Field Name	Description	Data Type
hostname	Virtual machine host name	String
workloadOS	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>](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 • 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

Field Name	Description	Data Type
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](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

Field Name	Description	Data Type	Mandatory
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: <ul style="list-style-type: none"> <li>• Amazon</li> <li>• Azure</li> </ul>	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](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
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
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



Field Name	Description	Data Type
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](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](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](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
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: <ul style="list-style-type: none"> <li>Amazon</li> <li>Azure</li> </ul>	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](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](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 BodyPart 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](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](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
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](https://<NSM_IP>/sdkapi/cloud/0/cluster)

#### Payload

```
{
  "name": "Cloud_Cluster",
  "description": "api updated",
  "cloudConnector": "Cloud_Controller",
  "subscription id",
  "subscription":
  "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](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](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](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

Field Name	Description	Data Type
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: <ul style="list-style-type: none"> <li>• Ingress</li> <li>• Egress</li> <li>• Ingress &amp; Egress</li> </ul>	String
inspectionMode	Inspection mode. Values can be : <ul style="list-style-type: none"> <li>• IPS</li> <li>• IDS</li> </ul>	String

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/cloud/cluster/101/vmgroups](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
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: <ul style="list-style-type: none"> <li>Ingress</li> <li>Egress</li> <li>Ingress &amp; Egress</li> </ul>	String	Yes
inspectionMode	Inspection mode. Values can be: <ul style="list-style-type: none"> <li>IPS</li> <li>IDS</li> </ul>	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](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
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 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: <ul style="list-style-type: none"> <li>• Ingress</li> <li>• Egress</li> <li>• Ingress &amp; Egress</li> </ul>	String
inspectionMode	Inspection mode. Values can be : <ul style="list-style-type: none"> <li>• IPS</li> <li>• IDS</li> </ul>	String

## Example

### Request

PUT [https://<NSM\\_IP>/sdkapi/cloud/cluster/101/getvmgroup](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: <ul style="list-style-type: none"><li>• Ingress</li><li>• Egress</li><li>• Ingress &amp; Egress</li></ul>	String	Yes
inspectionMode	Inspection mode. Values can be : <ul style="list-style-type: none"><li>• IPS</li><li>• IDS</li></ul>	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](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](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: <ul style="list-style-type: none"><li>Windows (default)</li><li>Linux</li></ul>	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](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: <ul style="list-style-type: none"><li>• Windows (default)</li><li>• Linux</li></ul>	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](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
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](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
awsInstanceId	Unique ID generated by AWS	String

## Example

### Request

POST [https://<NSM\\_IP>/sdkapi/cloud/cluster/101/getProtectedVMHosts](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

## Quarantine zone resource

### Contents

- *Get quarantine zone Details using QuarantineZone ID at domain level*
- *Get all quarantine zones at domain level*
- *Update quarantine zone*
- *Add quarantine zone*
- *Delete quarantine zone*

---

## Get quarantine zone Details using QuarantineZone 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

Field Name	Description	Data Type
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
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](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

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	404	1105	Invalid domain
2	500	1001	Invalid QuarantineZone 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
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](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**

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](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**

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Invalid QuarantineZone ID
2	500	1001	Given policy cannot be updated at this domain
3	404	1105	Invalid domain
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	QuarantineZoneDescription: field should not be empty
7	500	1001	QuarantineZoneName: The maximum length for the field is 64
8	500	1001	QuarantineZoneDescription: The maximum length for the field is 150
9	500	1001	QuarantineZoneName: 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 QuarantineZone	number

## Example

### Request

POST [https://<NSM\\_IP>/sdkapi/domain/0/quarantineZone](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**

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	QuarantineZoneDescription: field should not be empty
6	500	1001	QuarantineZoneName: The maximum length for the field is 64
7	500	1001	QuarantineZoneDescription: The maximum length for the field is 150
8	500	1001	QuarantineZoneName: 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 IDs	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](https://<NSM_IP>/sdkapi/domain/0/quarantineZone)

### Payload

```
{"quarantineZoneIdsList": [216]}
```

### Response

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

## Error Information

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



# 81

## GTI and Telemetry Resource

### Contents

- *Get the GTI private cloud configuration*
- *Update the GTI private cloud configuration*
- *Import GTI private cloud certificate to the Manager*
- *Get the IP status from a GTI private cloud*
- *Get the Telemetry configuration*
- *Update the Telemetry configuration*

---

### 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**

The URL returns the following Error Codes:

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](https://<NSM_IP>/sdkapi/gticonfiguration/private)

**Payload**

```
{
  "enabled":false,"server":null,"certificateStatus":false
}
```

**Response**

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



## Error Information

The URL returns the following Error Codes:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	1111	Certificate should be present on the NSM
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 BodyPart	object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart [0]	Holds the FileFormat 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 InputStream	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](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

The URL returns the following Error Codes:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	400	5301	Invalid FileType given for import : The file name does not have any extension
3	400	5301	Invalid FileType 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](https://<NSM_IP>/sdkapi/gticonfiguration/private/1.1.1.1/testconnection)

#### Payload

None

#### Response

```
{
  "status": "High", "country": ""
}
```

### Error Information

The URL returns the following Error Codes:

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

Field Name	Description	Data Type
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	IPs excluded	array
alertDataDetailsFilterLevel	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 alertDataDetailsFilterLevel:

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](https://<NSM_IP>/sdkapi/gticonfiguration)

### Payload

None

### Response

```
{
  "alertDataDetails": {"AlertDataDetailsEnabled": true, "excludedIpList":
    ["1.1.1.1/32"], "alertDataDetailsFilterLevel":
    {"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": "123
    4567890", "email": "EIT@mcafee.com"}
}
```

## Error Information

The URL returns the following Error Codes:

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
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
alertDataDetailsFilterLevel	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 alertDataDetailsFilterLevel:

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](https://<NSM_IP>/sdkapi/gticonfiguration)

### Payload

```
{
  "alertDataDetails": {"AlertDataDetailsEnabled": true, "excludedIpList": ["1.1.1.1/32"],
    "alertDataDetailsFilterLevel": {"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

The URL returns the following Error Codes:

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

### Contents

- *Get the vIPS licenses present on the Manager*
- *Get the Proxy licenses present on the Manager*
- *Get the Capacity licenses present on the Manager*
- *Import license to the Manager*
- *Assign a license*
- *Unassign a license*
- *Delete licenses*
- *Get the Sensors for association*

---

## 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 VMIPSLicenseDetails	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

Field Name	Description	Data Type
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](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

The URL returns the following Error Codes:

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 LicenseDetails 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/proxy](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

The URL returns the following Error Codes:

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 Proxy 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 LicenseDetails 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](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

The URL returns the following Error Codes:

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 BodyPart objects	object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the FileFormat 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 InputStream	application/octet-stream	Yes

Details of license file:

Field Name	Description	Data Type	Mandatory
File	The license file data	ByteArrayInputStream	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/license](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

The URL returns the following Error Codes:

No	HTTP Error Code	SDK API errorId	SDK API errorMessage
1	500	1001	Internal error
2	500	1207	Invalid proxy decryption license detected. The license is expired.
3	500	1208	Invalid capacity license detected. The license has expired.

## 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 IS 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](https://<NSM_IP>/sdkapi/assignlicense)

### Payload

```
{
  "licenseId": "50002",
  "grantIndex": "3",
  "grantId": "0030080",
  "sensorId": "1006"
}
```

### Response

```
{
  'status' : 1
}
```

## Error Information

The URL returns the following Error Codes:

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 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](https://<NSM_IP>/sdkapi/unassignlicense)

### Payload

```
{
  "licenseId": "50002",
  "grantIndex": "3",
  "grantId": "0030080",
}
```

### Response

```
{
  'status' : 1
}
```

## Error Information

The URL returns the following Error Codes:

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 IDs	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](https://<NSM_IP>/sdkapi/license/delete/proxy)

#### Payload

```
{
  'licenseId': ['10004']
}
```

#### Response

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

### Error Information

The URL returns the following Error Codes:

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](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

The URL returns the following Error Codes:

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



## IPS Inspection Whitelist Resource

### Contents

- ▶ *Get IPS Inspection whitelist from the Manager*
- ▶ *Get Details of a domain name from IPS Inspection Whitelist*
- ▶ *Add domain name to IPS Inspection whitelist*
- ▶ *Import the Domain Name Exceptions to the Manager*
- ▶ *Export the Domain Name Exceptions from the Manager*
- ▶ *Update the details of Domain Name Exceptions*
- ▶ *Delete Domain Name Exceptions from the IPS Inspection Whitelist*
- ▶ *Delete all Domain Names from IPS Inspection Whitelist*
- ▶ *Update status of Domain Name Exceptions from IPS Inspection Whitelist*

---

### Get IPS Inspection whitelist from the Manager

This URL retrieves the Domain Name Exceptions from the Manager.

#### Resource URL

GET /domainnameexceptions /ipsinspectionwhitelist

#### 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 whitelist	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

Field Name	Description	Data Type
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/ipsinspectionwhitelist](https://<NSM_IP>/sdkapi/domainnameexceptions/ipsinspectionwhitelist)

#### 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 Whitelist

This URL retrieves the details of the Domain Name Exception from the IPS Inspection whitelist.

### Resource URL

GET /domainnameexceptions/ipsinspectionwhitelist/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 whitelist	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/ipsinspectionwhitelist/IPSDNEDetail/www.google.com](https://<NSM_IP>/domainnameexceptions/ipsinspectionwhitelist/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

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 whitelist

This URL adds domain name to IPS Inspection whitelist.

### Resource URL

POST /domainnameexceptions/ipsinspectionwhitelist

### 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 whitelist	number

### Example

#### Request

POST [https://<NSM\\_IP>/sdkapi/domainnameexceptions/ipsinspectionwhitelist](https://<NSM_IP>/sdkapi/domainnameexceptions/ipsinspectionwhitelist)

#### Payload

```
{
  "state": "E",
  "domainName": "www.google1.com",
  "comment": "updated domain"
}
```

#### Response

```
{
  "createdResourceId": 10010
}
```

### 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 Field is required
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

## Import the Domain Name Exceptions to the Manager

This URL imports the Domain Names from the IPS inspection whitelist to the Manager.

### Resource URL

POST /domainnameexceptions/ipsinspectionwhitelist/import

## Request Parameters

URL Parameters: None

Payload Request Parameters

Field Name	Description	Data Type	Mandatory
MultiPart	Holds the BodyPart objects	object	Yes

Details of BodyPart[0]:

Field Name	Description	Data Type	Mandatory
BodyPart[0]	Holds the DNEFileElement 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	FileType should be .csv	string	No

Details of BodyPart[1]:

Field Name	Description	Data Type	Mandatory
BodyPart[1]	Holds the InputStream	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

## Example

### Request

POST [https://<NSM\\_IP>/sdkapi/domainnameexceptions/ipsinspectionwhitelist/import](https://<NSM_IP>/sdkapi/domainnameexceptions/ipsinspectionwhitelist/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---
```

## 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	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 whitelist.

## Resource URL

GET /domainnameexceptions/ipsinspectionwhitelist/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://<NSM\_IP>/sdkapi/domainnameexceptions/ipsinspectionwhitelist/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 whitelist.

### Resource URL

PUT /domainnameexceptions/ipsinspectionwhitelist

### 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
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://<NSM\\_IP>/sdkapi/domainnameexceptions/ipsinspectionwhitelist](https://<NSM_IP>/sdkapi/domainnameexceptions/ipsinspectionwhitelist)

#### 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
2	500	1001	Internal Error Message: Domain name is not found <domainName>

S.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

## Delete Domain Name Exceptions from the IPS Inspection Whitelist

This URL deletes the Domain Name Exceptions specified in the stringList.

### Resource URL

DELETE /domainnameexceptions/ipsinspectionwhitelist

### 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://<NSM\\_IP>/sdkapi/domainnameexceptions/ipsinspectionwhitelist](https://<NSM_IP>/sdkapi/domainnameexceptions/ipsinspectionwhitelist)

#### 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 Whitelist

This URL deletes all Domain Name Exceptions.

### Resource URL

DELETE /domainnameexceptions/ipsinspectionwhitelist/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/ipsinspectionwhitelist/all

#### Payload

None

#### 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	Error while deleting all DNEs

## Update status of Domain Name Exceptions from IPS Inspection Whitelist

This URL updates the status of Domain Name Exceptions specified in the Integer List.

### Resource URL

PUT /domainnameexceptions/ipsinspectionwhitelist/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 entryIDs of domain names to be updated	IntegerList	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/domainnameexceptions/ipsinspectionwhitelist/bulkUpdate](https://<NSM_IP>/sdkapi/domainnameexceptions/ipsinspectionwhitelist/bulkUpdate)

#### Payload

```
{
  "state": "D"
  "entryIDs": [10118,10119]
}
```

#### 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: Error while bulk update



# 84

## SSL Exception Rules

### Contents

- *Get all the SSL Outbound Exception Rules*
- *Get single Outbound Exception Rule*
- *Create an Outbound Exception Rule*
- *Update an Outbound Exception Rule*
- *Delete an Outbound Exception Rule*

---

## 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

Field Name	Description	Data Type
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: <ul style="list-style-type: none"> <li>• 0: The resource type is domain (for rules defined at the domain level)</li> <li>• 1: The resource type is Sensor (for rules defined that the Sensor level)</li> <li>• 2: The resource type is Vids (for rules defined at the interface and the sub-interface level)</li> <li>• 3: The resource type is NTBA_ZONE (for rules defined at NTBA inside and outside zones)</li> <li>• 4: The resource type is NTBA_SENSOR (for rules defined at NTBA level)</li> <li>• 5: The resource type is NTBA_DOMAIN</li> </ul>	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

## Example

### Request

GET [https://<NSM\\_IP>/sdkapi/domain/0/outboundsslexceptions](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
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: <ul style="list-style-type: none"> <li>• 0: The resource type is domain (for rules defined at the domain level)</li> <li>• 1: The resource type is Sensor (for rules defined that the Sensor level)</li> <li>• 2: The resource type is Vids (for rules defined at the interface and the sub-interface level)</li> <li>• 3: The resource type is NTBA_ZONE (for rules defined at NTBA inside and outside zones)</li> <li>• 4: The resource type is NTBA_SENSOR (for rules defined at NTBA level)</li> <li>• 5: The resource type is NTBA_DOMAIN</li> </ul>	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

## Example

### Payload

None

### Request

GET [https://<NSM\\_IP>/sdkapi/domain/0/outboundsslexceptions/101](https://<NSM_IP>/sdkapi/domain/0/outboundsslexceptions/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

## Response Parameters

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://<NSM\\_IP>/sdkapi/domain/0/outboundsslexceptions](https://<NSM_IP>/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.
6	400	1422	Resource is not visible in this domain
7	400	1001	Ignore Rule with the same name already exists

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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
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

## 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/outboundsslexceptions/101](https://<NSM_IP>/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, commas, periods, hyphen, or an underscore

S.No	HTTP Error Code	SDK API errorId	SDK API errorMessage
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 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
status	Set to 1 if the operation was successful	number

### Example

#### Request

DELETE https://<NSM\_IP>/sdkapi/domain/0/outboundsslexceptions/101

#### 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	404	1408	Invalid Rule ID or Provided Rule ID is not visible to this domain

# 85

## Dashboard Monitors

### Contents

- ▶ *Get top active botnets*
- ▶ *Get top attack applications*
- ▶ *Get top attack subcategories*
- ▶ *Get top attacker countries*
- ▶ *Get top attackers*
- ▶ *Get top attacks*
- ▶ *Get top highrisk hosts*
- ▶ *Get top malware downloads*
- ▶ *Get top target countries*
- ▶ *Get top targets*
- ▶ *Get top unblocked malware downloads*
- ▶ *Get top endpoint executables*

---

### 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: <ul style="list-style-type: none"><li>• LAST_5_MINUTES</li><li>• LAST_1_HOUR</li><li>• LAST_6_HOURS</li><li>• LAST_12_HOURS</li><li>• LAST_24_HOURS</li><li>• LAST_48_HOURS</li><li>• LAST_7_DAYS</li><li>• LAST_14_DAYS</li></ul>	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](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: <ul style="list-style-type: none"><li>• LAST_5_MINUTES</li><li>• LAST_1_HOUR</li><li>• LAST_6_HOURS</li><li>• LAST_12_HOURS</li><li>• LAST_24_HOURS</li><li>• LAST_48_HOURS</li><li>• LAST_7_DAYS</li><li>• LAST_14_DAYS</li></ul>	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](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: <ul style="list-style-type: none"><li>• LAST_5_MINUTES</li><li>• LAST_1_HOUR</li><li>• LAST_6_HOURS</li><li>• LAST_12_HOURS</li><li>• LAST_24_HOURS</li><li>• LAST_48_HOURS</li><li>• LAST_7_DAYS</li><li>• LAST_14_DAYS</li></ul>	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](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: <ul style="list-style-type: none"><li>• LAST_5_MINUTES</li><li>• LAST_1_HOUR</li><li>• LAST_6_HOURS</li><li>• LAST_12_HOURS</li><li>• LAST_24_HOURS</li><li>• LAST_48_HOURS</li><li>• LAST_7_DAYS</li><li>• LAST_14_DAYS</li></ul>	string	No

### 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: <ul style="list-style-type: none"><li>• LAST_5_MINUTES</li><li>• LAST_1_HOUR</li><li>• LAST_6_HOURS</li><li>• LAST_12_HOURS</li><li>• LAST_24_HOURS</li><li>• LAST_48_HOURS</li><li>• LAST_7_DAYS</li><li>• LAST_14_DAYS</li></ul>	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](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
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: <ul style="list-style-type: none"> <li>• LAST_5_MINUTES</li> <li>• LAST_1_HOUR</li> <li>• LAST_6_HOURS</li> <li>• LAST_12_HOURS</li> <li>• LAST_24_HOURS</li> <li>• LAST_48_HOURS</li> <li>• LAST_7_DAYS</li> <li>• LAST_14_DAYS</li> </ul>	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](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: <ul style="list-style-type: none"> <li>• LAST_5_MINUTES</li> <li>• LAST_1_HOUR</li> <li>• LAST_6_HOURS</li> <li>• LAST_12_HOURS</li> <li>• LAST_24_HOURS</li> <li>• LAST_48_HOURS</li> <li>• LAST_7_DAYS</li> <li>• LAST_14_DAYS</li> </ul>	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](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: <ul style="list-style-type: none"><li>• LAST_5_MINUTES</li><li>• LAST_1_HOUR</li><li>• LAST_6_HOURS</li><li>• LAST_12_HOURS</li><li>• LAST_24_HOURS</li><li>• LAST_48_HOURS</li><li>• LAST_7_DAYS</li><li>• LAST_14_DAYS</li></ul>	string	No

## 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](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 LAST_14_DAYS. Duration can be: <ul style="list-style-type: none"><li>• LAST_5_MINUTES</li><li>• LAST_1_HOUR</li><li>• LAST_6_HOURS</li><li>• LAST_12_HOURS</li><li>• LAST_24_HOURS</li><li>• LAST_48_HOURS</li><li>• LAST_7_DAYS</li><li>• LAST_14_DAYS</li></ul>	string	No

### 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](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: <ul style="list-style-type: none"><li>• LAST_5_MINUTES</li><li>• LAST_1_HOUR</li><li>• LAST_6_HOURS</li><li>• LAST_12_HOURS</li><li>• LAST_24_HOURS</li><li>• LAST_48_HOURS</li><li>• LAST_7_DAYS</li><li>• LAST_14_DAYS</li></ul>	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](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
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](/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: <ul style="list-style-type: none"><li>• LAST_5_MINUTES</li><li>• LAST_1_HOUR</li><li>• LAST_6_HOURS</li><li>• LAST_12_HOURS</li><li>• LAST_24_HOURS</li><li>• LAST_48_HOURS</li><li>• LAST_7_DAYS</li><li>• LAST_14_DAYS</li></ul>	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](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: <ul style="list-style-type: none"> <li>LAST_5_MINUTES</li> <li>LAST_1_HOUR</li> <li>LAST_6_HOURS</li> <li>LAST_12_HOURS</li> <li>LAST_24_HOURS</li> <li>LAST_48_HOURS</li> <li>LAST_7_DAYS</li> <li>LAST_14_DAYS</li> </ul>	string	No
counttype	Allowed values are: <ul style="list-style-type: none"> <li>attackCount</li> <li>endpointcount</li> </ul> Default value is endpointcount.	string	No
confidencetype	Confidence type can be: <ul style="list-style-type: none"> <li>malwareConfAny</li> <li>malwareConfHigh</li> </ul> Default value is malwareConfHigh.	string	No
classificationtype	Allowed values are: <ul style="list-style-type: none"> <li>any</li> <li>blacklisted</li> <li>whitelisted</li> <li>unclassified</li> </ul> Default value is any.	string	No

**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





## 86

## 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



# Index

## A

about this guide [19](#)

## C

conventions and icons used in this guide [19](#)

## D

documentation

audience for this guide [19](#)

typographical conventions and icons [19](#)

